ON THE DISTRIBUTION OF THE SIGNS OF THE CONJUGATES OF THE CYCLOTOMIC UNITS IN THE MAXIMAL REAL SUBFIELD OF THE qth CYCLOTOMIC FIELD, q A PRIME

Thesis by

Daniel Lee Davis

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California 91109

1969

(Submitted April 4, 1969)

Acknowledgements

I am happy to have this opportunity to thank the many people who have helped in the preparation of this thesis. First of all I am most indebted to my advisor, Dr. Olga Taussky Todd, not only for her advice and constant encouragement in the preparation of this thesis but also for her interest in my well being as a graduate student. It is to her that I am most grateful. Also, I wish to express my sincere gratitude to Dr. Everett C. Dade who not only formulated the problem studied in this thesis but who was also a constant source of ideas. I am also very grateful to Dr. Dennis Estes and Dr. Hershey Kisilevsky for their comments and suggestions on particular chapters of this thesis.

I wish to acknowledge the patience and assistance of my wife, Susan. She has been a constant source of inspiration. I wish also to express my gratitude to my parents, who started it all.

I should also like to thank the Woodrow Wilson Foundation for providing me with a fellowship during the first year of graduate study and the U. S. Office of Education, for providing generous financial assistance during the last three years through a National Defense Education Act Fellowship. I wish to thank the California Institute of Technology for financial support for summer research and the National Science Foundation for providing me with computer time.

Abstract

Let $F = Q(\zeta + \zeta^{-1})$ be the maximal real subfield of the cyclotomic field $Q(\zeta)$ where ζ is a primitive qth root of unity and q is an odd rational prime. The numbers $\upsilon_1 = -1$, $\upsilon_k = (\zeta^k - \zeta^{-k})/(\zeta - \zeta^{-1})$, $k = 2, \dots, p$, $p = (q-1)/2$, are units in F and are called the cyclotomic units. In this thesis the sign distribution of the conjugates in F of the cyclotomic units is studied.

Let $G(F/Q)$ denote the Galois group of F over Q, and let V denote the units in F. For each $\sigma \in G(F/Q)$ and $\mu \in V$ define a mapping $sgn_\sigma : V \to GF(2)$ by $sgn_\sigma(\mu) = 1$ iff $\sigma(\mu) < 0$ and $sgn_\sigma(\mu) = 0$ iff $\sigma(\mu) > 0$. Let $\{\sigma_1, \dots, \sigma_p\}$ be a fixed ordering of $G(F/Q)$. The matrix $M_q = (sgn_{\sigma_j}(\upsilon_i))$, $i, j = 1, \dots, p$ is called the matrix of cyclotomic signatures. The rank of this matrix determines the sign distribution of the conjugates of the cyclotomic units. The matrix of cyclotomic signatures is associated with an ideal in the ring $GF(2)[x] / \langle x^p + 1 \rangle$ in such a way that the rank of the matrix equals the GF(2)-dimension of the ideal. It is shown that if $p = (q-1)/2$ is a prime and if 2 is a primitive root mod p, then M_q is non-singular. Also let p be arbitrary, let ℓ be a primitive root mod q and let $L = \{i \mid 0 \leqslant i \leqslant p-1$, the least positive residue of ℓ^i mod q is greater than $p\}$. Let $H_q(x) \in GF(2)[x]$ be defined by $H_q(x) = \text{g.c.d.}\left((\sum_{i \in L} x^i)(x+1) + 1,\ x^p + 1 \right)$. It is shown that the rank of M_q equals the difference p - degree $H_q(x)$.

Further results are obtained by using the reciprocity theorem of class field theory. The reciprocity maps for a certain abelian extension of F and for the infinite primes in F are associated with the signs of conjugates. The product formula for the reciprocity maps is used to

associate the signs of conjugates with the reciprocity maps at the primes which lie above (2). The case when (2) is a prime in F is studied in detail. Let T denote the group of totally positive units in F. Let U be the group generated by the cyclotomic units. Asume that (2) is a prime in F and that p is odd. Let $F_{(2)}$ denote the completion of F at (2) and let $V_{(2)}$ denote the units in $F_{(2)}$. The following statements are shown to be equivalent. 1) The matrix of cyclotomic signatures is non-singular. 2) $U \cap T = U^2$. 3) $U \cap F_{(2)}^2 = U^2$. 4) $V_{(2)}/V_{(2)}^2 = \langle \upsilon_1 V_{(2)}^2 \rangle \oplus \cdots \oplus \langle \upsilon_p V_{(2)}^2 \rangle \oplus \langle 3V_{(2)}^2 \rangle$.

The rank of M_q was computed for $5 \leq q \leq 929$ and the results appear in tables. On the basis of these results and additional calculations the following conjecture is made: If q and $p = (q-1)/2$ are both primes, then M_q is non-singular.

Table of Contents

Acknowledgements ii

Abstract iii

Chapter I. Introduction 1

Chapter II. The Matrix of Cyclotomic Signatures 5

Chapter III. The $G(F/Q)$ - Submodule $sgn(U)$ of the Group Ring $GF(2)[G(F/Q)]$ as an Ideal in the Ring $GF(2)[x]/\langle x^p+1\rangle$ 18

Chapter IV. Application of the Reciprocity Theorem of Class Field Theory 41

Chapter V. The Case when (2) is a Prime in F. 55

Appendix I - Tables 69

Appendix II - Polynomial Calculations 75

Index of Notation 77

References 79

Chapter I

Introduction

This thesis is a study of the distribution of the signs of the conjugates of the cyclotomic units[1] in the maximal real subfield of the qth cyclotomic field[2], q a prime. My interest in this subject arose from a problem considered by O.Taussky [13]. The idea of studying the distribution of the signs of the conjugates of the cyclotomic units for the problem of Taussky is due to E. C. Dade.

In Chapter II we introduce some preliminary material and then proceed to associate with the $p = (q-1)/2$ cyclotomic units a $p \times p$ matrix whose entries lie in the Galois field of two elements, $GF(2)$. This matrix is called the matrix of cyclotomic signatures. A similar association is found in Hasse [8], p. 27. The rank of the matrix of cyclotomic signatures determines the distribution of the signs of the conjugates of the cyclotomic units. It is shown that if the rank of the matrix of cyclotomic signatures is p, i.e. the matrix is non-singular, then every unit in the maximal real subfield F of the qth cyclotomic field which is totally positive is the norm of a unit in the qth cyclotomic field[3]. This fact gives a criterion needed in Taussky [13]. We then associate with the matrix of cyclotomic signatures a submodule of the group ring of the Galois group $G(F/Q)$ over $GF(2)$ in such a way that

---

1 The units defined in this thesis are not identical to the "Kreiseinheiten" in Hilbert [9] but generate the same group and hence the same sign distribution.

2 The field of qth roots of unity over the rationals.

3 It can also be shown that if the matrix of cyclotomic signatures is non-singular, then the class number of F is odd (see Hasse [8], p. 27).

the GF(2)-dimension of the submodule equals the rank of the matrix of cyclotomic signatures (Theorem 2.6). Also it is shown that this submodule is a $G(F/Q)$-submodule. We conclude Chapter II by exhibiting a simple procedure for calculating the matrix of cyclotomic signatures.

In Chapter III we use the fact that $G(F/Q)$ is cyclic of order p to obtain a GF(2)-module isomorphism of the group ring of $G(F/Q)$ over GF(2) and the GF(2)-module $GF(2)[x]/\langle x^p+1\rangle$, x indeterminate. Then there exists an $H_q(x) \in GF(2)[x]$ such that the matrix of cyclotomic signatures is associated to the ideal $\langle H_q(\tilde{x})\rangle$, $\tilde{x} = x + \langle x^p+1\rangle$, and such that the rank of the matrix equals the GF(2) - dimension of the ideal. We may assume that $H_q(x)$ divides x^p+1. Then the ideal structure of the ring $GF(2)[x]/\langle x^p+1\rangle$ is studied. Finally we obtain an expression (Theorem 3.4) for the GF(2)-dimension of any ideal in $GF(2)[x]/\langle x^p+1\rangle$. This expression is then used to prove that if p is a prime and if 2 is a primitive root mod p, then the matrix of cyclotomic signatures is non-singular (Theorem 3.5). Chapter III is concluded by determining an explicit means for calculating $H_q(x)$ and hence the ideal corresponding to the matrix of cyclotomic signatures. It follows from other results in Chapter III that the rank of the matrix of cyclotomic signatures equals p-degree $H_q(x)$.

Whereas the results in Chapters II and III are obtained by rather elementary methods, Chapter IV lays the groundwork for the use of deeper results. I am particularly indebted to E. C. Dade for the ideas found in this chapter. The first part of Chapter IV is devoted to introducing the preliminary material necessary for the statement of the reciprocity theorem of class field theory (Theorem 4.1). Then the basic idea is to consider the abelian extension E of F which is given by adjoining to F the square roots of the cyclotomic units, and then relate the corresponding reciprocity maps $\varphi_{\mathfrak{p}}$ for infinite primes $\mathfrak{p}$ in F to the signs of conjugates (Lemma 4.5). Let U denote the group generated by the cyclotomic units and let T be the group of all totally positive units in F. We have from Corollary 2.6.1 of Chapter II that the number of even invariants of the elementary abelian quotient group $U/U \cap T$ equals the rank of the matrix of cyclotomic signatures. It is shown that the quotient group $U/U \cap T$ is isomorphic to the product of the decomposition groups for E/F at all of the infinite primes in F (Theorem 4.2). Hence the number of even invariants of the latter group equals the rank of the matrix of cyclotomic signatures. Then the ultimate object of this chapter is attained. The product formula of the reciprocity theorem is used to shift the various criteria from infinite primes to primes in F which lie above (2). We obtain the result that every totally positive element in U is a square in U, i.e. $U \cap T = U^2$, if and only if the homomorphism $\Phi: U/U^2 \to G(E/F)$ defined by $\Phi(\mu U^2) = \prod_{\mathfrak{p} | (2)} \varphi_{\mathfrak{p}}(\mu)$ is a monomorphism. Finally a property of reciprocity maps is used to reduce the calculation of reciprocity maps for E/F to the calculation of the Hilbert symbol in F (Corollary 4.4.1).

In Chapter V we assume that (2) is a prime in F. This assumption simplifies the criteria from Chapter IV. Having reduced the criteria to statements about the Hilbert symbol at (2) on F we are led to the study of binary quadratic forms on $F_{(2)}$, the completion of F at (2). The first part of Chapter V is devoted to preliminary results on quadratic forms. In particular, in the case of p odd, explicit representatives for the quotient group of 2-adic units in $F_{(2)}$ with respect to the subgroup of their squares are determined. Then several calculation lemmas are proved. These results are applied to the case $q = 7$ and are used to compute the coset representatives for the cyclotomic units. This example then motivates the main results of the chapter. Assume that p is odd. Every unit in U which is a 2-adic square in $F_{(2)}$ is in U^2 if and only if the quotient group of 2-adic units in $F_{(2)}$ with respect to the subgroup of squares equals the direct sum of the subgroups generated by the cosets containing the cyclotomic units and the unit 3 (Theorem 5.7). It is shown that the homomorphism $\Phi : U/U^2 \rightarrow G(E/F)$ is a monomorphism if and only if every unit in U which is a square in $F_{(2)}$ is in U^2, i.e. $U \cap F^2_{(2)} = U^2$ (Theorem 5.8). These theorems have several consequences (Corollary 5.8.1), among them the result that in the case of p odd, the matrix of cyclotomic signatures is non-singular if and only if every unit in U which is a 2-adic square in $F_{(2)}$ is in fact in U^2.

The rank of the matrix of cyclotomic signatures was computed on an IBM 7094 for all primes q, $3 \leq q \leq 929$ using the method given at the end of Chapter II. The results of this computation are found in tables in Appendix I. It happens that for these q $(3 \leq q \leq 929)$ whenever $p = (q-1)/2$ is a prime then the matrix of cyclotomic signatures is non-singular. Using results in Chapter III the cases for $929 \leq q \leq 4703$, q prime and $p = (q-1)/2$ prime were computed and in each case the matrix of cyclotomic signatures was non-singular. The calculations for these cases are explained in Appendix II. We have the following

<u>Conjecture</u>: If q is a prime and $p = (q-1)/2$ is a prime then the matrix of cyclotomic signatures is non-singular.

Chapter II

The Matrix of Cyclotomic Signatures

The object of this chapter is to introduce preliminary material, define the matrix of cyclotomic signatures and prove a theorem which exemplifies its significance. We conclude the chapter by giving a procedure for obtaining the matrix of cyclotomic signatures.

Throughout let q denote a rational odd prime, let $p = (q-1)/2$ and let ζ denote a primitive qth root of unity. We consider the field $Q(\zeta)$ where Q denotes the field of rational numbers. The field $Q(\zeta)$ is called the qth cyclotomic field. We have the following theorem.

Theorem 2.1. The qth cyclotomic field $Q(\zeta)$ is a Galois extension of Q with a Galois group $G(Q(\zeta)/Q)$ which is cyclic of order $q-1$.

Proof: See Weiss [15], p. 255.

By Theorem 2.1 the group $G(Q(\zeta)/Q)$ is isomorphic to the multiplicative group $GF(q)^*$ of non-zero residues mod q. Therefore $G(Q(\zeta)/Q)$ contains an element σ of order 2, namely the element whose image in $GF(q)$ is -1. The element σ is unique, for if k is a rational integer and $k^2 \equiv 1 \bmod q$, then $k \equiv 1$ or $k \equiv -1 \bmod q$. Therefore σ is the automorphism defined by complex conjugation. We shall denote the complex conjugate of a number α by $\overline{\alpha}$. If F is the fixed field of the subgroup generated by σ, then by Galois theory F is a cyclic extension of Q of degree $p = (q-1)/2$ which is contained in $Q(\zeta)$ and which has a Galois group $G(F/Q)$ isomorphic to the quotient group $G(Q(\zeta)/Q)/\langle\sigma\rangle$. Furthermore F is a real field; it is the maximal real subfield of $Q(\zeta)$, i.e. $F = Q(\zeta + \overline{\zeta})$. The automorphisms of F over Q are obtained by restricting the automorphisms of $Q(\zeta)$ over Q to F, for under this restriction the two elements of any coset of the subgroup $\langle\sigma\rangle$ in $G(Q(\zeta)/Q)$ may be identified. In the following it will be assumed that automorphisms of F over Q have been obtained in this way.

Corollary 2.1.1. The maximal real subfield $F = Q(\zeta + \zeta^{-1})$ of the qth cyclotomic field is a Galois extension of Q which has a Galois group $G(F/Q)$ which is cyclic of order $p = (q-1)/2$.

Let Z denote the ring of rational integers.

Theorem 2.2. The numbers $1, \zeta, \ldots, \zeta^{q-2}$ form an integral basis, a Z-basis, for the ring of algebraic integers in $Q(\zeta)$.

Proof: See Weyl [16], p. 81.

Corollary 2.2.1. The real numbers $\zeta + \zeta^{-1}, \ldots, \zeta^{p} + \zeta^{-p}$, $p = (q-1)/2$, form an integral basis for the ring of algebraic integers in $F = Q(\zeta + \zeta^{-1})$.

Proof: Theorem 2.2 implies that $\zeta, \ldots, \zeta^{q-1}$ form an integral basis for the ring of algebraic integers in $Q(\zeta)$ because ζ is a unit in this ring. If α is an algebraic integer in $Q(\zeta + \zeta^{-1})$, it is one in $Q(\zeta)$. Therefore α has a unique representation

$$\alpha = a_1 \zeta + a_2 \zeta^2 + \cdots + a_{q-1} \zeta^{q-1}, \quad a_i \in Z.$$

Since α is real, $\alpha = \bar{\alpha}$. Hence

$$a_1 \zeta + a_2 \zeta^2 + \cdots + a_{q-1} \zeta^{q-1} = a_1 \zeta^{-1} + a_2 \zeta^{-2} + \cdots + a_{q-1} \zeta.$$

Since $\zeta, \zeta^2, \ldots, \zeta^{q-1}$ form an independent field basis for $Q(\zeta)$ we conclude that

$$a_1 = a_{q-1}, \; a_2 = a_{q-2}, \; \ldots, \; a_p = a_{q-p}.$$

Hence

$$\alpha = a_1(\zeta + \zeta^{-1}) + a_2(\zeta^2 + \zeta^{-2}) + \cdots + a_p(\zeta^p + \zeta^{-p}).$$

Therefore we have a basis for the ring of algebraic integers in $Q(\zeta + \zeta^{-1})$. We now describe some units in this ring. We need the following

Lemma 2.1. If k is a rational integer such that $k \not\equiv 0 \bmod q$, then

$$(1 - \zeta^k) / (1-\zeta)$$

is a unit in $Q(\zeta)$.

Proof: See Weiss [15], p. 267.

It is clear that ζ^k is a unit in $Q(\zeta)$ for any $k \in Z$. Let k be a rational integer such that $k \not\equiv 0 \bmod q$. Then $2k \not\equiv 0 \bmod q$. Hence

$$(\zeta^{2k} - 1) / (\zeta - 1)$$

is a unit in $Q(\zeta)$.

Also

$$\frac{\zeta^2 - 1}{\zeta - 1}$$

is a unit in $Q(\zeta)$.

Therefore

$$\frac{\zeta^{2k}-1}{\zeta-1} \cdot \frac{\zeta-1}{\zeta^2-1} \cdot \frac{\zeta^{-k}}{\zeta^{-1}} = \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}}$$

is a unit in $Q(\zeta)$ for every $k \in Z$ for which $k \not\equiv 0 \bmod q$. But these units are real, therefore they are units in $Q(\zeta + \zeta^{-1})$. The real units

$$\upsilon_1 = -1$$

$$\upsilon_k = \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \qquad k = 2, 3, \ldots, p$$

are called the qth <u>cyclotomic units</u>.

Let σ be an element of $G(F/Q)$, the Galois group of $F=Q(\zeta+\zeta^{-1})$ over Q, and let α be an element of F^*. Let $|\cdot|$ denote ordinary absolute value. Then we call

$$\operatorname{sign}_\sigma(\alpha) = \frac{\sigma(\alpha)}{|\sigma(\alpha)|}$$

the <u>σ-sign</u> of α. If $\{\sigma_1, \sigma_2, \ldots, \sigma_p\}$ is a fixed but arbitrary ordering of $G(F/Q)$ then we call the p-tuple

$$(\operatorname{sign}_{\sigma_1}(\alpha), \operatorname{sign}_{\sigma_2}(\alpha), \ldots, \operatorname{sign}_{\sigma_p}(\alpha))$$

the <u>$G(F/Q)$-sign</u> of α. And if ρ is the map from $\{1, -1\}$ to $GF(2)$ defined by $\rho(-1) = 1$, $\rho(1) = 0$, then we call

$$\operatorname{sgn}_\sigma(\alpha) = \rho \operatorname{sign}_\sigma(\alpha)$$

the <u>σ-signature</u> of α. We call the p-tuple

$$(\rho \operatorname{sign}_{\sigma_1}(\alpha), \ldots, \rho \operatorname{sign}_{\sigma_p}(\alpha))$$

the <u>$G(F/Q)$ - signature</u> of α. The sign and signature functions defined above exhibit the sign behavior of the conjugates of α. In particular the $p \times p$ matrix

$$M_q = (m_{ij})$$

where

$$m_{ij} = \operatorname{sgn}_{\sigma_j}(\upsilon_i), \; i,j = 1, \ldots, p$$

exhibits the sign structure of the cyclotomic units. We call M_q the <u>matrix</u> of <u>cyclotomic signatures</u>.

Before we describe the significance of the matrix M_q we shall need to know more about the units in $Q(\zeta+\zeta^{-1})$. Denote the units in $Q(\zeta+\zeta^{-1})$ by V. As a result of the Dirichlet Unit Theorem (Weiss [15], p. 207) we have

Theorem 2.3. The group V of units in the field $F = Q(\zeta+\zeta^{-1})$ is the direct sum of the subgroup generated by -1 and p-1 infinite cyclic subgroups.

If we apply the Dirichlet Unit Theorem to $Q(\zeta)$, we find that the same result holds if -1 is replaced by ζ. We also have

Theorem 2.4. If α is a unit in $Q(\zeta)$ then there exists a rational integer k and a real unit β in $Q(\zeta+\zeta^{-1})$ such that

$$\alpha = \zeta^k\beta .$$

Proof: See Borevich and Shafarevich [5], p. 158.

Let U denote the subgroup of V generated by the cyclotomic units $\upsilon_1, \upsilon_2, \ldots, \upsilon_p$.

Theorem 2.5. The subgroup U of V is a subgroup of finite index.

Proof: See Borevich and Shafarevich [5], p. 362 or Bass [3]. Recall that we are assuming that q is a prime.

An element $\mu \in V$ is said to be totally positive if and only if for all automorphisms $\sigma \in G(F/Q)$, $\sigma(\mu) > 0$. An element $\mu \in V$ is said to be a norm if and only if there exists a unit ν in $Q(\zeta)$ such that $\mu = \nu\bar{\nu}$. An element μ in V is said to be a square if and only if there exists a unit ν in V such that $\mu = (\nu)^2$. Let

$$T = \{\mu \mid \mu \in V,\ \mu \text{ is totally positive}\}$$

$$N = \{\mu \mid \mu \in V,\ \mu \text{ is a norm}\}$$

$$S = \{\mu \mid \mu \in V,\ \mu \text{ is a square}\} .$$

Lemma 2.2. The sets T, N and S are multiplicative subgroups of V and $S \subseteq N \subseteq T$.

Proof: It is clear that T, N and S are subgroups of V. Moreover it is clear that $S \subseteq N$. If $\mu \in N$ then $\mu = \nu\bar{\nu}$. If $\sigma \in G(Q(\zeta)/Q)$ then $\sigma\mu = (\sigma\nu)\,(\overline{\sigma\nu}) > 0$. Therefore $\mu \in T$. Hence $N \subseteq T$.

Lemma 2.3. $S = N$.

Proof: We need only show that $N \subseteq S$. If $\mu \in N$, then there exists a unit ν in $Q(\zeta)$ such that $\mu = \nu\bar{\nu}$. By Theorem 2.4, there exist a rational integer k and a unit θ in $Q(\zeta + \zeta^{-1})$ such that $\nu = \zeta^k\theta$. Hence $\mu = \zeta^k\theta \cdot \zeta^{-k}\theta = \theta^2$. Hence $\mu \in S$. Therefore $N \subseteq S$.

Naturally we might ask if it ever happens that $S = N = T$. We shall find a condition on the matrix M_q which implies $S = N = T$.

Consider the group ring $GF(2)\,[G(F/Q)]$ of the Galois group of F over Q over the Galois field of two elements. Let sgn be the mapping from the units V to $GF(2)[G(F/Q)]$ defined by

$$\operatorname{sgn}(\mu) = \sum_{\sigma \in G(F/Q)} \operatorname{sgn}_\sigma(\mu)\cdot\sigma \qquad \mu \in V.$$

Lemma 2.4. The mapping $\operatorname{sgn}: V \to GF(2)\,[G(F/Q)]$ is a homomorphism of groups and $\ker \operatorname{sgn} = T$.

Proof: We need only prove for each $\sigma \in G(F/Q)$ that the mapping $\operatorname{sgn}_\sigma : V \to GF(2)$ is a homomorphism. But $\operatorname{sgn}_\sigma$ is a homomorphism of groups iff $\operatorname{sign}_\sigma : V \to \{+1, -1\}$ is a homomorphism. We have

$$\operatorname{sign}_\sigma(\mu_1\mu_2) = \frac{\sigma(\mu_1\mu_2)}{|\sigma(\mu_1\mu_2)|} = \frac{\sigma(\mu_1)\,\sigma(\mu_2)}{|\sigma(\mu_1)|\cdot|\sigma(\mu_2)|} = \operatorname{sign}_\sigma(\mu_1)\operatorname{sign}_\sigma(\mu_2).$$

Also $\mu \in T$ iff $\operatorname{sign}_\sigma(\mu) = 1$ for all $\sigma \in G(F/Q)$. Hence $\mu \in T$ iff $\operatorname{sgn}_\sigma(\mu) = 0$ for all $\sigma \in G(F/Q)$. Therefore $\mu \in T$ iff $\operatorname{sgn}(\mu) = 0$, iff $\mu \in \ker \operatorname{sgn}$.

Theorem 2.6. The dimension of sgn(U) as a vector space over GF(2) equals the rank of the matrix M_q of cyclotomic signatures.

Proof: Let $\{\sigma_1, \ldots, \sigma_p\}$ be an ordering of G(F/Q). The matrix M_q has rank r over GF(2) iff it has exactly r independent rows, i.e. iff r of the p-tuples

$$(\mathrm{sgn}_{\sigma_1}(\upsilon_i), \ldots, \mathrm{sgn}_{\sigma_p}(\upsilon_i)), i = 1, \ldots, p$$

are linearly independent over GF(2). Since $\sigma_1, \ldots, \sigma_p$ form a free GF(2)-basis for GF(2) [G(F/Q)], exactly r of the above p-tuples are linearly independent iff r of the elements

$$\mathrm{sgn}_{\sigma_1}(\upsilon_i) \cdot \sigma_1 + \cdots + \mathrm{sgn}_{\sigma_p}(\upsilon_i) \cdot \sigma_p \ , \quad i = 1, \ldots, p$$

are linearly independent over GF(2). Therefore the rank of the matrix M_q is r iff the elements $\mathrm{sgn}(\upsilon_i)$, $i = 1, \ldots, p$ generate a vector space over GF(2) of dimension r.

Corollary 2.6.1. The number of even invariants of the group $U/U \cap T$ equals the rank of the matrix of cyclotomic signatures.

Proof: By Lemma 2.4, we have the following isomorphism of vector spaces over GF(2).

$$U/U \cap T \cong \mathrm{sgn}(U)$$

Hence by Theorem 2.6, the GF(2)-dimension of $U/U \cap T$, i.e. the number of even invariants, equals the rank of the matrix of cyclotomic signatures.

Theorem 2.7. The homomorphism $\mathrm{sgn}: V \to GF(2)[G(F/Q)]$ is an epimorphism iff $S = N = T$.

Proof: Since $S = N \subseteq T$, $S = N = T$ iff $[V:S] = [V:T]$, i.e. $[V:T] = 2^p$ by Theorem 2.3. Assume that $sgn: V \to GF(2)[G(F/Q)]$ is onto. Then sgn induces an isomorphism of groups,

$$V/T = V/\ker sgn \cong GF(2)[G(F/Q)] .$$

But the order of the additive group $GF(2)[G(F/Q)]$ is 2^p because $G(F/Q)$ has order p. Therefore $[V:T] = 2^p$, and hence $S = N = T$. Conversely, assume $[V:T] = 2^p$. By Lemma 2.4 sgn induces a monomorphism of groups,

$$V/T \to GF(2)[G(F/Q)] .$$

Hence the image of V/T under this monomorphism is a subgroup of the additive group $GF(2)[G(F/Q)]$ which has order 2^p, that is, $GF(2)[G(F/Q)]$ itself. Therefore $sgn: V \to GF(2)[G(F/Q)]$ is onto.

Corollary 2.7.1. Let W be a subgroup of V. If $sgn|W: W \to GF(2)[G(F/Q)]$ is an epimorphism, then $S = N = T$.

Proof: If $sgn|W: W \to GF(2)[G(F/Q)]$ is onto, then $sgn: V \to GF(2)[G(F/Q)]$ is onto, hence $S = N = T$ by Theorem 2.7.

We can apply Corollary 2.7.1 to the subgroup U generated by the cyclotomic units. Moreover we have

Corollary 2.7.2. If the matrix M_q of cyclotomic signatures is non-singular over $GF(2)$, then $S = N = T$.

Proof: If M_q is non-singular, then the $GF(2)$-dimension of $sgn(U)$ is p by Theorem 2.6. Hence $sgn|U$ is an epimorphism. Hence $S = N = T$ by Corollary 2.7.1.

Given the generators of any subgroup of finite index in the group of units V we could define a matrix of signatures and prove a result analogous to the above corollary. The advantage of using the cyclotomic units is that the associated matrix of signatures can be calculated easily. Before we show how the matrix of cyclotomic signatures is calculated we prove some results which are exploited in the next chapter.

Theorem 2.8. Let W be a subgroup of the group of units V. If for all $\sigma \in G(F/Q)$, $\sigma | W$ defines a multiplicative automorphism on W, then $\mathrm{sgn}(W)$ is a $G(F/Q)$ - submodule of the group ring $GF(2)[G(F/Q)]$.

Proof: We must show for all $\sigma \in G(F/Q)$ and $w \in \mathrm{sgn}(W)$ that $\sigma \cdot w$ is in $\mathrm{sgn}(W)$, where the multiplication is multiplication in $GF(2)[G(F/Q)]$. Let $w = \mathrm{sgn}(\omega)$, $\omega \in W$, and let $\sigma \in G(F/Q)$. We have,

$$\sigma \cdot w = \sigma \cdot \mathrm{sgn}(\omega) = \sigma \sum_{\tau \in G(F/Q)} \mathrm{sgn}_{\tau}(\omega) \cdot \tau$$

$$= \sum_{\tau \in G(F/Q)} \mathrm{sgn}_{\tau}(\omega)\, \sigma\tau = \sum_{\tau \in G(F/Q)} \mathrm{sgn}_{\sigma^{-1}\tau}(\omega)\, \tau$$

$$= \sum_{\tau \in G(F/Q)} \mathrm{sgn}_{\tau\sigma^{-1}}(\omega)\, \tau = \sum_{\tau \in G(F/Q)} \mathrm{sgn}_{\tau}\left(\sigma^{-1}(\omega)\right) \cdot \tau = \mathrm{sgn}\left(\sigma^{-1}(\omega)\right).$$

Since $\sigma | W$ is an automorphism of W, $\sigma^{-1}(\omega) \in W$. Hence $\sigma \cdot w \in \mathrm{sgn}(W)$.

Corollary 2.8.1. Let V be the group of units in F. Then $\mathrm{sgn}(V)$ is a $G(F/Q)$ - submodule of $GF(2)[G(F/Q)]$.

Proof: If $\sigma \in G(F/Q)$ then $\sigma | V$ is an automorphism of V. Apply Theorem 2.8.

Corollary 2.8.2. Let U be the subgroup of the group V which is generated by the cyclotomic units. Then $\mathrm{sgn}(U)$ is a $G(F/Q)$ - submodule of the group ring $GF(2)[G(F/Q)]$.

Proof: By Theorem 2.8 it is sufficient to show that $\sigma(U) \subseteq U$ for all

$\sigma \in G(F/Q)$. Therefore it is sufficient to show that $\sigma(\upsilon_i) \in U$ for all $\sigma \in G(F/Q)$ and for all $i = 1, \dots, p$. Assume $\sigma \in G(Q(\zeta)/Q)$. Then there exists $j \in Z, 0 \leqslant j \leqslant q-1$ such that $\sigma(\zeta) = \zeta^j$. We have

$$\sigma(\upsilon_1) = \sigma(-1) = -1 .$$

If $2 \leqslant i \leqslant p$, then

$$\sigma(\upsilon_i) = \sigma\left(\frac{\zeta^i - \zeta^{-i}}{\zeta - \zeta^{-1}}\right) = \frac{\zeta^{ij} - \zeta^{-ij}}{\zeta^j - \zeta^{-j}} .$$

There exist (uniquely) $k \in Z$, $0 \leqslant k \leqslant p$ and $\delta = +1$ or -1 such that $k \equiv \delta i j \bmod q$. Then

$$\sigma(\upsilon_i) = \delta \frac{\zeta^{\delta ij} - \zeta^{-\delta ij}}{\zeta^j - \zeta^{-j}} = \delta \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \cdot \frac{\zeta - \zeta^{-1}}{\zeta^j - \zeta^{-j}} = \delta \upsilon_k \upsilon_j^{-1} .$$

Therefore $\sigma(\upsilon_i) \in U$ for all $\sigma \in G(F/Q)$ and all $i = 1, \dots, p$.

We now show how to calculate M_q. We are interested in the rank of M_q. Therefore we are not interested in the ordering of the rows or columns of M_q. Hence we may choose any convenient ordering of the Galois group $G(F/Q)$. The elements of $G(F/Q)$ can be chosen as coset representatives of the cosets of the subgroup generated by complex conjugation in $G(Q(\zeta)/Q)$. Each element of $G(Q(\zeta)/Q)$ is determined by its action on ζ and two distinct elements are in the same coset if their actions on ζ are complex conjugates. Therefore we can write $G(F/Q)$ as

$$\{\sigma_1, \sigma_2, \dots, \sigma_p\}$$

where $\sigma_j(\zeta) = \zeta^j$, $j = 1, \dots, p$. We must choose a particular primitive qth root of unity. Hence for the purpose of calculation let

$$\zeta = e^{2\pi\sqrt{-1}/q} = \cos(2\pi/q) + \sqrt{-1}\,\sin(2\pi/q) .$$

Then for $k = 2, \ldots, p$,

$$\upsilon_k = \frac{e^{2\pi\sqrt{-1}\,k/q} - e^{-2\pi\sqrt{-1}\,k/q}}{e^{2\pi\sqrt{-1}} - e^{-2\pi\sqrt{-1}}} = \frac{\sin(2k\pi/q)}{\sin(2\pi/q)} .$$

Hence for $k = 2, \ldots, p$ and $j = 1, \ldots, p$ we have

$$\sigma_j(\upsilon_k) = \frac{e^{2\pi\sqrt{-1}\,jk/q} - e^{-2\pi\sqrt{-1}\,jk/q}}{e^{2\pi\sqrt{-1}\,j/q} - e^{-2\pi\sqrt{-1}\,j/q}} = \frac{\sin(2\pi jk/q)}{\sin(2\pi j/q)} .$$

We define a function $[\![\cdot]\!] : Z \to \{0, 1, \ldots, q-1\}$ by

$$[\![k]\!] = j \quad \text{for} \quad k \in Z,\ j \in \{0, 1, \ldots, q-1\}$$

if and only if

$$k \equiv j \bmod q.$$

That is, $[\![k]\!]$ is the least positive residue of $k \bmod q$. Let n be an arbitrary integer such that $n \not\equiv 0 \bmod q$. Then the sign of $\sin(2\pi n/q)$ is determined by the least positive residue of $n \bmod q$. Namely

$$\frac{\sin(2\pi n/q)}{|\sin(2\pi n/q)|} = \begin{cases} +1 & \text{if } 0 < [\![n]\!] \leq p \\ -1 & \text{if } p < [\![n]\!] \leq q-1 \end{cases} .$$

Therefore for $k = 2, \ldots, p$ and $j = 1, \ldots, p$

$$\operatorname{sign}_{\sigma_j}(\upsilon_k) = \begin{cases} +1 & \text{if } 0 < [\![jk]\!] \leq p \\ -1 & \text{if } p < [\![jk]\!] \leq q-1 \end{cases} .$$

Hence for $k = 2, \ldots, p$ and $j = 1, \ldots, p$

$$\operatorname{sgn}_{\sigma_j}(\upsilon_k) = \begin{cases} 0 & \text{if } 0 < [\![jk]\!] \leq p \\ 1 & \text{if } p < [\![jk]\!] \leq q-1 \end{cases} .$$

Also it is clear that $\operatorname{sgn}_{\sigma_j}(\upsilon_1) = 1$ for $j = 1, \ldots, p$. The matrix of cyclotomicsignatures M_q is given by

$$M_q = (m_{kj}) \text{ where } m_{kj} = \operatorname{sgn}_{\sigma_j}(\upsilon_k), \; j, k = 1, \ldots, p.$$

Hence

$$m_{1j} = 1 \text{ for } j = 1, \ldots, p$$

$$m_{kj} = \begin{cases} 0 & \text{if } 0 < [\![jk]\!] \leq p \\ 1 & \text{if } p < [\![jk]\!] \leq q-1 \end{cases} \quad \text{for } \begin{array}{l} k = 2, \ldots, p \\ j = 1, \ldots, p \end{array} .$$

We are interested in the rank of M_q. If we add the first row of M_q to each successive row then we obtain a matrix M_q' which has the same rank as M_q. The matrix M_q' can be expressed easily.

$$M_q' = (m_{ij}') \text{ where}$$

$$m_{ij}' = \begin{cases} 1 & \text{if } [\![ij]\!] \leq p \\ 0 & \text{if } [\![ij]\!] > p \end{cases} .$$

The computation of M_7 and M_7' follows.

Consider the following multiplication table of least positive residues mod 7.

	1	2	3
1	1	2	3
2	2	4	6
3	3	6	2

Using the definition of M_7 we have

$$M_7 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and

$$M_7' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} .$$

Clearly M_7 and M_7' have rank 3 over GF(2). The matrix M_q' and its rank over GF(2) were computed for all primes q, $3 \leq q \leq 929$. The tables of rank appear in Appendix I.

Chapter III

The $G(F/Q)$ Submodule $\mathrm{sgn}(U)$ of the Group Ring $GF(2)[G(F/Q)]$ as an Ideal in the Ring $GF(2)[x]/\langle x^p+1\rangle$.

By Corollary 2.8.2 of Chapter II, the subring $\mathrm{sgn}(U)$ of $GF(2)[G(F/Q)]$ is a $G(F/Q)$-submodule. The group $G(F/Q)$ is a cyclic group of order p. Let σ be a generator of $G(F/Q)$, so that $G(F/Q) = \langle\sigma\rangle$. Let x be an indeterminate. The $GF(2)$-homomorphism from the polynomial ring $GF(2)[x]$ to $GF(2)[G(F/Q)]$ which is induced by $x \to \sigma$ is an epimorphism of $GF(2)$-modules. The kernel of this epimorphism is the ideal $\langle x^p+1\rangle$ in $GF(2)[x]$. We therefore have the following isomorphism of $GF(2)$-modules.

$$GF(2)[x] / \langle x^p+1\rangle \cong GF(2)[G(F/Q)] .$$

Furthermore under this isomorphism ideals in $GF(2)[x]/\langle x^p+1\rangle$ correspond uniquely to $G(F/Q)$-submodules in $GF(2)[G(F/Q)]$. By Theorem 2.6 of Chapter II we are interested in the $GF(2)$-dimension of the $G(F/Q)$-submodule $\mathrm{sgn}(U)$. In this chapter we first study the ideal structure of $GF(2)[x]/\langle x^p+1\rangle$. Then we find an expression for the ideal in $GF(2)[x]/\langle x^p+1\rangle$ which corresponds to $\mathrm{sgn}(U)$. Also we find an expression for its $GF(2)$-dimension.

It is not difficult to theoretically determine the ideal structure of the ring $GF(2)[x]/\langle x^p+1\rangle$. However, for specific cases it is difficult to actually obtain the structure by calculation. We are interested in both aspects. We study the former aspect first (see Jacobson [10], p. 9).

Let

$$x^p+1 = f_0(x)\, f_1(x) \cdots f_h(x)$$

be a complete factorization of $x^p + 1$ into relatively prime factors in $GF(2)[x]$, so that each factor is irreducible or a power of an irreducible polynomial in $GF(2)[x]$. For $i = 0, \ldots, h$ let

$$\hat{f}_i(x) = (x^p + 1)/f_i(x) .$$

Then

$$\text{g.c.d.}\ (\hat{f}_0(x), \ldots, \hat{f}_h(x)) = 1 \quad \text{in } GF(2)[x] .$$

Hence there exist polynomials $\ell_0(x), \ldots, \ell_h(x)$ in $GF(2)[x]$ such that

$$\ell_0(x)\hat{f}_0(x) + \cdots + \ell_h(x)\hat{f}_h(x) = 1.$$

For $i = 0, \ldots, h$, let

$$e_i(x) = \ell_i(x)\hat{f}_i(x).$$

Let

$$\tilde{x} = x + \langle x^p + 1 \rangle .$$

The mapping $k(x) \rightarrow k(\tilde{x})$ for any polynomial $k(x)$ defines the natural epimorphism from $GF(2)[x]$ to $GF(2)[x]/\langle x^p + 1 \rangle$. Also we can write

$$GF(2)[x]/\langle x^p + 1 \rangle = GF(2)[\tilde{x}] .$$

We have

<u>Lemma 3.1.</u> The ring $GF(2)[\tilde{x}]$ is equal to the direct sum of the ideals $\langle e_i(\tilde{x}) \rangle$, $i = 0, \ldots, h$. That is,

$$GF(2)[\tilde{x}] = \langle e_0(\tilde{x}) \rangle \oplus \cdots \oplus \langle e_h(\tilde{x}) \rangle .$$

Proof: We have $\quad e_0(x) + \cdots + e_h(x) = 1, \quad$ hence

$$e_0(\tilde{x}) + \cdots + e_h(\tilde{x}) = 1 .$$

Therefore if $k(\tilde{x}) \in GF(2)[\tilde{x}]$, then

$$k(\tilde{x}) = k(\tilde{x})\, e_0(\tilde{x}) + \cdots + k(\tilde{x})\, e_h(\tilde{x}) .$$

Hence

$$GF(2)[\tilde{x}] = \langle e_0(\tilde{x})\rangle + \cdots + \langle e_h(\tilde{x})\rangle .$$

If $i \neq j$, x^p+1 divides $e_i(x)\, e_j(x)$ over $GF(2)[x]$. Therefore

$$e_i(\tilde{x})\, e_j(\tilde{x}) = 0 \quad \text{if} \quad i \neq j.$$

Hence, if we multiply the relation $e_0(\tilde{x}) + \cdots + e_h(\tilde{x}) = 1$ by $e_i(\tilde{x})$, $0 \leqslant i \leqslant h$, we obtain

$$e_i(\tilde{x})\, e_i(\tilde{x}) = e_i(\tilde{x}) .$$

Summarizing, we can write

$$e_i(\tilde{x})\, e_j(\tilde{x}) = \delta_{ij}\, e_i(\tilde{x})$$

where δ_{ij} is the Kronecker delta. If

$$k_0(\tilde{x}) + \cdots + k_h(\tilde{x}) = 0$$

where $k_i(\tilde{x})$ is an element of $\langle e_i(\tilde{x}) \rangle$, then there exist elements $k_i'(\tilde{x})$ in $GF(2)[\tilde{x}]$ such that

$$k_i(\tilde{x}) = k_i'(\tilde{x})\, e_i(\tilde{x}).$$

Hence,

$$k_0'(\tilde{x})\, e_0(\tilde{x}) + \cdots + k_h'(\tilde{x})\, e_h(\tilde{x}) = 0.$$

Then multiplying by $e_i(\tilde{x})$ and using the above relations, we get that

$$k_i(\tilde{x}) = k_i'(\tilde{x})\, e_i(\tilde{x}) = 0.$$

Hence $\langle e_0(\tilde{x})\rangle + \cdots + \langle e_h(\tilde{x})\rangle$ is actually direct.

We see by the proof above that the elements $e_0(\tilde{x}), \ldots, e_h(\tilde{x})$ form a set of orthogonal idempotents for $GF(2)[\tilde{x}]$. We now classify the ideals $\langle e_i(\tilde{x})\rangle$ for $i = 0, \ldots, h$.

Lemma 3.2. Let i be an integer such that $0 \leqslant i \leqslant h$. Then the ideal $\langle e_i(\tilde{x})\rangle$ considered as a subring of $GF(2)[\tilde{x}]$ is isomorphic to the ring $GF(2)[x]/\langle f_i(x)\rangle$.

Proof: Consider the mapping $T_i: \langle e_i(\tilde{x})\rangle \rightarrow GF(2)[x]/\langle f_i(x)\rangle$ defined by

$$T_i(g(\tilde{x})\, e_i(\tilde{x})) = g(x) + \langle f_i(x)\rangle$$

where $g(x)$ is an element of $GF(2)[x]$. We show that T_i is an isomorphism. T_i is well-defined: Let $g(x)$, $g'(x) \in GF(2)[x]$. The relation

$$g(\tilde{x})\; e_i(\tilde{x}) = g'(\tilde{x})\; e_i(\tilde{x})$$

implies that $x^p + 1 \,\big|\, (g(x) - g'(x))\, e_i(x)$, hence $f_i(x) \,\big|\, (g(x) - g'(x))$, hence $g(x) - g'(x') \in \langle f_i(x)\rangle$. Therefore

$$g(x) + \langle f_i(x)\rangle = g'(x) + \langle f_i(x)\rangle\ .$$

T_i is a homomorphism:

$$T_i(g(\tilde{x})e_i(\tilde{x}) + g'(\tilde{x})e_i(\tilde{x})) = T_i((g(\tilde{x}) + g'(\tilde{x}))e_i(\tilde{x})) = (g(x) + g'(x)) + \langle f_i(x)\rangle$$

$$= g(x) + \langle f_i(x)\rangle + g'(x) + \langle f_i(x)\rangle = T_i(g(\tilde{x})\, e_i(\tilde{x})) + T_i(g'(\tilde{x})\, e_i(\tilde{x})).$$

T_i is onto: If $g(x) + \langle f_i(x)\rangle \in GF(2)[x]/\langle f_i(x)\rangle$, then

$$T_i(g(\tilde{x})\, e_i(\tilde{x})) = g(x) + \langle f_i(x)\rangle.$$

T_i is one-to-one: If $T_i(g(\tilde{x})\, e_i(\tilde{x})) = 0$, then $f_i(x) \,|\, g(x)$. Since

$f_i(x)\,\hat{f}_i(x) = x^p + 1$, we then have that $x^p + 1 \mid g(x)\,e_i(x)$, i.e. $g(\tilde{x})e_i(\tilde{x}) = 0$. Therefore T_i is an isomorphism.

Combining these lemmas we have

Theorem 3.1.

$$GF(2)[x]/\langle x^p + 1\rangle \cong GF(2)[x]/\langle f_0(x)\rangle \oplus \cdots \oplus GF(2)[x]/\langle f_h(x)\rangle .$$

Proof: Lemma 3.1 and Lemma 3.2.

The projection from $GF(2)[x]/\langle x^p + 1\rangle$ to the summand $GF(2)[x]/\langle f_i(x)\rangle$ is given by

$$g(x) + \langle x^p + 1\rangle \rightarrow g(x) + \langle f_i(x)\rangle$$

where $g(x)$ is in $GF(2)[x]$. Hence the ideal structure of $GF(2)[x]/\langle x^p + 1\rangle$ is determined by the ideal structure of $GF(2)[x]/\langle f_i(x)\rangle$ where $f_i(x)$ is irreducible or a power of an irreducible element in $GF(2)[x]$. The ideal structure of such a ring is easily determined by a general result.

Lemma 3.3. Let $k(x) \in GF(2)[x]$. Let $x_k = x + \langle k(x)\rangle$. If $\langle g(x_k)\rangle$ is a non-zero ideal of the ring $GF(2)[x_k] = GF(2)[x]/\langle k(x)\rangle$, then there is a unique factor $g'(x)$ of $k(x)$ such that

$$\langle g(x_k)\rangle = \langle g'(x_k)\rangle .$$

Proof: We prove the existence. Let $g(x)$ be any pre-image in $GF(2)[x]$ of $g(x_k)$. Let $g'(x) = \text{g.c.d.}\,(k(x), g(x))$ over $GF(2)[x]$. There exist $m(x)$, $n(x)$ in $GF(2)[x]$ such that $m(x)\,g(x) + n(x)\,k(x) = g'(x)$. Hence

$$g'(x_k) = m(x_k)\,g(x_k).$$

Therefore

$$\langle g'(x_k)\rangle \subseteq \langle g(x_k)\rangle .$$

However, $g'(x) \mid g(x)$, and therefore

$$\langle g'(x_k)\rangle \supseteq \langle g(x_k)\rangle .$$

Hence

$$\langle g'(x_k)\rangle = \langle g(x_k)\rangle .$$

Now we prove uniqueness. Suppose there exist two factors $g'(x)$, $g''(x)$ of $k(x)$ such that

$$\langle g'(x_k)\rangle = \langle g''(x_k)\rangle = \langle g(x_k)\rangle .$$

Then there exists $m(x)$ in $GF(2)[x]$ such that

$$g''(x_k) = m(x_k)g'(x_k) .$$

Hence

$$g''(x) + \langle k(x)\rangle = m(x)g'(x) + \langle k(x)\rangle .$$

There exists $n(x)$ in $GF(2)[x]$ such that

$$g''(x) = m(x)g'(x) + n(x)k(x) .$$

By assumption $g'(x) \mid k(x)$. Hence $g'(x) \mid g''(x)$. In a similar way we can show that $g''(x) \mid g'(x)$. Hence $g'(x) = g''(x)$.

Let $\phi(x)$ be an irreducible element in $GF(2)[x]$, let n be a positive integer and let $x_\phi = x + \langle \phi^n(x)\rangle$. By the above lemma the ideals of $GF(2)[x_\phi] = GF(2)[x]/\langle \phi^n(x)\rangle$ are precisely

$$\langle 0\rangle \subseteq \langle \phi^{n-1}(x_\phi)\rangle \subseteq \cdots \subseteq \langle \phi(x_\phi)\rangle \subseteq \langle 1\rangle .$$

In particular $GF(2)[x] / \langle \phi(x)\rangle$ is a field. Also by the above lemma the ideals of $GF(2)[\tilde{x}] = GF(2)[x] / \langle x^p+1\rangle$ correspond uniquely to the factors of x^p+1. This result enables us to characterize the $GF(2)$-dimension of every ideal in $GF(2)[\tilde{x}]$. More generally we prove

Theorem 3.2. Let $\ell(x) \in GF(2)[x]$. Let $x_\ell = x + \langle \ell(x) \rangle$. Let $g(x)$ be an element in $GF(2)[x]$ such that $g(x) \mid \ell(x)$. Then the $GF(2)$-dimension of $\langle g(x_\ell) \rangle$ equals degree $\ell(x)$ - degree $g(x)$.

Proof: We show that every element of $\langle g(x_\ell) \rangle$ has a unique representation in the form

$$\sum_{i=0}^{n-1} b_i x_\ell^i g(x_\ell)$$

where $n = \deg \ell - \deg g$ and $b_i \in GF(2)$ for $i = 0, \ldots, n-1$.

We prove existence: Let $k(x_\ell) \in \langle g(x_\ell) \rangle$. Then there exists $m(x_\ell)$ such that $k(x_\ell) = m(x_\ell)\, g(x_\ell)$. Let $k(x)$ and $m(x)$ be pre-images in $GF(2)[x]$ of $k(x_\ell)$ and $m(x_\ell)$. We may assume that $\deg k(x) < \deg \ell(x)$. Then there exists $n(x)$ in $GF(2)[x]$ such that $k(x) = m(x)\, g(x) + n(x)\, \ell(x)$. By assumption $g(x) \mid \ell(x)$, hence there exists $g'(x)$ in $GF(2)[x]$ such that $g(x)\, g'(x) = \ell(x)$. Therefore

$$k(x) = m(x)\, g(x) + n(x)\, g'(x)\, g(x)$$

$$= (m(x) + n(x)\, g'(x))\, g(x).$$

Hence, $\deg(m(x) + n(x)\, g'(x)) \leq \deg \ell(x) - \deg g(x) - 1 = n-1$. Let

$$\sum_{i=0}^{n-1} b_i x^i = m(x) + n(x)\, g'(x)\,, \quad b_i \in GF(2).$$

Then

$$\sum_{i=0}^{n-1} b_i x_\ell^i\, g(x_\ell) = k(x_\ell)\,.$$

We prove uniqueness: If $\sum_{i=0}^{n-1} b_i x_\ell^i\, g(x_\ell) = \sum_{i=0}^{n-1} b_i' x_\ell^i\, g(x_\ell)$, then

$$\sum_{i=0}^{n-1} (b_i - b_i') x_\ell^i g(x_\ell) = 0.$$

Hence,

$$\ell(x) \Bigm| \sum_{i=0}^{n-1} (b_i - b_i') x^i g(x).$$

But

$$\deg \sum_{i=0}^{n-1} (b_i - b_i') x^i g(x) \leq n-1 + \deg g(x) = \deg \ell(x) - 1 < \deg \ell(x).$$

Therefore

$$\sum_{i=0}^{n-1} (b_i - b_i') x^i g(x) = 0, \quad \text{hence } b_i = b_i' \text{ for } i = 0,\ldots,n-1.$$

The information about the ideal structure of $GF(2)[\tilde{x}] = GF(2)[x]/\langle x^p+1\rangle$ which can be obtained from the above results depends completely on how much is known about the factorization of x^p+1 over $GF(2)[x]$. So we study the factorization of x^p+1 over $GF(2)[x]$. First we may assume that p is odd, for if $p = 2^k p'$ where p' is odd, then $(x^p+1) = (x^{p'}+1)^{2k}$ over $GF(2)$. We have the following well known result concerning the factorization of x^p-1 over Q.

Lemma 3.4. For each positive integer d, let ζ_d be a primitive dth root of unity. Let

$$\Psi_d(x) = \prod_{(i,d)=1} (x - \zeta_d^i).$$

Then

i) $\Psi_d(x)$ is a polynomial with rational integral coefficients.

ii) $\Psi_d(x)$ is Q-irreducible and has degree $\varphi(d)$, where φ is the Euler function.

iii) For any positive integer p,

$$x^p - 1 = \prod_{d|p} \Psi_d(x)$$

is the complete factorization of x^p-1.

Proof: Van der Waerden [14], p. 113 and p. 162.

The polynomial $\Psi_d(x)$ for d a positive integer is called the dth <u>cyclotomic polynomial</u>. We have

$$x^p + 1 = \prod_{d|p} \Psi_d(x) \quad \text{over} \quad GF(2)[x] .$$

In general this is not a complete factorization; some $\Psi_d(x)$ may not be GF(2)-irreducible. Therefore we consider the factorization of $\Psi_d(x)$ over GF(2). Since we may assume that p is odd, we may also assume that <u>d is odd</u>. Let A_d denote the multiplicative group of non-zero least positive residues mod d which are relatively prime to d. Then $2 \in A_d$ because d is odd. Let B_d denote the multiplicative group which is the quotient group of A_d with respect to the subgroup of A_d generated by 2.

$$B_d = A_d / \langle 2 \rangle .$$

That is, B_d is the multiplicative group of cosets of the subgroup $\langle 2 \rangle$ of A_d. If $b \in B_d$, that is if b is such a coset, we define

$$\psi_b(x) = \prod_{i \in b} (x - \zeta_d^i)$$

where the product is taken over the field $GF(2)[\zeta_d]$.

<u>Theorem 3.3.</u> Let d be a positive odd rational integer. Let e be the order of the subgroup $\langle 2 \rangle$ of A_d. Then

i) For every $b \in B_d$, $\psi_b(x) \in GF(2)[x]$.

ii) For every $b \in B_d$, $\psi_b(x)$ is GF(2)-irreducible and has degree e.

iii) Also

$$\Psi_d(x) = \prod_{b \in B_d} \psi_b(x)$$

is the complete factorization of $\Psi_d(x)$ into irreducible polynomials over GF(2).

Proof: By definition of A_d we have

$$\Psi_d(x) = \prod_{i \in A_d} (x - \zeta_d^i) .$$

Since the cosets in B_d partition A_d, we have that

$$\Psi_d(x) = \prod_{b \in B_d} \psi_b(x) \quad \text{over } GF(2)[\zeta_d].$$

Each $\psi_b(x) \in GF(2)[\zeta_d][x]$ has degree equal to the number of elements in a coset b in B_d, that is, the order of $\langle 2 \rangle$ in A_d, which is e. We need only show that each $\psi_b(x)$ is an element of $GF(2)[x]$ and is irreducible. The Galois group of the field $GF(2)[\zeta_d]$ over GF(2) is a cyclic group generated by the automorphism $\alpha \to \alpha^2$ for $\alpha \in GF(2)[\zeta_d]$ (see Albert [1], p. 127). If we apply this automorphism to $\psi_b(x)$ we obtain

$$\sigma\psi_b(x) = \prod_{i \in b} (x - \zeta_d^{2i}).$$

But $\zeta_d^d = 1$, hence we may choose representatives for all the powers of ζ_d to be least positive residues mod d. However if $i \in b$, the least positive residue of 2i mod d is again in b because b is a coset of $\langle 2 \rangle$. The mapping which takes each least positive residue $i \in b$ onto the least positive residue of 2i mod d is a one-to-one mapping of b onto itself.

Hence

$$\sigma\psi_b(x) = \psi_b(x) .$$

Therefore all the coefficients of $\psi_b(x)$ are fixed by the Galois group of $GF(2)[\zeta_d]$ over $GF(2)$. Hence $\psi_b(x)$ is a polynomial whose coefficients are in $GF(2)$. Moreover each $\psi_b(x)$ is irreducible because $\psi_b(x)$ is the minimum polynomial in $GF(2)[x]$ for ζ_d^i if $i \in b$. For if $\psi(x)$ is a polynomial in $GF(2)[x]$ such that $\psi(\zeta_d^i) = 0$ for some $i \in b$, then applying the automorphism σ and its powers to $\psi(\zeta_d^i)$ we would conclude that $\psi(\zeta_d^{2^k i}) = 0$ for all k. But then $\psi(\zeta_d^j) = 0$ for $j \in b$. Hence $\psi_b(x)$ divides $\psi(x)$. Therefore $\psi_b(x)$ is $GF(2)$-irreducible.

If d is an odd positive integer, then the order of the subgroup $\langle 2 \rangle$ of the multiplicative group A_d is called the <u>exponent</u> of $2 \bmod d$. The order of $B_d = A_d / \langle 2 \rangle$ is called the <u>index</u> of $2 \bmod d$. If e_d is the exponent of $2 \bmod d$, then clearly $e_d | \varphi(d)$ where φ is the Euler phi function. Adopt the convention that $e_1 = 1$ and $\varphi(1) = 1$.

<u>Theorem 3.4.</u> Let p be an arbitrary positive integer. Let $p = 2^k p'$ where p' is odd and for each $d|p'$ let e_d be the exponent of $2 \bmod d$. Then every ideal of $GF(2)[x]/\langle x^p+1\rangle$ has $GF(2)$-dimension of the form

$$p - \sum_{d|p'} a_d e_d$$

where

$$0 \leq a_d \leq 2^k \varphi(d)/e_d .$$

Proof: We shall use Lemma 3.3, Theorem 3.2, Lemma 3.4 and Theorem 3.3. Let $\tilde{x} = x + \langle x^p+1\rangle$ in $GF(2)[x]$. Let $\langle k(\tilde{x})\rangle$ be an arbitrary ideal in $GF(2)[x]/\langle x^p+1\rangle$. If $\langle k(\tilde{x})\rangle$ is the zero ideal, then let $a_d = 2^k \varphi(d)/e_d$ for every $d|p'$. We have

$$p - \sum_{d|p'} 2^k \varphi(d) = p - 2^k \sum_{d|p'} \varphi(d).$$

By Theorem 63, Hardy and Wright [7],

$$\sum_{d|p'} \varphi(d) = p' .$$

Hence

$$p - 2^k \sum_{d|p'} \varphi(d) = p - 2^k p' = p - p = 0$$

which is the dimension of $\langle 0 \rangle$. Therefore assume that $\langle k(\tilde{x}) \rangle$ is not the zero ideal. Assume $k(x) \in GF(2)[x]$. By Lemma 3.3 we may assume that $k(x) | x^p+1$. By Theorem 3.2 the $GF(2)$-dimension of $\langle k(\tilde{x}) \rangle$ is p-degree $k(x)$. By Lemma 3.4 and Theorem 3.3 the factorization of x^p+1 over $GF(2)$ is

$$x^p+1 = \left(\prod_{d|p'} \prod_{b \in B_d} \psi_b(x) \right)^{2^k} .$$

If $b \in B_d$, degree $\psi_b(x)$ is e_d. The order of B_d is $\varphi(d)/e_d$. Therefore if $k(x) | x^p+1$ then degree $k(x)$ has the form

$$\sum_{d|p'} a_d e_d$$

where

$$0 \leq a_d \leq 2^k \varphi(d)/e_d .$$

Hence the dimension of $\langle k(\tilde{x}) \rangle$ has the form

$$p - \sum_{d|p'} a_d e_d .$$

Corollary 3.4.1. Let q be an odd prime and let $p = (q-1)/2$. Let $p = 2^k p'$ where p' is odd and for each $d | p'$ let e_d be the exponent of

2 mod d. Then the rank of the matrix of cyclotomic signatures M_q has the form

$$p - \sum_{d|p'} a_d e_d$$

where

$$0 \leq a_d \leq 2^k \varphi(d)/e_d \qquad \text{for } d|p'.$$

Proof: Theorem 2.7 and Theorem 3.4.

For example consider the case $q = 29$. Then $p = 14 = 2 \cdot 7$. The requirement $d|7$ implies $d = 1$ or $d = 7$. Then $e_1 = 1$ and $e_7 = 3$. Also $\varphi(1) = 1$ and $\varphi(7) = 6$. We obtain the expression $14 - a_1 - 3a_7$ where $0 \leq a_1 \leq 2$, $0 \leq a_7 \leq 4$. From Appendix I we have that M_{29} has rank 11. Hence $a_1 = 0$, $a_7 = 1$.

Corollary 3.4.1 limits the value of the rank of the matrix of cyclotomic signatures. Before more can be said about the rank of M_q we must study the ideal in $GF(2)[x]/\langle x^p+1\rangle$ which corresponds to it.

In Chapter II we introduced a homomorphism $\mathrm{sgn}: V \to GF(2)[G(F/Q)]$ from the group of units in the field F to the group ring $GF(2)[G(F/Q)]$. Let σ be a generator of $G(F/Q)$. Then we have an isomorphism from $GF(2)[G(F/Q)]$ to $GF(2)[x]/\langle x^p+1\rangle$ given by $\sigma \to \tilde{x} = x + \langle x^p+1\rangle$. Therefore there is a homomorphism $\overline{\mathrm{sgn}}: V \to GF(2)[x]/\langle x^p+1\rangle$ from the group of units in F to $GF(2)[x]/\langle x^p+1\rangle$ and it is defined by

$$\overline{\mathrm{sgn}}(\mu) = \sum_{i=0}^{p-1} \mathrm{sgn}_{\sigma^i}(\mu)\, \tilde{x}^i, \quad \mu \in V. \qquad [1]$$

We are interested in the ideal in $GF(2)[x]/\langle x^p+1\rangle$ which is generated by the images $\overline{\mathrm{sgn}}(\upsilon_1), \ldots, \overline{\mathrm{sgn}}(\upsilon_p)$.

---

[1] The homomorphism $\overline{\mathrm{sgn}}$ is therefore dependent on the choice σ of a generator of $G(F/Q)$.

Let ℓ be a primitive root mod q. Let σ_ℓ be the automorphism on $Q(\zeta)$ which is induced by setting $\sigma_\ell(\zeta) = \zeta^\ell$. Then $\sigma_\ell^i(\zeta) = \zeta^{\ell^i}$ and therefore the order of σ_ℓ is q-1, whence σ_ℓ generates the Galois group of $Q(\zeta)$ over Q. Therefore the restriction of σ_ℓ to $Q(\zeta+\zeta^{-1}) = F$ generates the Galois group of F over Q. Hence

$$\overline{\operatorname{sgn}}(\mu) = \sum_{i=0}^{p-1} \operatorname{sgn}_{\sigma_\ell^i}(\mu)\tilde{x}^i.$$

In Chapter II we defined the automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_p$ by $\sigma_j(\zeta) = \zeta^j$. Let $0 \leqslant i \leqslant p-1$. If $1 \leqslant j \leqslant p$ is such that $j \equiv \ell^i \bmod q$ or $-j \equiv \ell^i \bmod q$, then σ_j and σ_ℓ^i determine the same automorphism on $Q(\zeta+\zeta^{-1})$. We adopt the following notation: If j is a non-zero residue mod q, let $\ell g_\ell j = i$ iff $j \equiv \ell^i \bmod q$ and $0 \leqslant i \leqslant q-1$. We write $\ell g j$ in place of $\ell g_\ell j$ unless there may be some confusion. It is asserted that as j ranges through the set $\{1, 2, \ldots, p\}$ then the least positive residues of $\ell g j \bmod p$ range through the set $\{0, \ldots, p-1\}$. We need only show that $\ell g 1, \ldots, \ell g p$ are incongruent mod p. If $\ell g j_1 \equiv \ell g j_2 \bmod p$, then

$$\ell^{\ell g j_1} \equiv \pm\, \ell^{\ell g j_2} \bmod q, \quad \text{since} \quad \ell^p \equiv -1 \bmod q.$$

Therefore $j_1 \equiv \pm j_2 \bmod q$. But $1 \leqslant j_1, j_2 \leqslant p$ implies that $j_1 \equiv j_2 \bmod q$. Hence $j_1 = j_2$.

We have that $\tilde{x} = x + \langle x^p + 1 \rangle$ satisfies $\tilde{x}^i = \tilde{x}^j$ iff $i \equiv j \bmod p$. Therefore, if $1 \leqslant j \leqslant p$, then

$$\begin{aligned} \overline{\operatorname{sgn}}(\upsilon_j) &= \sum_{i=0}^{p-1} \operatorname{sgn}_{\sigma_\ell^i}(\upsilon_j)\tilde{x}^i \\ &= \sum_{i=1}^{p} \operatorname{sgn}_{\sigma_\ell^{\ell g i}}(\upsilon_j)\tilde{x}^{\ell g i}. \end{aligned}$$

But $\sigma_\ell^{\ell g i} = \sigma_i$ by the definition of $\ell g i$. Hence

$$\overline{\mathrm{sgn}}\,(\upsilon_j) = \sum_{i=1}^{p} \mathrm{sgn}_{\sigma_i}(\upsilon_j)\,\tilde{x}^{\ell g\, i}.$$

From Chapter II we have that $M_q = (m_{ji})$, $i,j = 1, \ldots, p$ where

$$m_{ji} = \mathrm{sgn}_{\sigma_i}(\upsilon_j).$$

Hence

$$\overline{\mathrm{sgn}}\,(\upsilon_j) = \sum_{i=1}^{p} m_{ji}\,\tilde{x}^{\ell g\, i}.$$

Let

$$h_j(\tilde{x}) = \overline{\mathrm{sgn}}\,(\upsilon_j) \qquad j = 1, \ldots, p.$$

Then the ideal $\langle h_1(\tilde{x}), \ldots, h_p(\tilde{x})\rangle$ in $GF(2)[\tilde{x}]$ is the ideal corresponding to the $G(F/Q)$-submodule $\mathrm{sgn}(U)$ in $GF(2)[G(F/Q)]$. Hence the $GF(2)$-dimension of $\langle h_1(\tilde{x}), \ldots, h_p(\tilde{x})\rangle$ equals the rank of M_q. The ring $GF(2)[\tilde{x}] = GF(2)[x]/\langle x^p+1\rangle$ is a principal ideal ring and therefore there exists $H_q(x)$ in $GF(2)[x]$ such that

$$\langle H_q(\tilde{x})\rangle = \langle h_1(\tilde{x}), \ldots, h_p(\tilde{x})\rangle.$$

By Lemma 3.3 we may assume that $H_q(x) \mid x^p+1$.[2]

We prove

Theorem 3.5. Let q be an odd prime. If $p = (q-1)/2$ is a prime and if 2 is a primitive root mod p then the matrix M_q of cyclotomic signatures is non-singular over $GF(2)$.

Proof: We show that the rank of M_q is exactly p. It is easy to see that for any odd prime q the first two rows of the matrix M_q are distinct and therefore the rank of M_q is at least 2. Since the rank of

---

[2] The polynomial $H_q(x)$ is not uniquely defined. It depends on the chosen generator of $G(F/Q)$. However the ideal $\langle H_q(\tilde{x})\rangle$ is unique up to automorphisms of $GF(2)[\tilde{x}]$.

M_q equals the dimension of $\langle H_q(\tilde{x})\rangle$ it follows that degree $H_q(x) \leq p-2$ by Theorem 3.2. By Lemma 3.4 and Theorem 3.3 the complete factorization of x^p+1 over $GF(2)$ is

$$x^p+1 = (x+1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

But $H_q(x) \mid x^p+1$. Since $h_1(\tilde{x}) = 1 + \tilde{x} + \cdots + \tilde{x}^{p-1} \in \langle H_q(\tilde{x})\rangle$ we have that $H_q(x) \mid 1 + x + \cdots + x^{p-1}$. But degree $H_q(x) \leq p-2$. Hence $H_q(x) = 1$. Therefore $\langle H_q(\tilde{x})\rangle = GF(2)[\tilde{x}]$ and hence the rank of M_q is p.

Corollary 3.5.1. Let q be an odd prime ≥ 7. If $p = (q-1)/2$ is a prime, $p \equiv 3 \bmod 8$ and if $(p-1)/2$ is a prime, then the matrix M_q of cyclotomic signatures is non-singular over $GF(2)$.

Proof: We show that 2 is a primitive root mod p and then apply Theorem 3.5. It is known that 2 is a quadratic residue of primes $p \equiv \pm 1 \bmod 8$ and a non-residue of primes $p \equiv \pm 3 \bmod 8$ (Hardy and Wright [7] p. 75). Therefore

$$\left(\frac{2}{p}\right) = -1 \qquad \left(\frac{\cdot}{\cdot}\right) \text{ is the Legendre symbol}$$

since $p \equiv 3 \bmod 8$. It is also known that for any non-zero residue $m \bmod p$ that

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \bmod p$$

if p is prime (Hardy and Wright [7] p. 74). If $(p-1)/2$ is a prime then the exponent of $2 \bmod p$ is $p-1$, $(p-1)/2$ or 2. If the exponent of $2 \bmod p$ is 2 then $p \mid 2^2-1 = 3$, hence $p = 3$ and hence 2 is a primitive root mod p. If the exponent of $2 \bmod p$ is $(p-1)/2$ then

$$2^{(p-1)/2} \equiv 1 \bmod p$$

which contradicts

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

Therefore, in every case the exponent of 2 mod p is p-1 and hence 2 is a primitive root mod p.

For example the above corollary applies to the following cases:

1) $q = 23, \quad p = 11, \quad (p-1)/2 = 5$

2) $q = 2039, \quad p = 1019, \quad (p-1)/2 = 509$

Theorem 3.5 is a stronger result however for it applies to the following cases but the corollary does not.

3) $q = 59, \quad p = 29, \quad (p-1)/2 = 14$

4) $q = 107, \quad p = 53, \quad (p-1)/2 = 26$

In fact the corollary applies precisely to a triple of primes q, $p=(q-1)/2$, $p' = (p-1)/2$ where $p' \equiv 1 \bmod 4$.

We now prove a general theorem about $H_q(x)$. Recall the definition of the least positive residue function $[\![\cdot]\!]$ from Chapter II.

<u>Theorem 3.6.</u> Let q be an odd prime and let ℓ be a primitive root mod q. If L is the set of positive integers defined by

$$L = \{ i \mid 0 \leq i \leq p-1, \ [\![\ell^i]\!] > p \}$$

and if

$$G(x) = \sum_{i \in L} x^i$$

then,

$$H_q(x) = \text{g.c.d. } (G(x)(x+1)+1, \ x^p+1)$$

over $GF(2)[x]$.

Proof: $H_q(x)$ is the polynomial in $GF(2)[x]$ such that

$$\langle H_q(\tilde{x}) \rangle = \langle h_1(\tilde{x}), \ \dots, \ h_p(\tilde{x}) \rangle \qquad \text{and}$$

$$H_q(x) \mid x^p+1$$

where

$$h_j(\tilde{x}) = \overline{\operatorname{sgn}}(\upsilon_j) = \sum_{i=0}^{p-1} \operatorname{sgn}_{\sigma_\ell^i}(\upsilon_j)\,\tilde{x}^i .$$

Recall that $\sigma_\ell(\zeta) = \zeta^\ell$. If $m \equiv \pm\, \ell^i \bmod q$, $0 \leqslant i \leqslant p\text{-}1$, $1 \leqslant m \leqslant p$, then

$$\operatorname{sgn}_{\sigma_\ell^i}(\upsilon_j) = \begin{cases} 0 \text{ if } & [\![jm]\!] \leqslant p \\ 1 \text{ if } & [\![jm]\!] > p \quad \text{for } j = 2, \ldots, p, \end{cases}$$

$$\operatorname{sgn}_{\sigma_\ell^i}(\upsilon_1) = \quad 1 .$$

For each $i = 0, \ldots, p\text{-}1$ there exists a unique integer r_i such that a) $r_i = +1$ or -1, b) $1 \leqslant [\![r_i \ell^i]\!] \leqslant p$. Then we can write

$$\operatorname{sgn}_{\sigma_\ell^i}(\upsilon_{[\![r_j \ell^j]\!]}) = \begin{cases} 0 \text{ if } [\![r_i \ell^i r_j \ell^j]\!] \leqslant p \\ 1 \text{ if } [\![r_i \ell^i r_j \ell^j]\!] > p. \end{cases}$$

We have that $r_i \ell^i r_j \ell^j \equiv r_i r_j \ell^{i+j} \bmod q$. Also $\ell^p \equiv -1 \bmod q$. Hence for $0 \leqslant k \leqslant q\text{-}1$, let

$$d_k = (-1)^{[k/p]}$$

where $[\,\cdot\,]$ is the greatest integer function. If k is any integer let

$$r_k = r_j \text{ if } j \equiv k \bmod p, \quad 0 \leqslant j \leqslant p\text{-}1$$
$$d_k = d_j \text{ if } j \equiv k \bmod q, \quad 0 \leqslant j \leqslant q\text{-}1.$$

Then,

$$r_i \ell^i r_j \ell^j \equiv r_i r_j \ell^{i+j} \equiv r_i r_j r_{i+j} d_{i+j} (r_{i+j} \ell^t) \bmod q$$

where $0 \leqslant t \leqslant p\text{-}1$ and $t \equiv i + j \bmod p$. Also

$$1 \leqslant [\![r_{i+j} \ell^t]\!] \leqslant p.$$

Therefore,

$$\operatorname{sgn}_{\sigma_\ell^i}(\upsilon_{[\![r_j \ell^j]\!]}) = \begin{cases} 0 \text{ if } r_i r_j r_{i+j} d_{i+j} = 1 \\ 1 \text{ if } r_i r_j r_{i+j} d_{i+j} = -1 \end{cases} .$$

Let

$$\rho_i = \begin{cases} 0 \in GF(2) \text{ if } r_i = 1 \\ 1 \in GF(2) \text{ if } r_i = -1 \end{cases} ; \qquad \delta_i = \begin{cases} 0 \in GF(2) \text{ if } d_i = 1 \\ 1 \in GF(2) \text{ if } d_i = -1 \end{cases} .$$

Then

$$\operatorname{sgn}_{\sigma_\ell^i}(\upsilon_{[\![r_j \ell^j]\!]}) = \rho_i + \rho_j + \rho_{i+j} + \delta_{i+j} .$$

Hence

$$h_{[\![r_j \ell^j]\!]}(\tilde{x}) = \sum_{i=0}^{p-1} (\rho_i + \rho_j + \rho_{i+j} + \delta_{i+j}) \tilde{x}^i$$

for $j = 0, \ldots, p-1$. For ease of notation, let

$$h'_j(\tilde{x}) = h_{[\![r_j \ell^j]\!]}(\tilde{x}) , \; j = 0, \ldots, p-1.$$

Then $h'_0(\tilde{x}), \ldots, h'_{p-1}(\tilde{x})$ is a rearrangement of $h_1(\tilde{x}), \ldots, h_p(\tilde{x})$. Also let

$$t_j(\tilde{x}) = \sum_{i=0}^{p-1} \delta_{i+j} \tilde{x}, \; j = 0, \ldots, p-1.$$

Note that,

$$G(\tilde{x}) = \sum_{i \in L} \tilde{x}^i = \sum_{i=0}^{p-1} \rho_i \tilde{x}^i$$

since $i \in L$ iff $[\![\ell^i]\!] > p$, iff $r_i = -1$, iff $\rho_i = 1$ in $GF(2)$. We have

$$\tilde{x}^{p-j} G(\tilde{x}) = \sum_{i=0}^{p-1} \rho_i \tilde{x}^{i+p-j} = \sum_{i=0}^{p-1} \rho_i \tilde{x}^{i-j} .$$

But $r_k = r_j$ iff $k \equiv j \bmod p$, hence $\rho_k = \rho_j$ iff $k \equiv j \bmod p$. Therefore

$$\tilde{x}^{p-j}\, G(\tilde{x}) = \sum_{i=0}^{p-1} \rho_{i+j}\, \tilde{x}^{i}.$$

Also note that

$$h_0'(\tilde{x}) = 1 + \tilde{x} + \cdots + \tilde{x}^{p-1}.$$

Hence

$$\begin{aligned} h_j'(\tilde{x}) &= G(\tilde{x}) + \rho_j h_0'(\tilde{x}) + \tilde{x}^{p-j}\, G(\tilde{x}) + t_j(\tilde{x}) \\ &= \rho_j h_0'(\tilde{x}) + t_j(\tilde{x}) + (\tilde{x}^{p-j} + 1)\, G(\tilde{x}) \end{aligned}$$

$$\text{for } j = 0, \ldots, p-1.$$

Note that

$$t_j(\tilde{x}) = \tilde{x}^{p-j}\, (1 + \tilde{x} + \cdots + \tilde{x}^{j-1}).$$

We have for $0 \leqslant j \leqslant p-1$

$$h'_j(\tilde{x}) + \rho_j h_0'(\tilde{x}) = t_j(\tilde{x}) + (\tilde{x}^{p-j}+1)\, G(\tilde{x})$$

whence, if $2 \leqslant j \leqslant p$,

$$\begin{aligned} & h'_{p-j}(\tilde{x}) + \rho_{p-j} h_0'(\tilde{x}) + h'_{p-(j-1)}(\tilde{x}) + \rho_{p-(j-1)} h_0'(\tilde{x}) \\ &= \tilde{x}^{j}(1+\tilde{x}+\cdots+\tilde{x}^{p-j}) + \tilde{x}^{j-1}(1+\tilde{x}+\cdots+\tilde{x}^{p-(j-1)}) + (\tilde{x}^{j} + \tilde{x}^{j-1})G(\tilde{x}) \\ &= \tilde{x}^{j-1} + \tilde{x}^{j-1}(\tilde{x}+1)\, G(\tilde{x}) \\ &= \tilde{x}^{j-1}(1+(1+\tilde{x})\, G(\tilde{x})\,). \end{aligned}$$

But $\tilde{x}^{j-1}$ is a unit in $GF(2)[\tilde{x}]$.

Hence

$$\langle H_q(\tilde{x}) \rangle \supseteq \langle G(\tilde{x})\, (\tilde{x} + 1) + 1 \rangle.$$

Since $x + 1 \nmid G(x)\,(x+1) + 1$, it follows that

$$h_0'(\tilde{x}) = 1 + \tilde{x} + \cdots + \tilde{x}^{p-1} \in \langle G(\tilde{x})\, (\tilde{x}+1) + 1 \rangle.$$

We have for $2 \leqslant j \leqslant p$

$$h'_{p-j}(\tilde{x}) + \rho_{p-j}h'_0(\tilde{x}) + h'_{p-(j-1)}(\tilde{x}) + \rho_{p-(j-1)}h'_0(\tilde{x}) = \tilde{x}^{j-1}(1+(1+\tilde{x})G(\tilde{x})).$$

Successively setting $j = p, p-1, p-2, \ldots, 2$ we conclude that

$$h'_1(\tilde{x}),\ h'_2(\tilde{x}),\ \ldots,\ h'_{p-1}(\tilde{x}) \in \langle G(\tilde{x})\ (\tilde{x}+1)+1\rangle.$$

Hence

$$\langle H_q(\tilde{x})\rangle = \langle G(\tilde{x})\ (\tilde{x}+1)+1\rangle.$$

Then applying Lemma 3.3 we conclude that

$$H_q(x) = \text{g.c.d.}\ (G(x)(x+1)+1,\ x^p+1).$$

One significant feature of Theorem 3.6 is that it can be used to compute $H_q(x)$ and hence the rank of M_q. And if q is large it is definitely easier to compute $H_q(x)$ with a computer than to compute the rank of M_q. Moreover if $H_q(x)$ can be factored into irreducibles we can obtain information about the ideal $\langle H_q(x)\rangle$. The methods for factoring $H_q(x)$ are discussed in Appendix II. The following theorem was used to verify by computer that for all primes q, $7 \leq q \leq 4703$ such that $p = (q-1)/2$ is prime, the matrix M_q is non-singular. Of course for each of these cases it had to be shown that $H_q(x) = 1$.

Theorem 3.7. Let q be an odd prime such that $p = (q-1)/2$ is odd. Let ℓ be a primitive root mod q and let $k = \ell^2$. If L' is the set of integers defined by

$$L' = \{ i \mid 0 \leq i \leq p-1,\ [\![k^i]\!] > p \}$$

and if

$$G'(x) = \sum_{i \in L'} x^i$$

then

$$H_q(x) = \text{g.c.d.}\,(G'(x),\ x^{p-1}+x^{p-2}+\cdots+x+1)$$

Proof: The proof is analogous to the proof of Theorem 3.6. The element σ_k is a generator of $G(F/Q)$. For if $k^i \equiv \pm 1 \bmod q$, then $\ell^{2i} \equiv \pm 1 \bmod q$, hence $4i \equiv 0 \bmod q-1$. Therefore $2i \equiv 0 \bmod p$. But since p is odd, we have that $i \equiv 0 \bmod p$. Therefore σ_k has order p. Let

$$n_j(x) = \sum_{i=0}^{p-1} \operatorname{sgn}_{\sigma_k}(\upsilon_j)\, x^i, \quad j = 1, \ldots, p.$$

Then

$$\langle H_q(\tilde{x}) \rangle = \langle n_1(\tilde{x}), \ldots, n_p(\tilde{x}) \rangle .$$

For each $i = 0, \ldots, p-1$ there exists a unique integer r'_i such that a) $r'_i = 1$ or -1, b) $1 \leqslant [\![r'_i k^i]\!] \leqslant p$. Then we can write

$$\operatorname{sgn}_{\sigma_k^i}(\upsilon_{[\![r'_j k^j]\!]}) = \begin{cases} 0 \text{ if } [\![r'_i k^i r'_j k^j]\!] \leqslant p \\ 1 \text{ if } [\![r'_i k^i r'_j k^j]\!] > p. \end{cases}$$

If n is any integer let

$$r'_n = r'_j \quad \text{if } n \equiv j \bmod p, \quad 0 \leqslant j \leqslant p-1.$$

Then

$$r'_i k^i r'_j k^j \equiv r'_i r'_j k^{i+j} \equiv r'_i r'_j r'_{i+j} (r'_{i+j} k^{i+j}) \bmod q$$

and

$$1 \leqslant [\![r'_{i+j} k^{i+j}]\!] \leqslant p \quad \text{since } k^p \equiv 1 \bmod q.$$

Therefore,

$$\operatorname{sgn}_{\sigma_k^i}(\upsilon_{[\![r'_j k^j]\!]}) = \begin{cases} 0 \text{ if } r'_i r'_j r'_{i+j} = 1 \\ 1 \text{ if } r'_i r'_j r'_{i+j} = -1. \end{cases}$$

Let

$$\rho'_i = \begin{cases} 0 \in GF(2) \text{ if } r'_i = 1 \\ 1 \in GF(2) \text{ if } r'_i = -1. \end{cases}$$

Then

$$\operatorname{sgn}_{\sigma_k}{}^{i}\,(\upsilon_{[\![r'_j k^j]\!]}) = \rho'_i + \rho'_j + \rho'_{i+j}\,.$$

Hence

$$n_{[\![r'_j k^j]\!]}(\tilde{x}) = \sum_{i=0}^{p-1} (\rho'_i + \rho'_j + \rho'_{i+j})\, \tilde{x}^i$$

$$\text{for } j = 0, \ldots, p-1.$$

Now let

$$n'_j(\tilde{x}) = n_{[\![r'_j k^j]\!]}(\tilde{x}) \qquad j = 0, \ldots, p-1.$$

Then,

$$n'_0(\tilde{x}) = 1 + \tilde{x} + \cdots + \tilde{x}^{p-1}.$$

Also,

$$G'(x) = \sum_{i \in L'} x^i = \sum_{i=0}^{p-1} \rho'_i x^i.$$

Then,

$$n'_j(\tilde{x}) = \rho'_j n'_0(\tilde{x}) + (\tilde{x}^{p-j}+1) G'(\tilde{x}) \qquad j = 0, \ldots, p-1.$$

Hence,

$$\sum_{j=0}^{p-1} n'_j(\tilde{x}) + (\sum_{j=0}^{p-1} \rho'_j)\, n'_0(\tilde{x}) = ((\sum_{j=0}^{p-1} \tilde{x}^{p-j}) + p)\, G'(\tilde{x}) = (n'_0(\tilde{x}) + 1)\, G'(\tilde{x}).$$

Therefore,

$$G'(\tilde{x}) = \sum_{j=0}^{p-1} n'_j(\tilde{x}) + (\sum_{j=0}^{p-1} \rho'_j) n'_0(\tilde{x}) + G'(\tilde{x}) n'_0(\tilde{x}).$$

Hence

$$\langle G'(\tilde{x}) \rangle \subseteq \langle n'_0(\tilde{x}), \ldots, n'_p(\tilde{x}) \rangle = \langle n_1(\tilde{x}), \ldots, n_p(\tilde{x}) \rangle.$$

But,

$$n'_j(\tilde{x}) = \rho'_j n'_0(\tilde{x}) + (\tilde{x}^{p-j}+1)\, G'(\tilde{x}), \; j = 1, \ldots, p-1.$$

Therefore

$$\langle G'(\tilde{x}),\; n'_0(\tilde{x}) \rangle = \langle n_1(\tilde{x}), \ldots, n_p(\tilde{x}) \rangle = \langle H_q(\tilde{x}) \rangle.$$

Chapter IV

Application of the Reciprocity Theorem of Class Field Theory

The object of this chapter is to use the reciprocity theorem of class field theory to replace the problem of the sign distribution of cyclotomic units in F' by a problem in the completion of F at the primes which lie above (2). Before stating the reciprocity theorem we must recall some elementary definitions and facts of algebraic number theory (see O'Meara [11]).

Let K be a number field, i.e., a finite field extension of Q, and let L be a finite Galois extension of K with Galois group $G(L/K)$. A <u>prime</u> of K is an equivalence class of valuations of K. If $\mathfrak{p}$ is a prime of K, we let $|\cdot|_{\mathfrak{p}}$ denote some particular valuation in $\mathfrak{p}$ (for example, the normalized valuation if $\mathfrak{p}$ is discrete). We let $K_{\mathfrak{p}}$ denote the completion of K at the prime $\mathfrak{p}$. There is a natural embedding of K into $K_{\mathfrak{p}}$, so we may assume that $K \subseteq K_{\mathfrak{p}}$.

Let $\mathfrak{q}$ be a prime in L which lies over the prime $\mathfrak{p}$ in K, i.e. $\mathfrak{q}$ induces the prime $\mathfrak{p}$ if it is restricted to K. We write $\mathfrak{q}|\mathfrak{p}$. Let σ be an element of $G(L/K)$. The relation

$$|\alpha|_{\sigma\mathfrak{q}} = |\sigma^{-1}(\alpha)|_{\mathfrak{q}}, \ \alpha \in L$$

defines a prime of L (which we denote by $\sigma\mathfrak{q}$) which also lies over $\mathfrak{p}$. If $\tau \in G(L/K)$ then $\sigma(\tau\mathfrak{q}) = (\sigma\tau)\mathfrak{q}$. If σ acts on a Cauchy sequence for $\mathfrak{q}$ in L then it gives a Cauchy sequence for $\sigma\mathfrak{q}$ in L. Conversely, if σ^{-1} acts on a Cauchy sequence for $\sigma\mathfrak{q}$ in L, it gives a Cauchy sequence for $\mathfrak{q}$ in L. Therefore σ induces an isomorphism $\sigma_{\mathfrak{q}}$ of the completions $L_{\mathfrak{q}}$ and $L_{\sigma\mathfrak{q}}$ of L. Moreover this isomorphism is a $K_{\mathfrak{p}}$-

isomorphism, i.e. it fixes the completion $K_{\mathfrak{p}}$ element wise.

Let $\mathfrak{q}$ be a prime in L which lies over the prime $\mathfrak{p}$ in K. The subgroup $G_{\mathfrak{q}}(L/K)$ of $G(L/K)$ defined by

$$G_{\mathfrak{q}}(L/K) = \{\sigma \mid \sigma \in G(L/K), \quad \sigma\mathfrak{q} = \mathfrak{q}\}$$

is called the <u>decomposition group</u> of $\mathfrak{q}$. If $\sigma \in G(L/K)$, it is easy to see that

$$G_{\sigma\mathfrak{q}}(L/K) = \sigma\, G_{\mathfrak{q}}(L/K)\, \sigma^{-1}.$$

Also if $\sigma \in G_{\mathfrak{q}}(L/K)$ then σ induces a $K_{\mathfrak{p}}$-automorphism $\sigma_{\mathfrak{q}}$ of $L_{\mathfrak{q}}$. We now state two lemmas without proof (see Cassels and Fröhlich [6], p. 163).

<u>Lemma 4.1</u>. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be primes of L which lie over the prime $\mathfrak{p}$ in K. Then there exists a $\sigma \in G(L/K)$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$.

<u>Lemma 4.2</u>. Let $\mathfrak{q}$ be a prime in L which lies over the prime $\mathfrak{p}$ in K. Then

i) $L_{\mathfrak{q}}$ is Galois over $K_{\mathfrak{p}}$.

ii) The mapping from $G_{\mathfrak{q}}(L/K)$ to $G(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ given by $\sigma \to \sigma_{\mathfrak{q}}$ is an isomorphism.

Let $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$ be the norm from $L_{\mathfrak{q}}$ to $K_{\mathfrak{p}}$ where $\mathfrak{q}$ lies above $\mathfrak{p}$. We apply the two lemmas above to prove

<u>Lemma 4.3</u>. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be primes in L which lie above the prime $\mathfrak{p}$ in K. Then

$$N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(L_{\mathfrak{q}}^{*}) = N_{L_{\mathfrak{q}'}/K_{\mathfrak{p}}}(L_{\mathfrak{q}'}^{*}).$$

Proof: By Lemma 4.1, there exists a $\sigma \in G(L/K)$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$. We show that if $\alpha \in L^*_{\mathfrak{q}}$ then

$$\sigma_{\mathfrak{q}}(N_{L_{\mathfrak{q}}/K_p}(\alpha)) = N_{L_{\mathfrak{q}'}/K_p}(\sigma_{\mathfrak{q}}(\alpha)) .$$

We have,

$$\sigma_{\mathfrak{q}}(N_{L_{\mathfrak{q}}/K_p}(\alpha)) = \sigma_{\mathfrak{q}} \prod_{\tau \in G(L/K)} \tau_{\mathfrak{q}}(\alpha) \qquad \text{by Lemma 4.2.}$$

Hence

$$\sigma_{\mathfrak{q}}(N_{L_{\mathfrak{q}}/K_p}(\alpha)) = \prod_{\tau \in G_{\mathfrak{q}}(L/K)} \sigma_{\mathfrak{q}}\tau_{\mathfrak{q}}\sigma_{\mathfrak{q}}^{-1}(\sigma_{\mathfrak{q}}(\alpha))$$

$$= \prod_{\tau \in \sigma(G_{\mathfrak{q}}(L/K))\sigma^{-1}} \tau_{\mathfrak{q}}(\sigma_{\mathfrak{q}}(\alpha))$$

$$= \prod_{\tau \in G_{\sigma\mathfrak{q}}(L/K)} \tau_{\mathfrak{q}}(\sigma_{\mathfrak{q}}(\alpha)) \qquad \text{by Lemma 4.2.}$$

Hence

$$\sigma_{\mathfrak{q}}(N_{L_{\mathfrak{q}}/K_p}(\alpha)) = N_{L_{\mathfrak{q}'}/K_p}(\sigma_{\mathfrak{q}}(\alpha)).$$

Therefore $\sigma_{\mathfrak{q}}$ maps $N_{L_{\mathfrak{q}}/K_p}(L^*_{\mathfrak{q}})$ onto $N_{L_{\mathfrak{q}'}/K_p}(L^*_{\mathfrak{q}'})$. Since $N_{L_{\mathfrak{q}}/K_p}(L^*_{\mathfrak{q}})$ and $N_{L_{\mathfrak{q}'}/K_p}(L^*_{\mathfrak{q}'})$ are subgroups of K^*_p and since $\sigma_{\mathfrak{q}}$ fixes K_p, we conclude that

$$N_{L_{\mathfrak{q}}/K_p}(L^*_{\mathfrak{q}}) = N_{L_{\mathfrak{q}'}/K_p}(L^*_{\mathfrak{q}'}) .$$

Lemma 4.3 shows that the subgroup $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(L_{\mathfrak{q}}^{*})$ of the multiplicative group $K_{\mathfrak{p}}^{*}$ depends only on the prime $\mathfrak{p}$ in K and not upon the prime $\mathfrak{q}$ in L which lies above $\mathfrak{p}$. Therefore we write,

$$N(L/K,\mathfrak{p}) = N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(L_{\mathfrak{q}}^{*}) .$$

If L/K is abelian then $G_{\sigma\mathfrak{q}}(L/K) = \sigma G_{\mathfrak{q}}(L/K)\sigma^{-1} = G_{\mathfrak{q}}(L/K)$. Therefore if L/K is abelian, $G_{\mathfrak{q}}(L/K)$ depends only on $\mathfrak{p}$ where $\mathfrak{q}$ lies above $\mathfrak{p}$. Hence if L/K is abelian we write

$$G_{\mathfrak{p}}(L/K) = G_{\mathfrak{q}}(L/K).$$

We can now state the reciprocity theorem.

Theorem 4.1. Let L be a finite Galois extension of the number field K such that G(L/K) is abelian. Then for all primes $\mathfrak{p}$ in K there exists a homomorphism $\varphi_{\mathfrak{p}}: K_{\mathfrak{p}}^{*} \to G_{\mathfrak{p}}(L/K)$ such that

i) $\varphi_{\mathfrak{p}}: K_{\mathfrak{p}}^{*} \to G_{\mathfrak{p}}(L/K)$ is surjective and $\ker \varphi_{\mathfrak{p}} = N(L/K,\mathfrak{p})$.

ii) If $\alpha \in K^{*}$, then $\varphi_{\mathfrak{p}}(\alpha) = 1$ for almost all $\mathfrak{p}$, and

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\alpha) = 1 .$$

Remarks: If it becomes necessary to identify the extension L/K with the map $\varphi_{\mathfrak{p}}$, we shall write $\varphi_{\mathfrak{p},L/K}$. The proof of the reciprocity theorem will be omitted. The theorem stated here with i) appears as Theorem 2, Cassels and Fröhlich [6], p. 140, if we recall that $G_{\mathfrak{p}}(L/K)$ is canonically isomorphic to $G(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ (Lemma 4.2). In this form the theorem becomes the local reciprocity theorem. Property ii) is referred to on p. 188 of Cassels and Fröhlich [6]. The reciprocity map

$\varphi_{\mathfrak{p}}$ is also studied in Artin [2] pp. 144-164, where it is called the norm residue symbol.

We shall need one elementary property of the reciprocity map. Let K and L be fields which satisfy the hypotheses of Theorem 4.1, and let M be a field such that $K \subseteq M \subseteq L$. Then M is a finite Galois extension of K and its Galois group G(M/K) is abelian. Let $\mathfrak{p}$ be a prime in K. Then by Theorem 4.1 we have maps $\varphi_{\mathfrak{p},L/K}: K_{\mathfrak{p}}^* \to G_{\mathfrak{p}}(L/K)$ and $\varphi_{\mathfrak{p},M/K}: K_{\mathfrak{p}}^* \to G_{\mathfrak{p}}(M/K)$. Then we have the

<u>Supplemental property of the reciprocity map</u>. The diagram

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\varphi_{\mathfrak{p},L/K}} & G_{\mathfrak{p}}(L/K) \\ \text{(identity)} \downarrow & & \downarrow \text{(projection)} \\ K_{\mathfrak{p}}^* & \xrightarrow{\varphi_{\mathfrak{p},M/K}} & G_{\mathfrak{p}}(M/K) \end{array}$$

is commutative.

<u>Remarks</u>: The projection map from $G_{\mathfrak{p}}(L/K)$ to $G_{\mathfrak{p}}(M/K)$ is defined by $\sigma \to \sigma|M$. The above property is property 4), Serre [12], p. 178, or equivalently property 2), Artin [2], p. 158.

We apply the reciprocity theorem to the following situation. Let $F = Q(\zeta + \zeta^{-1})$, where as before, ζ is a primitive qth root of unity. Let E be the field $F(\sqrt{\upsilon_1}, \sqrt{\upsilon_2}, \ldots, \sqrt{\upsilon_p})$ where $\upsilon_1, \ldots, \upsilon_p$ are the cyclotomic units. The field F is a subfield of the real numbers. Since E is the compositum of the fields $F(\sqrt{\upsilon_i})$, $i = 1, \ldots, p$, E is Galois over F and its Galois group G(E/F) is an elementary abelian 2-group. Therefore we can apply Theorem 4.1.

Let $\mathfrak{p}$ be a prime in F. There exists an epimorphism

$\varphi_{\mathfrak{p}}$ of $F^*_{\mathfrak{p}}$ onto $G_{\mathfrak{p}}(E/F)$ which induces an isomorphism

$$\varphi'_{\mathfrak{p}} : F^*_{\mathfrak{p}} / N(E/F, \mathfrak{p}) \cong G_{\mathfrak{p}}(E/F)$$

and if $\alpha \in F^*$, then

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\alpha) = 1.$$

If K is any subfield of the real numbers, let ∞_K be the prime on K which is determined by ordinary absolute value. We shall write ∞ instead of ∞_K when there is no chance of confusion. A prime $\mathfrak{p}$ in F is called <u>infinite</u> if $\mathfrak{p}$ lies above ∞_Q, i.e. $\mathfrak{p} \mid \infty_Q$. Clearly ∞_F is an infinite prime in F. Hence, by Lemma 4.1 every infinite prime in F has the form $\sigma \infty_F$ for some $\sigma \in G(F/Q)$. Let $\sigma \infty_F$ be such a prime in F. The completion of F at $\sigma \infty_F$ is the same as the completion of σF at ∞_F. Hence the completion of F at $\sigma \infty_F$ is a subfield of the reals because F itself is. However the completion of F at $\sigma \infty_F$ must contain the completion of Q at ∞, and $Q_\infty = R$, the reals. Therefore $F_{\sigma \infty} = R$. The embedding of F into $F_{\sigma\infty}$ is given by the injection $\alpha \to \sigma(\alpha)$ for $\alpha \in F$.

Consider the field E. Note that $\sqrt{v_1} = \sqrt{-1}$ is an element of E, therefore $Q(\sqrt{-1}) \subseteq E \subseteq C$, where C is the field of complex numbers. If $\mathfrak{q}$ is a prime in E such that $\mathfrak{q} \mid \infty$, then it follows as above that $E_{\mathfrak{q}} = C$.

<u>Lemma 4.4</u>. Let E and F be the fields above. Let R^+ denote the positive nonzero reals. Let $\mathfrak{p} = \sigma\infty$ be an infinite prime in F, where $\sigma \in G(F/Q)$. Then

$$N(E/F, \mathfrak{p}) = R^+.$$

Proof: Let $\mathfrak{q}$ be a prime in E such that $\mathfrak{q} \mid \mathfrak{p}$. Then $E_{\mathfrak{q}} = C$ and $F_{\mathfrak{p}} = R$. The only automorphisms of C which fix R are the identity and $\alpha + \sqrt{-1}\,\beta \to \alpha - \sqrt{-1}\,\beta$. Therefore,

$$N(E/F, \mathfrak{p}) = \{\alpha^2 + \beta^2 \mid \alpha, \beta \in R,\ \alpha^2 + \beta^2 \neq 0\}$$

$$= \{\alpha^2 \mid \alpha \in R^*\} = R^+ .$$

Recall the definition of σ-sign from Chapter II.

Lemma 4.5. Let E and F be the fields above. Let $\mathfrak{p} = \sigma\infty, \sigma \in G(F/Q)$ be an infinite prime in F, and let $\varphi_{\mathfrak{p}}$ be the reciprocity map given by Theorem 4.1 for E/F. Then for $\alpha \in F^*$, $\varphi_{\mathfrak{p}}(\alpha) = 1$ iff $\operatorname{sign}_\sigma(\alpha) = 1$.

Proof: Suppose that $\alpha \in F^*$. The image of α under the embedding of F into $F_{\mathfrak{p}}$ is $\sigma(\alpha)$. Then $\varphi_{\mathfrak{p}}(\alpha) = 1$ iff $\sigma(\alpha) \in N(E/F, \mathfrak{p})$ by property i) of Theorem 4.1. By Lemma 4.4., $\sigma(\alpha) \in N(E/F, \mathfrak{p})$ iff $\sigma(\alpha) \in R^+$, i.e. iff $\operatorname{sign}_\sigma(\alpha) = 1$.

Lemma 4.5. gives the connection between the reciprocity map and the σ-sign. It is essentially this connection which allows the use of the reciprocity theorem. From the corollary, p. 29, Cassels and Fröhlich [6], we have

Lemma 4.6. Let L be a finite Galois extension of the number field K. Let $\mathfrak{q}$ be a prime in L which is unramified over the prime $\mathfrak{p}$ in K. Then every unit in $K_{\mathfrak{p}}$ is the norm of a unit in $L_{\mathfrak{q}}$.

We apply Lemma 4.6. to obtain

Lemma 4.7. Let E and F be as before. For each prime $\mathfrak{p}$ in F let $\varphi_{\mathfrak{p}}$ be the reciprocity map given by Theorem 4.1. Let (2) denote the prime on Q which is determined by the prime rational integer 2. If μ is a unit in F, i.e. $\mu \in V$, then the following relation holds:

$$\left(\prod_{p|\infty} \varphi_p(\mu)\right)\left(\prod_{p|(2)} \varphi_p(\mu)\right) = 1 .$$

Proof: Call a prime p in F odd if $p \nmid (2)$ and if $p \nmid \infty$. Let p be a prime in F such that $p \nmid \infty$. A prime q in E such that $q \mid p$ is unramified iff the value of p on the discriminant of E over F is not less than 1. But E is obtained from F by successively adjoining square roots of units in F. Hence the discriminant of E over F is a product of the primes which lie over (2). Therefore if p is a prime of F which is odd, then p is unramified. Therefore, by Lemma 4.6, if p is odd and if $\mu \in V$ then $\mu \in N(E/F, p)$. Hence $\varphi_p(\mu) = 1$ if $\mu \in V$ and p is odd. Therefore, by property ii) of Theorem 4.1. :

$$\left(\prod_{p|\infty} \varphi_p(\mu)\right)\left(\prod_{p|(2)} \varphi_p(\mu)\right) = 1.$$

The mapping

$$\mu \rightarrow \prod_{p|\infty} \varphi_p(\mu)$$

of the units V in F into G(E/F) is a homomorphism. Each $\varphi_p, p|\infty$ gives an isomorphism

$$\varphi_p' : F_p^*/N(E/F, p) \cong G_p(E/F),$$

and

$$F_p^*/N(E/F, p) = R^*/R^{*2}.$$

Hence $G_p(E/F)$ is cyclic of order 2 for each $p|\infty$. Let $\alpha \in F^*$ and let $p = \sigma\,\infty$, $\sigma \in G(F/Q)$ be a prime in F. Then we write $\alpha > 0$ at p if $\mathrm{sign}_\sigma(\alpha) = 1$, and $\alpha < 0$ at p if $\mathrm{sign}_\sigma(\alpha) = -1$. We prove

<u>Theorem 4.2.</u> Let $U = \langle \upsilon_1, \ldots, \upsilon_p \rangle$ be the multiplicative group generated by the cyclotomic units in F. Let T be the group of totally positive units in F. Then

$$U/U \cap T \cong \prod_{p|\infty} G_p(E/F).$$

Proof: Let $G_p(E/F) = \langle \sigma_p \rangle$ for each $p|\infty$. The group $\prod_{p|\infty} G_p(E/F)$ is an elementary abelian 2-group with exponent 2, hence if k is the number of even invariants of $\prod_{p|\infty} G_p(E/F)$ then there exist primes $p_1, \ldots, p_k$ such that

$$\prod_{p|\infty} G_p(E/F) = \bigoplus_{i=1}^{k} G_{p_i}(E/F).$$

Let $(U/U^2)^{\#}$ denote the dual or character group of U/U^2. Define a mapping

$$\chi: \prod_{p|\infty} G_p(E/F) \rightarrow (U/U^2)^{\#}$$

by $$\chi(\sigma)\,(\mu U^2) = \sigma(\sqrt{\mu}) / \sqrt{\mu}\ , \quad \mu \in U.$$

The mapping χ is a homomorphism, for if $\sigma, \tau \in \prod_{p|\infty} G_p(E/F)$ then

$$\chi(\sigma\tau)(\mu U^2) = (\sigma\tau)(\sqrt{\mu})/\sqrt{\mu} = \sigma((\tau(\sqrt{\mu})/\sqrt{\mu})\cdot\sqrt{\mu})/\sqrt{\mu} = (\tau(\sqrt{\mu})/\sqrt{\mu})\cdot(\sigma(\sqrt{\mu})/\sqrt{\mu})\ ,$$

since $\tau(\sqrt{\mu})/\sqrt{\mu} = \pm 1$. Hence,

$$\chi(\sigma\tau)\,(\mu U^2) = \chi(\sigma)\,(\mu U^2)\cdot\chi(\tau)\,(\mu U^2)\ , \quad \mu \in U.$$

Therefore

$$\chi(\sigma\tau) = \chi(\sigma)\cdot\chi(\tau).$$

The mapping χ is even a monomorphism, for if $\sigma \in \prod_{p|\infty} G_p(E/F)$ and $\chi(\sigma) = 1$, then $\chi(\sigma)(\mu U^2) = 1$ for all $\mu \in U$. Hence $\sigma(\sqrt{\mu}) = \sqrt{\mu}$ for all $\mu \in U$. Hence σ fixes every element of the field E and therefore $\sigma = 1$. Hence χ is a monomorphism. We chose $p_1, \ldots, p_k$ so that the elements $\sigma_{p_1}, \ldots, \sigma_{p_k}$ form a basis for $\prod_{p|\infty} G_p(E/F)$. Then the elements $\chi(\sigma_{p_1}), \ldots, \chi(\sigma_{p_k})$ form a basis for $\chi(\prod_{p|\infty} G_p(E/F))$, because χ is a monomorphism. Then there exist $\mu_1, \ldots, \mu_k \in U$ which are dual to $\chi(\sigma_{p_1}), \ldots, \chi(\sigma_{p_k})$. That is,

$$\chi(\sigma_{p_i})(\mu_j U^2) = (-1)^{\delta_{ij}}, \; i,j = 1, \ldots, k.$$

Hence,

$$\sigma_{p_i}(\sqrt{\mu_j}) = (-1)^{\delta_{ij}} \sqrt{\mu_j} \;, i,j = 1, \ldots, k.$$

Then,

$$\mu_j < 0 \text{ at } p_i = p_j$$

$$\mu_j > 0 \text{ at } p_i \neq p_j \qquad i,j = 1, \ldots, k.$$

If $p_i = \sigma_i \infty$, $\sigma_i \in G(F/Q)$, $i = 1, \ldots, k$, then we have

$$\text{sign}_{\sigma_i}(\mu_j) = (-1)^{\delta_{ij}} \quad i,j = 1, \ldots, k.$$

Hence,

$$\left| \prod_{p|\infty} G_p(E/F) \right| = 2^k \leq \left| U/U \cap T \right| .$$

We shall show that in fact equality holds. Define a mapping Λ: $U \to \prod_{p|\infty} G_p(E/F)$ by

$$\Lambda(\mu) = \bigoplus_{i=1}^{k} \varphi_{p_i}(\mu) \;, \quad \mu \in U.$$

Clearly Λ is a homomorphism. Consider $\ker \Lambda$. If $\mu \in U \cap T$, then $\varphi_{\mathfrak{p}}(\mu) = 1$ for all $\mathfrak{p}|\infty$. Hence $\mu \in \ker \Lambda$. On the other hand, if $\mu \in \ker \Lambda$, then $\bigoplus_{i=1}^{k} \varphi_{\mathfrak{p}_i}(\mu) = 1$. Hence $\varphi_{\mathfrak{p}_i}(\mu) = 1$ for $i = 1, \ldots, k$. Then $\mu > 0$ at $\mathfrak{p}_i$ for $i = 1, \ldots, k$. Therefore $\sigma_{\mathfrak{p}_i}(\sqrt{\mu}) = \sqrt{\mu}$ for $i = 1, \ldots, k$. The elements $\sigma_{\mathfrak{p}_1}, \ldots, \sigma_{\mathfrak{p}_k}$ form a basis for $\prod_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F)$. Hence if $\mathfrak{p}|\infty$, then $\sigma_{\mathfrak{p}}(\sqrt{\mu}) = \sqrt{\mu}$. Hence $\mu > 0$ at $\mathfrak{p}$ for all $\mathfrak{p}|\infty$ and therefore $\mu \in U \cap T$. We have shown that $\ker \Lambda = U \cap T$. Hence Λ induces a monomorphism $\Lambda' : U/U \cap T \to \prod_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F)$. By the previous inequality it follows that Λ' is an isomorphism.

We have the following

<u>Corollary 4.2.1.</u> Let $U = \langle \upsilon_1, \ldots, \upsilon_p \rangle$ be the multiplicative group generated by the cyclotomic units in F. Let T be the group of totally positive units in F. Then $U \cap T = U^2$ iff $G(E/F)$ has order 2^p and

$$G(E/F) = \bigoplus_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F).$$

Proof: Assume that $T \cap U = U^2$. Then $U/U \cap T = U/U^2$ has order 2^p by Theorem 2.5. Hence the group $\prod_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F)$ has p even invariants by Theorem 4.2. Therefore $\prod_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F)$ is direct. Since $|G(E/F)| \leq 2^p$ it follows that

$$G(E/F) = \bigoplus_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F)$$

and $|G(E/F)| = 2^p$.

Conversely, assume that $G(E/F)$ has order 2^p and

$$G(E/F) = \bigoplus_{\mathfrak{p}|\infty} G_{\mathfrak{p}}(E/F).$$

Then by Theorem 4.2, $U/U \cap T$ has order 2^p. But U^2 is a subgroup of $U \cap T$ and U/U^2 has order 2^p. Hence

$$U^2 = U \cap T.$$

<u>Corollary 4.2.2.</u> The homomorphism from the group U/U^2 to the group $G(E/F)$ which is defined by

$$\mu U^2 \to \prod_{p|\infty} \varphi_p(\mu) \quad , \quad \mu \in U,$$

is a monomorphism iff

$$U \cap T = U^2 .$$

Proof: Assume that the homomorphism $\mu U^2 \to \prod_{p|\infty} G_p(E/F)$ is a monomorphism, i.e. its kernel is exactly U^2. If $\mu \in U \cap T$, then $\varphi_p(\mu) = 1$ for every $p|\infty$. Hence if $\mu \in U \cap T$ then $\prod_{p|\infty} \varphi_p(\mu) = 1$. Hence $\mu \in U^2$. Hence $U \cap T \subseteq U^2$. In any case, $U^2 \subseteq U \cap T$, therefore $U \cap T = U^2$. Conversely assume that $U^2 = U \cap T$. Consider the homomorphism $\mu U^2 \to \prod_{p|\infty} \varphi_p(\mu)$. We shall show that its kernel is $U^2 = U \cap T$. By Corollary 4.2.1, $G(E/F)$ has order 2^p and

$$G(E/F) = \bigoplus_{p|\infty} G_p(E/F) .$$

By Theorem 4.1, φ_p is a homomorphism from F_p^* into $G_p(E/F)$ for each $p|\infty$. Therefore if $\mu \in U$ and

$$\prod_{p|\infty} \varphi_p(\mu) = 1$$

then $\varphi_p(\mu) = 1$ for each $p|\infty$. But then $\mu \in U \cap T$ by Lemma 4.5. Clearly if $\mu \in U \cap T$ then $\prod_{p|\infty} \varphi_p(\mu) = 1$. Hence $U \cap T = U^2$ is the kernel of

$$\mu U^2 \to \prod_{p|\infty} \varphi_p(\mu)$$

and therefore it is a monomorphism.

We can apply Lemma 4.7 to obtain

<u>Theorem 4.3.</u> Every totally positive element in U is a square in U iff the homomorphism $\Phi: U/U^2 \to G(E/F)$ from U/U^2 to $G(E/F)$ defined by

$$\mu U^2 \to \prod_{p|(2)} \varphi_p(\mu), \quad \mu \in U$$

is a monomorphism.

Proof: By Lemma 4.7, if μ is a unit in F, then

$$\Big(\prod_{p|\infty} \varphi_p(\mu)\Big) \cdot \Big(\prod_{p|(2)} \varphi_p(\mu)\Big) = 1.$$

Therefore the homomorphism $\Phi: U/U^2 \to G(E/F)$ is a monomorphism iff the homomorphism from U/U^2 to $G(E/F)$ defined by

$$\mu U^2 \to \prod_{p|\infty} \varphi_p(\mu) \qquad \mu \in U$$

is a monomorphism. The latter mapping is a monomorphism iff $U^2 = U \cap T$ by Corollary 4.2.2.

In order to use Theorem 4.3 we shall need more results about the reciprocity maps. First we prove

<u>Theorem 4.4.</u> Let p be a prime in F. Then

$$N(E/F, \boldsymbol{p}) = \bigcap_{i=1}^{p} N(F(\sqrt{v_i})/F, p).$$

Proof: The supplemental property of the reciprocity map is used. We have that

$$N(E/F,\mathfrak{p}) \subseteq \bigcap_{i=1}^{p} N(F(\sqrt{\upsilon_i})/F,\mathfrak{p})$$

by the transitivity of the norm. Let α be an element of $\bigcap_{i=1}^{p} N(F(\sqrt{\upsilon_i})/F,\mathfrak{p})$. Let $\varphi_{\mathfrak{p}}$ be the reciprocity map from $F^*_{\mathfrak{p}}$ to $G_{\mathfrak{p}}(E/F)$. Then $\alpha \in N(E/F,\mathfrak{p})$ iff $\varphi_{\mathfrak{p}}(\alpha) = 1$ by Theorem 4.1. For each $i = 1, \ldots, p$, let $\varphi^{(i)}_{\mathfrak{p}}$ be the reciprocity map from $F^*_{\mathfrak{p}}$ to $G_{\mathfrak{p}}(F(\sqrt{\upsilon_i})/F)$ given by Theorem 4.1. Then $\varphi^{(i)}_{\mathfrak{p}}(\alpha) = 1$ for $i = 1, \ldots, p$, because $\alpha \in \bigcap_{i=1}^{p} N(F(\sqrt{\upsilon_i})/F,\mathfrak{p})$. By the supplemental property of the reciprocity map, $\varphi^{(i)}_{\mathfrak{p}}(\alpha)$ is the restriction of $\varphi_{\mathfrak{p}}(\alpha)$ to the field $F(\sqrt{\upsilon_i})$, $i = 1, \ldots, p$. Hence $\varphi_{\mathfrak{p}}(\alpha)$ is an element of $G_{\mathfrak{p}}(E/F)$ which fixes every subfield $F(\sqrt{\upsilon_i})$ element wise. Therefore $\varphi_{\mathfrak{p}}(\alpha) = 1$. Therefore $\alpha \in N(E/F,\mathfrak{p})$.

Let K be a number field and let $\mathfrak{p}$ be a prime in K. Let α, β be elements of K. The <u>Hilbert symbol</u> (O'Meara [11], p.164) $(\alpha,\beta)_{\mathfrak{p}}$ at $\mathfrak{p}$ is defined by

$$(\alpha,\beta)_{\mathfrak{p}} = \begin{cases} 1 \text{ if there exist } \gamma, \delta \in K \text{ such that } \alpha\gamma^2 + \beta\delta^2 = 1 \\ -1 \text{ otherwise .} \end{cases}$$

Therefore $(\alpha,\beta)_{\mathfrak{p}} = 1$ iff $\alpha \in N(K(\sqrt{\beta})/K,\mathfrak{p})$. Hence we have

<u>Corollary 4.4.1.</u> Let $\mathfrak{p}$ be a prime in F. Let $\varphi_{\mathfrak{p}}$ be the reciprocity map $\varphi_{\mathfrak{p}}: F^*_{\mathfrak{p}} \to G_{\mathfrak{p}}(E/F)$ and let $\mu \in U$. Then $\varphi_{\mathfrak{p}}(\mu) = 1$ iff $(\mu,\upsilon_i)_{\mathfrak{p}} = 1$ for every $i = 1, \ldots, p$.

Proof: By Theorem 4.1, $\varphi_{\mathfrak{p}}(\mu) = 1$ iff $\mu \in N(E/F,\mathfrak{p})$. By Theorem 4.4, $\mu \in N(E/F,\mathfrak{p})$ iff $\mu \in N(F(\sqrt{\upsilon_i})/F,\mathfrak{p})$ for every $i = 1, \ldots, p$. Therefore $\varphi_{\mathfrak{p}}(\mu) = 1$ iff $(\mu,\upsilon_i)_{\mathfrak{p}} = (\upsilon_i,\mu)_{\mathfrak{p}} = 1$ for every $i = 1, \ldots, p$.

Chapter V

The Case when (2) is a Prime in F.

The object of this chapter is to apply the results of the previous chapter to the case when (2) is a prime in F.[1] The first part of this chapter is devoted to preliminary results on quadratic forms. These results along with some additional results of a computational nature are used to do some computations in the case $q = 7$. The results of the computation motivate the main results of the chapter. However, the proofs of the main results rely mainly on results of the previous chapters.

Assume henceforth that (2) is a prime in F, i.e. there exists only one prime $\mathfrak{p}$ in F such that $\mathfrak{p} \mid (2)$. Since (2) cannot ramify we write $(2) = \mathfrak{p}$. Then we have by Theorem 4.3 of the previous chapter that a necessary and sufficient condition for the totally positive units in U to be the squares of elements of U is for the homomorphism $\Phi : U/U^2 \to G(E/F)$ defined by

$$\mu U^2 \to \varphi_{(2)}(\mu)$$

to be a momomorphism. By Corollary 4.4.1, we have that $\varphi_{(2)}(\mu) = 1$ iff $(\mu, \upsilon_i)_{(2)} = 1$ for every $i = 1, \ldots, p$, where $(\cdot\,,\cdot)_{(2)}$ is the Hilbert symbol at (2) on F. For a given i, the symbol $(\mu, \upsilon_i)_{(2)} = 1$ if and only if the quadratic form $x^2 - \mu y^2$ represents υ_i in $F_{(2)}$, the completion of F at (2). Thus we are led to the study of quadratic forms over $F_{(2)}$. The field $F_{(2)}$ is Galois over $Q_{(2)}$, has the same degree p as F over Q, and every integral basis for F over Q determines an integral basis

---

[1] If p is a prime integer then (2) is a prime in F (see Weyl [16] p. 83).

for $F_{(2)}$ over $Q_{(2)}$ by means of the natural embedding of F into $F_{(2)}$ (see Weiss [15], p.159). We shall assume that F is a subfield of $F_{(2)}$.

We shall use the terminology of O'Meara [11]. In particular we call a field K a <u>local field</u> if K is complete at a discrete prime p and if the residue class field at p is finite. An element π in K is a <u>prime element</u> if its value at the prime p generates the value group at p. We write N_p for the order of the residue class field of K at p. The positive integer N_p is called the <u>absolute norm</u> of p.

<u>Theorem 5.1</u>. (Local Square Theorem). Let K be a local field at a prime p and let π be a prime element in K. Let α be an integer in K. Then there is an integer β in K such that

$$1 + 4\pi\alpha = (1 + 2\pi\beta)^2 .$$

Proof: See O'Meara [11], p.159.

<u>Theorem 5.2.</u> Let K be a local field at the prime p and let V be its group of units. Then

$$[K^*:K^{*2}] = 2[V:V^2] = 4(N_p)^{\mathrm{ord}_p 2} .$$

Proof: See O'Meara [11], p. 163.

We apply these theorems to the local field $F_{(2)}$.

<u>Theorem 5.3.</u> Let $V_{(2)}$ be the group of units in $F_{(2)}$. Let $\mu, \nu \in V_{(2)}$. Then there exists $\omega \in V_{(2)}$ such that $\mu \equiv \nu\omega^2 \bmod(8)$ iff $\mu \in \nu V_{(2)}^2$.

Proof: We apply Theorem 5.1 with $K = F_{(2)}$ and $\pi = 2$. Assume there exists $\omega \in V_{(2)}$ such that $\mu \equiv \nu\omega^2 \bmod(8)$. Then $\mu = \nu\omega^2 + 8\alpha$ for some integer α in $F_{(2)}$. Then $\mu = \nu\omega^2(1+8\alpha(\nu\omega^2)^{-1})$, and $\alpha(\nu\omega^2)^{-1}$ is an integer in $F_{(2)}$ because ν, ω are in $V_{(2)}$. Hence by Theorem 5.1, there exists an integer β in $F_{(2)}$ such that $1+8\alpha(\nu\omega^2)^{-1} = (1+4\beta)^2$. Therefore $\mu = \nu\omega^2(1+4\beta)^2$. Hence $\mu \in \nu V_{(2)}^2$. Conversely, if $\mu \in \nu V_{(2)}^2$ then there exists $\omega \in V_{(2)}$ such that $\mu = \nu\omega^2$. Hence $\mu \equiv \nu\omega^2 \mod (8)$.

Theorem 5.4. Let $V_{(2)}$ be the group of units in $F_{(2)}$. Let $\nu_1, \ldots, \nu_n$ be a complete set of coset representatives for $V_{(2)}/V_{(2)}^2$. Then $\nu_1, \ldots, \nu_n, 2\nu_1, \ldots, 2\nu_n$ is a complete set of coset representatives for $F_{(2)}^*/F_{(2)}^{*2}$.

Proof: Let $\alpha \in F_{(2)}^*$. Then we can write $\alpha = 2^{\operatorname{ord}_{(2)}\alpha} \cdot \alpha'$ where α' is a unit in $F_{(2)}$. But $\alpha' \in \nu_i V_{(2)}^2$ for some i. If $\operatorname{ord}_{(2)}\alpha$ is even then $\alpha \in \nu_i F_{(2)}^{*2}$ and if $\operatorname{ord}_{(2)}\alpha$ is odd then $\alpha \in 2\nu_i F_{(2)}^{*2}$. Therefore $\nu_1, \ldots, \nu_n, 2\nu_1, \ldots, 2\nu_n$ is a set of coset representatives for $F_{(2)}^*/F_{(2)}^{*2}$. By Theorem 5.2 they represent distinct cosets of $F_{(2)}^{*2}$.

Theorem 5.5. The order of the group $F_{(2)}^*/F_{(2)}^{*2}$ is 2^{p+2}.

Proof: Apply Theorem 5.2. The absolute norm of p is 2^p and $\operatorname{ord}_{(2)}2=1$. Hence

$$\left[F_{(2)}^* : F_{(2)}^{*2}\right] = 4(2^p) = 2^{p+2}.$$

We shall now determine a set of coset representatives for $V_{(2)}/V_{(2)}^2$. Let $\overline{F}_{(2)}$ denote the residue class field of $F_{(2)}$. Let $O_{(2)}$ denote the ring of integers in $F_{(2)}$. Let A be a fixed set of representatives of $\overline{F}_{(2)}$ in $O_{(2)}$.

Theorem 5.6. Let p be odd and let ν be a unit in $F_{(2)}$. Then there exist uniquely $\alpha \in A$, $\beta = 0,1$ such that

$$\nu \in (1 + 2\alpha + 4\beta)\, V_{(2)}^2 .$$

Proof: By Theorem 5.3 it is sufficient to show that there exist uniquely $\alpha \in A, \beta = 0$ or 1 such that

$$\nu \equiv (1 + 2\alpha + 4\beta)\, \omega^2 \mod (8)$$

for some $\omega \in V_{(2)}$. We have that ν is a unit, therefore there exists a unit γ such that $\nu\gamma = 1$. The mapping $\delta \rightarrow \delta^2$ is an automorphism of $\overline{F}_{(2)}$, hence there exists $\delta \in V_{(2)}$ such that $\delta^2 \equiv \gamma \bmod (2)$. Then $\nu \delta^2 \equiv 1 \bmod (2)$. Then there exists $\alpha \in A$ such that $\nu\delta^2 \equiv 1 + 2\alpha \bmod (4)$. Moreover, α is uniquely determined by the class of ν in $V_{(2)}/V_{(2)}^2$. For if there exists $\rho \in V_{(2)}$ such that

$$(1 + 2\alpha)\rho^2 \equiv 1 + 2\alpha' \bmod (4),\ \alpha, \alpha' \in A,$$

then

$$\rho^2 \equiv 1 \bmod (2)\ .$$

Hence $\rho \equiv 1 \bmod (2)$ and $\rho = 1 + 2\rho'$, $\rho' \in O_{(2)}$. Then

$$(1 + 2\alpha)\rho^2 \equiv (1 + 2\alpha)\,(1 + 2\rho')^2 \equiv 1 + 2\alpha \bmod (4)\,.$$

Hence $1 + 2\alpha \equiv 1 + 2\alpha' \bmod (4)$. Then $\alpha \equiv \alpha' \bmod (2)$. But $\alpha, \alpha' \in A$, hence $\alpha = \alpha'$. By Theorems 5.2 and 5.5 the order of $V_{(2)}/V_{(2)}^2$ is 2^{p+1}. The set A has 2^p elements. Therefore, in order to complete the proof, it is sufficient to show that if $\alpha \in A$ and $\mu \in V_{(2)}$ then it cannot happen that

$$(1 + 2\alpha)\mu^2 \equiv (1 + 2\alpha + 4) \bmod (8).$$

Suppose it does happen. Then $\mu \equiv 1 \bmod (2)$. Hence $\mu = 1 + 2\mu_1, \mu_1 \in O_{(2)}$. Hence $(1 + 2\alpha)\mu^2 \equiv (1 + 2\alpha)\,(1 + 2\mu_1)^2 \equiv (1 + 2\alpha)\,(1 + 4(\mu_1 + \mu_1^2)) \equiv 1 + 2\alpha + 4\mu_1 + 4\mu_1^2 \bmod (8)$. Then we have

$$1 + 2\alpha + 4\mu_1 + 4\mu_1^2 \equiv 1 + 2\alpha + 4 \bmod (8)\ .$$

Hence

$$\mu_1^2 + \mu_1 + 1 \equiv 0 \bmod (2)\,.$$

This last relation would imply that $\overline{F}_{(2)}$ has a subfield of degree 2 over $GF(2)$, which contradicts the assumption that p is odd, since $\overline{F}_{(2)}$ has degree p over $GF(2)$. (O'Meara [11], p. 23).

For each $i = 1, \ldots, p$ let $\theta_i = -(\zeta^i + \zeta^{-i})$ where $F = Q(\zeta + \zeta^{-1})$. The numbers $\theta_1, \ldots, \theta_p$ are integers in F which give a Z-basis for all the integers in F. Therefore the set

$$A = \{\alpha \mid \alpha = \sum_{k=1}^{p} \alpha_k \theta_k, \alpha_k \in \{0,1\}\}$$

is a set of representatives for the residue class field $\overline{F}$ of F at (2). By O'Meara [11], p. 23 it follows that the set A is a set of representatives in $O_{(2)}$ for the residue class field of $F_{(2)}$. We are interested in finding the representatives for the cosets in $V_{(2)}/V^2_{(2)}$ which contain the units $\upsilon_1, \ldots, \upsilon_p$ because this information will enable us to compute the Hilbert symbol $(\mu, \upsilon_i)_{(2)}$ for $\mu \in U$. We shall develop some relations which will simplify the calculation of representatives. The relations are not used in the proof of the succeeding theorems but will be used in an example which motivates the succeeding theorems.

Let $k \in Z$. Then there exists uniquely $i \in Z$ such that $0 \leq i \leq p$ and $k \equiv i$ or $k \equiv -i \mod q$. Let $\langle\langle k \rangle\rangle$ denote this i.

<u>Lemma 5.1.</u> $\theta_1 + \cdots + \theta_p = 1$.

Proof: The number ζ satisfies $1 + \zeta + \zeta^2 + \cdots + \zeta^{q-1} = 0$. Hence $-\zeta - \zeta^{-1} - \zeta^2 - \zeta^{-2} - \cdots - \zeta^p - \zeta^{-p} = 1$. Hence $\theta_1 + \cdots + \theta_p = 1$.

<u>Lemma 5.2.</u> Let $1 \leq i, j \leq p$, $i \neq j$. Then

$$\theta_i \theta_i = 2 - \theta_{\langle\langle 2i \rangle\rangle}$$

and

$$\theta_i \theta_j = -\theta_{\langle\langle i+j \rangle\rangle} - \theta_{\langle\langle i-j \rangle\rangle} .$$

Proof: $-(\zeta^{i}+\zeta^{-i})(-(\zeta^{i}+\zeta^{-i})) = \zeta^{2i}+1+\zeta^{-2i}+1 = 2+(\zeta^{2i}+\zeta^{-2i}) = 2-\theta_{\langle\langle 2i\rangle\rangle}$.

$-(\zeta^{i}+\zeta^{-i})(-(\zeta^{j}+\zeta^{-j})) = \zeta^{i+j}+\zeta^{i-j}+\zeta^{-i+j}+\zeta^{-i-j} = \zeta^{i+j}+\zeta^{-i-j}+\zeta^{i-j}+\zeta^{-(i-j)}$

$= -\theta_{\langle\langle i+j\rangle\rangle} - \theta_{\langle\langle i-j\rangle\rangle}$.

The use of these lemmas is illustrated in the case $q = 7$:

Let $\alpha = a_1\theta_1 + a_2\theta_2 + a_3\theta_3$, $\beta = b_1\theta_1 + b_2\theta_2 + b_3\theta_3$.

Then,

$$\begin{aligned}
\alpha\beta &= a_1 b_1 \theta_1\theta_1 + a_1 b_2 \theta_1\theta_2 + a_1 b_3 \theta_1\theta_3 \\
&\quad + a_2 b_1 \theta_2\theta_1 + a_2 b_2 \theta_2\theta_2 + a_2 b_3 \theta_2\theta_3 \\
&\quad + a_3 b_1 \theta_3\theta_1 + a_3 b_2 \theta_3\theta_2 + a_3 b_3 \theta_3\theta_3 \\
&= a_1 b_1 (2-\theta_2) + a_1 b_2(-\theta_1-\theta_3) + a_1 b_3(-\theta_2-\theta_3) \\
&\quad + a_2 b_1(-\theta_1-\theta_3) + a_2 b_2 (2-\theta_3) + a_2 b_3(-\theta_1-\theta_2) \\
&\quad + a_3 b_1(-\theta_2-\theta_3) + a_3 b_2(-\theta_1-\theta_2) + a_3 b_3(2-\theta_1) \\
&= 2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 \\
&\quad + (-a_1 b_2 - a_2 b_1 - a_2 b_3 - a_3 b_2 - a_3 b_3)\theta_1 \\
&\quad + (-a_1 b_1 - a_1 b_3 - a_2 b_3 - a_3 b_1 - a_3 b_2)\theta_2 \\
&\quad + (-a_1 b_2 - a_1 b_3 - a_2 b_1 - a_2 b_2 - a_3 b_1)\theta_3 .
\end{aligned}$$

But

$$1 = \theta_1 + \theta_2 + \theta_3 .$$

Therefore

$$\begin{aligned}
\alpha\beta &= (2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 - a_1 b_2 - a_2 b_1 - a_2 b_3 - a_3 b_2 - a_3 b_3)\theta_1 \\
&\quad + (2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 - a_1 b_1 - a_1 b_3 - a_2 b_3 - a_3 b_1 - a_3 b_2)\theta_2 \\
&\quad + (2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 - a_1 b_2 - a_1 b_3 - a_2 b_1 - a_2 b_2 - a_3 b_1)\theta_3 .
\end{aligned}$$

This equation reduces to

$$\begin{aligned}
\alpha\beta &= ((a_1-a_2)(b_1-b_2) + (a_2-a_3)(b_2-b_3) + a_1 b_1)\theta_1 \\
&\quad + ((a_1-a_3)(b_1-b_3) + (a_2-a_3)(b_2-b_3) + a_2 b_2)\theta_2 \\
&\quad + ((a_1-a_3)(b_1-b_3) + (a_1-a_2)(b_1-b_2) + a_3 b_3)\theta_3 .
\end{aligned}$$

In particular

$$\alpha^2 = ((a_1 - a_2)^2 + (a_2 - a_3)^2 + a_1^2)\,\theta_1$$
$$+ ((a_1 - a_3)^2 + (a_2 - a_3)^2 + a_2^2)\,\theta_2$$
$$+ ((a_1 - a_3)^2 + (a_1 - a_2)^2 + a_3^2)\,\theta_3 .$$

In fact these relations hold in general.

Lemma 5.3. Let a_i, b_i, $i = 1, \ldots, p$ be arbitrary. Then

$$\left(\sum_{k=1}^{p} a_k\theta_k\right)\left(\sum_{k=1}^{p} b_k\theta_k\right) = \sum_{k=1}^{p} c_k\theta_k$$

where,

$$c_k = a_kb_k + \sum_{(i,j)\in C_k} (a_i - a_j)(b_i - b_j)$$

and

$$C_k = \{(i,j) \mid 1 \leq i < j \leq p,\ \langle\langle i+j\rangle\rangle = k \text{ or } \langle\langle i-j\rangle\rangle = k\}.$$

Proof:

$$\left(\sum_{i=1}^{p} a_i\theta_i\right)\left(\sum_{j=1}^{p} b_j\theta_j\right) = \sum_{j=1}^{p}\sum_{i=1}^{p} a_ib_j\theta_i\theta_j$$

$$= \sum_{j=1}^{p}\left(\sum_{\substack{i=1\\ i\neq j}}^{p} a_ib_j\left(-\theta_{\langle\langle i+j\rangle\rangle} - \theta_{\langle\langle i-j\rangle\rangle}\right) + \left(2 - \theta_{\langle\langle 2j\rangle\rangle}\right)a_jb_j\right)$$

and $2 = 2\theta_1 + 2\theta_2 + \cdots + 2\theta_p$. Hence the coefficient of θ_k above is

$$-\sum_{j=1}^{p}\sum_{\substack{i=1\\ i\neq j,\ \langle\langle i+j\rangle\rangle = k\\ \text{or } \langle\langle i-j\rangle\rangle = k}}^{p} a_ib_j + \sum_{j=1}^{p} 2a_jb_j - a_\ell b_\ell$$

where

$$\langle\langle 2\ell\rangle\rangle = k, \text{ and } 1 \leq \ell \leq p.$$

Consider

$$c_k = a_kb_k + \sum_{(i,j)\in C_k} (a_i - a_j)(b_i - b_j) .$$

For any $1 \leq i,j \leq p$, we have

$$(a_i - a_j)(b_i - b_j) = a_i b_i - a_i b_j - a_j b_i + a_j b_j .$$

Also

$$\sum_{(i,j) \in C_k} -a_i b_j - a_j b_i = - \sum_{j=1}^{p} \sum_{\substack{i=1 \\ i \neq j \ \langle\langle i+j \rangle\rangle = k \\ \text{or } \langle\langle i-j \rangle\rangle = k}}^{p} a_i b_j .$$

Fix k and ℓ, where $1 \leq \ell \leq p$ and $\langle\langle 2\ell \rangle\rangle = k$. The proof will be complete if it can be shown that

$$(*) \qquad \sum_{j=1}^{p} 2a_j b_j - a_\ell b_\ell = a_k b_k + \sum_{(i,j) \in C_k} (a_i b_i + a_j b_j) .$$

Write $C_k = \{(i_t, j_t) \mid t = 1, \ldots, r\}$ where r is the number of elements in C_k. It is asserted that

1) If $1 \leq m \leq p$ and $m \neq k, \ell$, then exactly one of the following occur. There exist exactly two integers f, g, $1 \leq f,g \leq r$ such that

i) $m = i_g = i_f$

ii) $m = j_g = j_f$

iii) $m = i_g = j_f$.

2) If $1 \leq m \leq p$ and $m = k$ or ℓ then exactly one of the following occur. There exists exactly one integer g, $1 \leq g \leq r$ such that

i) $m = i_g$

ii) $m = j_g$.

If statements 1) and 2) hold, then $(*)$ follows by comparing the terms of each side. We prove 1) by proving

3) Given any $m \neq k, \ell$ there exist $1 \leq n, n' \leq p$ such that $n \neq n'$, $m \neq n, n'$ and $\langle\langle m + k \rangle\rangle = n$, $\langle\langle m - k \rangle\rangle = n'$. Note n and n' are unique

if they exist. Let $n = \langle\langle m+k \rangle\rangle$ and $n' = \langle\langle m-k \rangle\rangle$. If $n = n'$, then $m+k \equiv \pm (m-k) \bmod q$, so either $k \equiv -k$ or $2m \equiv 0$, which is a contradiction to assumption. If $m = n$, then $m+k \equiv \pm m$, so either $2m \equiv -k$ whence $m = \ell$, or $k = 0$, both of which contradict the assumption. If $m = n'$ then $m-k \equiv \pm m$, so either $2m \equiv k$ whence $m = \ell$, or $-k \equiv 0$, again contradictions. Therefore 3) holds. Given m as in 1) choose n, n' as in 3). Then either

i) $m < n$ and $m < n'$, hence $(m,n), (m,n') \in C_k$

or ii) $m > n$ and $m < n'$, hence $(n,m), (m,n') \in C_k$

or iii) $m < n$ and $m > n'$, hence $(m,n), (n',m) \in C_k$

or iv) $m > n$ and $m > n'$, hence $(n,m), (n',m) \in C_k$.

But this proves 1). We prove 2) directly. If $m = k$ there exists $1 \leqslant n \leqslant p$ such that $k+k \equiv \pm n \bmod q$. Either i) $m < n$ or ii) $m > n$. Hence 2) holds for $m = k$. If $m = \ell$, then either

a) $\ell + \ell \equiv + k \bmod q$, whence $\ell - k \equiv -\ell$, and hence there exists n, $1 \leqslant n \leqslant p$ such that $\ell + k \equiv \pm n$; whence either i) $m < n$ or ii) $m > n$, or b) $\ell + \ell \equiv -k \bmod q$, whence $\ell + k \equiv -\ell$ and hence there exists n, $1 \leqslant n \leqslant p$ such that $\ell - k \equiv \pm n$; whence either i) $m < n$ or ii) $m > n$. This proves 2).

Suppose again that $q = 7$. In this case the coset representatives for $V_{(2)}/V_{(2)}^2$ are

$$\begin{array}{ll}
1 & 1+4 \\
1+2\theta_1 & 1+2\theta_1+4 \\
1+2\theta_2 & 1+2\theta_2+4 \\
1+2\theta_3 & 1+2\theta_3+4 \\
1+2(\theta_1+\theta_2) & 1+2(\theta_1+\theta_2)+4 \\
1+2(\theta_2+\theta_3) & 1+2(\theta_2+\theta_3)+4 \\
1+2(\theta_1+\theta_3) & 1+2(\theta_1+\theta_3)+4 \\
1+2(\theta_1+\theta_2+\theta_3) & 1+2(\theta_1+\theta_2+\theta_3)+4 \,.
\end{array}$$

We calculate the representatives for the class containing

$$\upsilon_1 = -1, \quad \upsilon_2 = (\zeta^2-\zeta^{-2})/(\zeta-\zeta^{-1}), \quad \upsilon_3 = (\zeta^3-\zeta^{-3})/(\zeta-\zeta^{-1})$$

where ζ is a primitive 7th root of unity. We have, $\upsilon_1 = -1 \equiv 7 \equiv 1+2+4 \bmod(8)$. Hence $\upsilon_1 \equiv 1+2(\theta_1+\theta_2+\theta_3)+4 \bmod(8)$. Hence the representative for υ_1 is $1+2(\theta_1+\theta_2+\theta_3)+4$, by Theorem 5.3.

We have $\upsilon_2 = (\zeta^2-\zeta^{-2})/(\zeta-\zeta^{-1}) = \zeta+\zeta^{-1} = -\theta_1$. By Lemma 5.3,

$$\begin{aligned}
(a_1\theta_1+a_2\theta_2+a_3\theta_3)(-\theta_1) = {} & ((a_1-a_2)(-1)+a_1)\theta_1 \\
& + (a_1-a_3)(-1)\theta_2 \\
& + ((a_1-a_3)(-1)+(a_1-a_2)(-1))\theta_3 \\
\equiv {} & a_2\theta_1+(a_1-a_3)\theta_2+(a_2-a_3)\theta_3 \bmod(2).
\end{aligned}$$

Therefore

$$(\theta_1+\theta_2)(-\theta_1) \equiv \theta_1+\theta_2+\theta_3 \equiv 1 \bmod(2).$$

Again by Lemma 5.3, $(a_1\theta_1+a_2\theta_2+a_3\theta_3)^2 \equiv \theta_1+\theta_2 \bmod(2)$

implies $\qquad a_3\theta_1+a_1\theta_2+a_2\theta_3 \equiv \theta_1+\theta_2 \bmod(2)$.

Hence $a_3 = a_1 = 1$, $a_2 = 0$. Therefore if we multiply $-\theta_1$ by the square of a unit congruent to $\theta_1+\theta_3 \bmod(2)$, then the result will be congruent to $1 \bmod(2)$. We have $(\theta_1+\theta_3+2(b_1\theta_1+b_2\theta_2+b_3\theta_3))^2 \equiv$

$\theta_1 + \theta_2 + 2(\theta_1 + \theta_3) + 4((b_1 + b_2 + b_3)\,\theta_1 + (b_1 + b_3)\,\theta_3) \bmod (8)$. Also,

$-\theta_1\ (\theta_1 + \theta_2 + 2(\theta_1 + \theta_3) + 4((b_1 + b_2 + b_3)\,\theta_1 + (b_1 + b_3)\,\theta_3)$

$\equiv \theta_1 + \theta_2 + \theta_3 + 2(\theta_1 + \theta_2) + 4((b_1 + b_2 + b_3)\,\theta_1 + (1 + b_1 + b_3)\,\theta_2) + 4(1 + b_2)\theta_3 \bmod (8)$.

Let $b_2 = b_3 = 1$, $b_1 = 0$. Then we have that

$$-\theta_1\ (\theta_1 + \theta_3 + 2(\theta_2 + \theta_3))^2 \equiv 1 + 2(\theta_1 + \theta_2) \bmod (8).$$

Therefore the class representative of υ_2 is $1 + 2(\theta_1 + \theta_2)$.

$$\upsilon_3 = (\zeta^3 - \zeta^{-3})/(\zeta - \zeta^{-1}) = \zeta(\zeta^6 - 1)/\zeta^3(\zeta^2 - 1) = \zeta^{-2}(\zeta^4 + \zeta^2 + \zeta^0)$$

$$= \zeta^2 + 1 + \zeta^{-2} = 1 - \theta_2 = \theta_1 + \theta_3 .$$

Using the method shown in detail above we find that

$$(\theta_1 + \theta_3)\,(\theta_2 + 2\theta_1)^2 \equiv 1 + 2\theta_2 + 4 \bmod (8) .$$

Therefore the coset representative of υ_3 is $1 + 2\theta_2 + 4$. We write $\alpha \sim \beta$ if $\alpha \in \beta V_{(2)}^2$. Then we have

$$\upsilon_1 \sim 1 + 2(\theta_1 + \theta_2 + \theta_3) + 4$$

$$\upsilon_2 \sim 1 + 2(\theta_1 + \theta_2)$$

$$\upsilon_3 \sim 1 + 2\theta_2 + 4 .$$

Additional calculation will show that

$$\upsilon_1\upsilon_2 \sim 1 + 2\theta_3 + 4 \qquad 3\upsilon_1\upsilon_2 \sim 1 + 2(\theta_1 + \theta_2) + 4$$

$$\upsilon_1\upsilon_3 \sim 1 + 2(\theta_1 + \theta_3) \qquad 3\upsilon_1\upsilon_3 \sim 1 + 2\theta_2$$

$$\upsilon_2\upsilon_3 \sim 1 + 2\theta_1 + 4 \qquad 3\upsilon_2\upsilon_3 \sim 1 + 2(\theta_2 + \theta_3) + 4$$

$$\upsilon_1\upsilon_2\upsilon_3 \sim 1 + 2(\theta_2 + \theta_3) \qquad 3\upsilon_1\upsilon_2\upsilon_3 \sim 1 + 2\theta_1 \ .$$

Also,

$$3\upsilon_1 \sim 1 + 4 \qquad 3\upsilon_3 \sim 1 + 2(\theta_1 + \theta_3) + 4$$

$$3\upsilon_2 \sim 1 + 2\theta_3 \qquad 3 \sim 1 + 2(\theta_1 + \theta_2 + \theta_3) \ .$$

Note that the cosets containing $\upsilon_1, \upsilon_2, \upsilon_3$, and 3 generate the entire group. We shall show that this situation is related to the distribution of signs. First we shall need the following

Lemma 5.4. Let p be odd. Let k be a rational (2)-adic number and let α be an element of $F_{(2)}$. The quadratic form $x^2 - ky^2$ represents α in $F_{(2)}$ iff the form $x^2 - ky^2$ represents $N_{F_{(2)}/Q_{(2)}}(\alpha)$ in $Q_{(2)}$.

Proof: Assume that there exist $\gamma, \delta \in F_{(2)}$ such that $\gamma^2 - k\delta^2 = \alpha$. If k is a square in $F_{(2)}$ then it is a square in $Q_{(2)}$. Hence $x^2 - ky^2$ represents all of $Q_{(2)}$ if k is a square in $F_{(2)}$. Assume then that k is not a square in $F_{(2)}$. The extension $F_{(2)}(\sqrt{k})$ is Galois over $Q_{(2)}$. Hence

$$N_{F_{(2)}(\sqrt{k})/Q_{(2)}(\sqrt{k})}(\gamma + \delta\sqrt{k}) = \gamma' + \delta'\sqrt{k}$$

where γ', δ' are elements in $Q_{(2)}$. Then it follows from the transitivity of the norm that

$$\gamma'^2 - \delta'^2 k = N_{F_{(2)}/Q_{(2)}}(\alpha) .$$

Hence $x^2 - ky^2$ represents $N_{F_{(2)}/Q_{(2)}}(\alpha)$ in $Q_{(2)}$. Conversely, assume that there exist g, d in $Q_{(2)}$ such that $g^2 - kd^2 = N_{F_{(2)}/Q_{(2)}}(\alpha)$. Given $\sigma \in G(F_{(2)}/Q_{(2)})$, the form $x^2 - ky^2$ represents α in $F_{(2)}$ iff it represents $\sigma(\alpha)$ in $F_{(2)}$. That is, $(k, \alpha)_{(2)} = 1$ iff $(k, \sigma(\alpha))_{(2)} = 1$. But the Hilbert symbol is multiplicative, i.e. $(k, \alpha\beta)_{(2)} = (k, \alpha)_{(2)} \cdot (k, \beta)_{(2)}$ (O'Meara [11], p. 166.). Hence if $(k, \alpha)_{(2)} = -1$, then

$$(k, N_{F_{(2)}/Q_{(2)}}(\alpha))_{(2)} = \prod_{\sigma \in G(F_{(2)}/Q_{(2)})} (k, \sigma(\alpha))_{(2)} = -1$$

because $G(F_{(2)}/Q_{(2)})$ has order p which is odd by assumption. But this is a contradiction. Therefore $(k, \alpha)_{(2)} = 1$, i.e. $x^2 - ky^2$ represents α in $F_{(2)}$.

Theorem 5.7. Let p be odd. Then

$$F_{(2)}^{2} \cap U = U^{2} \text{ iff } V_{(2)}/V_{(2)}^{2} = \langle \upsilon_1 V_{(2)}^{2}\rangle \oplus \cdots \oplus \langle \upsilon_p V_{(2)}^{2}\rangle \oplus \langle 3V_{(2)}^{2}\rangle .$$

Proof: Assume that $F_{(2)}^{2} \cap U = U^2$. Suppose that $\upsilon_1^{e_1}\upsilon_2^{e_2}\cdots\upsilon_p^{e_p}3^{e_0} \in V_{(2)}^{2}$ where $e_0, e_1, \ldots, e_p$ are in Z. Since p is odd by assumption, the degree of $F_{(2)}$ over $Q_{(2)}$ is odd, therefore we conclude by applying $N_{F_{(2)}/Q_{(2)}}$ that $+3^{e_0}$ or $-3^{e_0} \in Q_{(2)}^{2}$. Hence $e_0 \equiv 0 \bmod(2)$. Therefore assume that $\upsilon_1^{e_1}\upsilon_2^{e_2}\cdots\upsilon_p^{e_p} \in V_{(2)}^{2}$. Then $\upsilon_1^{e_1}\cdots\upsilon_p^{e_p} \in F_{(2)}^{2} \cap U = U^2$. But $\upsilon_1^{e_1}\cdots\upsilon_p^{e_p} \in U^2$ implies that $e_i \equiv 0 \bmod(2)$ for $i = 1, \ldots, p$. By Theorems 5.2 and 5.5, the order of $V_{(2)}/V_{(2)}^{2}$ is 2^{p+1}. Hence $V_{(2)}/V_{(2)}^{2} = \langle \upsilon_1 V_{(2)}^{2}\rangle \oplus \cdots \oplus \langle \upsilon_p V_{(2)}^{2}\rangle \oplus \langle 3V_{(2)}^{2}\rangle$. Conversely, assume that $V_{(2)}/V_{(2)}^{2} = \langle \upsilon_1 V_{(2)}^{2}\rangle \oplus \cdots \oplus \langle \upsilon_p V_{(2)}^{2}\rangle \oplus \langle 3V_{(2)}^{2}\rangle$. Clearly $U^2 \subseteq F_{(2)}^{2} \cap U$. If $\upsilon = \upsilon_1^{e_1}\cdots\upsilon_p^{e_p} \in F_{(2)}^{2} \cap U$, then $\upsilon \in V_{(2)}^{2}$. Hence by assumption $e_i \equiv 0 \bmod(2)$ for $i = 1, \ldots, p$. Therefore $\upsilon \in U^2$. Hence $U^2 = F_{(2)}^{2} \cap U$.

Theorem 5.8. Let p be odd. The mapping $\Phi: U/U^2 \to G(E/F)$ defined by

$$\mu U^2 \to \varphi_{(2)}(\mu) \qquad \mu \in U$$

is a monomorphism iff

$$F_{(2)}^{2} \cap U = U^2 .$$

Proof: Assume that the mapping $\Phi: U/U^2 \to G(E/F)$ is a monomorphism. If $\alpha \in F_{(2)}^{2} \cap U$, then $\varphi_{(2)}(\alpha) = 1$. Hence $\alpha \in U^2$ by the assumption. Therefore $U^2 = F_{(2)}^{2} \cap U$. Conversely, assume that $F_{(2)}^{2} \cap U = U^2$. If $\upsilon \in U$ and $\varphi_{(2)}(\upsilon) = 1$, then $(\upsilon, \upsilon_i)_{(2)} = 1$ for $i = 1, \ldots, p$, by Corollary 4.4.1. In particular, $(\upsilon, \upsilon_1)_{(2)} = 1$. Hence $x^2 + y^2$ represents υ in $F_{(2)}$. Therefore $x^2 + y^2$ represents $N_{F_{(2)}/Q_{(2)}}(\upsilon)$ in $Q_{(2)}$ by Lemma 5.4. But

$\upsilon \in U$ implies that $N_{F_{(2)}/Q_{(2)}}(\upsilon) = +1$ or -1. Therefore $N_{F_{(2)}/Q_{(2)}}(\upsilon) = +1$ (see Borevich and Shafarevich [5], p. 54). Then $x^2 - N_{F_{(2)}/Q_{(2)}}(\upsilon)y^2 = x^2 - y^2$ represents 3 in $Q_{(2)}$, therefore $x^2 - 3y^2$ represents $N_{F_{(2)}/Q_{(2)}}(\upsilon)$ in $Q_{(2)}$, whence $x^2 - 3y^2$ represents υ in $F_{(2)}$ by Lemma 5.4. Therefore $(\upsilon, 3)_{(2)} = 1$. Similarly $(\upsilon, 2)_{(2)} = 1$. Then by Theorem 5.7, the assumption $F^2_{(2)} \cap U = U^2$, and the multiplicativity of the Hilbert symbol, it follows that $(\upsilon, \alpha)_{(2)} = 1$ for all α in $F^*_{(2)}$. Hence $\upsilon \in F^2_{(2)}$ (see O'Meara [11], p. 166). Therefore $\upsilon \in U^2$. Hence $\Phi : U/U^2 \to G(E/F)$ is a monomorphism.

<u>Corollary 5.8.1.</u> Let p be odd. The following statements are equivalent.

1) $U \cap F^2_{(2)} = U^2$

2) $U \cap T = U^2$

3) $V_{(2)}/V^2_{(2)} = \langle \upsilon_1 V^2_{(2)} \rangle \oplus \cdots \oplus \langle \upsilon_p V^2_{(2)} \rangle \oplus \langle 3 V^2_{(2)} \rangle$

4) $G(E/F)$ has order 2^p and $G(E/F) = \bigoplus_{p|\infty} G_p(E/F)$

5) The matrix M_q of cyclotomic signatures is non-singular

6) $\Phi : U/U^2 \to G(E/F)$ is a monomorphism.

Proof:

1) $\Longleftrightarrow$ 6) : Theorem 5.8

1) $\Longleftrightarrow$ 3) : Theorem 5.7

2) $\Longleftrightarrow$ 6) : Theorem 4.3

2) $\Longleftrightarrow$ 4) : Corollary 4.2.1

2) $\Longleftrightarrow$ 5) : Corollary 2.6.1

Appendix I - Tables

For each prime q, $5 \leq q \leq 929$, the rank of the matrix of cyclotomic signatures was calculated on an IBM 7094 computer. The rank computation was actually made on the matrix M_q' defined in Chapter II. Two programs were written to perform this computation. The first program was written in Fortran IV without bit-processing. Hence this program could only be executed for $5 \leq q \leq 211$ because for greater q the core memory would be exceeded. The second program was written in IBMAP in order to take advantage of bit-processing and the binary nature of the computation. The results from the first program were used to check the initial results which were obtained using the second program. Although the Fortran program consisted of about 50 statements, the IBMAP program consisted of 640 IBMAP instructions. Using the IBMAP program, the computer performed the computation for $5 \leq q \leq 929$. The total time for the Fortran run for $5 \leq q \leq 211$ was 5 minutes, 5 seconds. The total time for the IBMAP run for $5 \leq q \leq 541$ was 23 minutes, 4 seconds. The total time for the IBMAP run for $547 \leq q \leq 739$ was 45 minutes, 51 seconds. The total time for the IBMAP run for $743 \leq q \leq 929$ was 1 hour, 32 minutes, 3 seconds. The following table contains the results. The first column contains the value of the prime q. The second column contains the value of $p = (q-1)/2$. The third column contains the rank of the matrix M_q of cyclotomic signatures. The fourth column contains the prime factorization of p if p is not a prime, and the index of 2 mod p if p is prime.

The Rank of the Matrix M_q

3	1	1	1
5	2	2	1
7	3	3	1
11	5	5	1
13	6	6	$2 \cdot 3$
17	8	8	2^3
19	9	9	3^2
23	11	11	1
29	14	11	$2 \cdot 7$
31	15	15	$3 \cdot 5$
37	18	18	$2 \cdot 3^2$
41	20	20	$2^2 \cdot 5$
43	21	21	$3 \cdot 7$
47	23	23	2
53	26	26	$2 \cdot 13$
59	29	29	1
61	30	30	$2 \cdot 3 \cdot 5$
67	33	33	$3 \cdot 11$
71	35	35	$5 \cdot 7$
73	36	36	$2^2 \cdot 3^2$
79	39	39	$3 \cdot 13$
83	41	41	2
89	44	44	$2^2 \cdot 11$
97	48	48	$2^4 \cdot 3$
101	50	50	$2 \cdot 5^2$
103	51	51	$3 \cdot 17$
107	53	53	1
109	54	54	$2 \cdot 3^3$
113	56	53	$2^3 \cdot 7$
127	63	63	$3^2 \cdot 7$
131	65	65	$5 \cdot 13$
137	68	68	$2^2 \cdot 17$
139	69	69	$3 \cdot 23$

149	74	74	$2 \cdot 37$
151	75	75	$3 \cdot 5^2$
157	78	78	$2 \cdot 3 \cdot 13$
163	81	79	3^4
167	83	83	1
173	86	86	$2 \cdot 43$
179	89	89	8
181	90	90	$2 \cdot 3^2 \cdot 5$
191	95	95	$5 \cdot 19$
193	96	96	$2^5 \cdot 3$
197	98	95	$2 \cdot 7^2$
199	99	99	$3^2 \cdot 11$
211	105	105	$3 \cdot 5 \cdot 7$
223	111	111	$2 \cdot 5 \cdot 11$
227	113	113	4
229	114	114	$2 \cdot 3 \cdot 19$
233	116	116	$2^2 \cdot 29$
239	119	116	$7 \cdot 17$
241	120	120	$2^3 \cdot 3 \cdot 5$
251	125	125	5^3
257	128	128	2^7
263	131	131	1
269	134	134	$2 \cdot 67$
271	135	135	$3^3 \cdot 5$
277	138	134	$2 \cdot 3 \cdot 23$
281	140	140	$2^2 \cdot 5 \cdot 7$
283	141	141	$3 \cdot 47$
293	146	146	$2 \cdot 73$
307	153	153	$3^2 \cdot 17$
311	155	145	$5 \cdot 31$
313	156	156	$2^2 \cdot 3 \cdot 13$
317	158	158	$2 \cdot 79$
331	165	165	$3 \cdot 5 \cdot 11$
337	168	162	$2^3 \cdot 3 \cdot 7$
347	173	173	1

349	174	170	$2\cdot3\cdot29$
353	176	176	$2^4\cdot11$
359	179	179	1
367	183	183	$3\cdot61$
373	186	181	$2\cdot3\cdot31$
379	189	189	$3^3\cdot7$
383	191	191	2
389	194	194	$2\cdot97$
397	198	194	$2\cdot3^2\cdot11$
401	200	200	$2^3\cdot5^2$
409	204	204	$2^2\cdot3\cdot17$
419	209	209	$11\cdot19$
421	210	206	$2\cdot3\cdot5\cdot7$
431	215	215	$5\cdot43$
433	216	216	$2^3\cdot3^3$
439	219	219	$3\cdot73$
443	221	221	$13\cdot17$
449	224	224	$2^5\cdot7$
457	228	228	$2^2\cdot3\cdot19$
461	230	230	$2\cdot5\cdot23$
463	231	228	$3\cdot7\cdot11$
467	233	233	8
479	239	239	2
491	245	239	$5\cdot7^2$
499	249	249	$3\cdot83$
503	251	251	5
509	254	254	$2\cdot127$
521	260	260	$2^2\cdot5\cdot13$
523	261	261	$3^2\cdot29$
541	270	270	$2\cdot3^3\cdot5$
547	273	271	$3\cdot7\cdot13$
557	278	278	$2\cdot139$
563	281	281	4
569	284	284	$2^2\cdot71$
571	285	285	$2\cdot3\cdot5\cdot19$

577	288	288	$2^5 \cdot 3^2$
587	293	293	1
593	296	296	$2^3 \cdot 37$
599	299	299	$2 \cdot 13 \cdot 23$
601	300	300	$2^2 \cdot 3 \cdot 5^3$
607	303	301	$3 \cdot 101$
613	306	306	$2 \cdot 3^2 \cdot 17$
617	308	308	$2^2 \cdot 7 \cdot 11$
619	309	309	$3 \cdot 103$
631	315	315	$3^2 \cdot 5 \cdot 7$
641	320	320	$2^6 \cdot 5$
643	321	321	$3 \cdot 107$
647	323	323	$17 \cdot 19$
653	326	326	$2 \cdot 163$
659	329	326	$7 \cdot 47$
661	330	330	$2 \cdot 3 \cdot 5 \cdot 11$
673	336	336	$2^4 \cdot 3 \cdot 7$
677	338	338	$2 \cdot 13^2$
683	341	336	$11 \cdot 31$
691	345	345	$3 \cdot 5 \cdot 23$
701	350	347	$2 \cdot 5^2 \cdot 7$
709	354	350	$2 \cdot 3 \cdot 59$
719	359	359	2
727	363	363	$3 \cdot 11^2$
733	366	366	$2 \cdot 3 \cdot 61$
739	369	369	$3^2 \cdot 41$
743	371	371	$7 \cdot 53$
751	375	371	$3 \cdot 5^3$
757	378	378	$2 \cdot 3^3 \cdot 7$
761	380	380	$2^2 \cdot 5 \cdot 19$
769	384	384	$2^7 \cdot 3$
773	386	386	$2 \cdot 193$
787	393	393	$3 \cdot 131$
797	398	398	$2 \cdot 199$
809	404	404	$2^2 \cdot 101$

811	405	405	$3^4 \cdot 5$
821	410	410	$2 \cdot 5 \cdot 41$
823	411	411	$3 \cdot 137$
<u>827</u>	<u>413</u>	<u>407</u>	$7 \cdot 59$
829	414	414	$2 \cdot 3^2 \cdot 23$
839	419	419	1
<u>853</u>	<u>426</u>	<u>424</u>	$2 \cdot 3 \cdot 71$
857	428	428	$2^4 \cdot 107$
859	429	429	$3 \cdot 11 \cdot 13$
863	431	431	10
877	438	438	$2 \cdot 3 \cdot 73$
881	440	440	$2^3 \cdot 5 \cdot 11$
<u>883</u>	<u>441</u>	<u>435</u>	$3^2 \cdot 7^2$
887	443	443	1
907	453	453	$3 \cdot 151$
911	455	455	$5 \cdot 7 \cdot 13$
919	459	459	$3^3 \cdot 17$
929	464	464	$2^4 \cdot 29$

Appendix II - Polynomial Calculations

By the results found in Chapter III, it is evident that polynomial calculations over GF(2) deserve some attention. The two most useful algorithms are the Euclidean algorithm for the computation of a greatest common divisor and the method of Berlekamp [4] which is used to factor polynomials over finite fields. Both of these algorithms are simple to apply over GF(2) because of the binary nature of digital computers, particularly if bit-processing is available.

Using IBMAP to achieve bit-processing, a program was written for an IBM 7094 to compute $H_q(x)$ by Theorem 3.7 for $929 \leq q \leq 4703$, q prime, p odd. The program was used to check the non-singularity of M_q for $929 \leq q \leq 4703$, q prime, p prime. There are 43 such cases. Of these 43 cases, 13 cases satisfy the hypotheses of Theorem 3.5 and hence M_q is non-singular in these cases. The remaining 30 cases required approximately 13 minutes of computer time. In each case it was found that M_q is non-singular. The same program was subsequently expanded (1200 statements) to include a method for factoring $H_q(x)$ in the case of p odd. The method used was an unpublished method due to Robert J. McEliece. McEliece's method is essentially the same method as Berlekamp's but apparently was found independently. The program was designed to compute the exponents of each irreducible factor. The computer time required was considerable. For example, the cases p = 245, 375, 441 required 1 hour, 9 minutes. The following tables summarize the results of all computations made with $H_q(x)$. Polynomials are expressed by writing down their coefficients in octal notation. For example, the polynomial $x^3 + x+1$ is denoted by 13 octal, which is 1011 binary.

Polynomial Calculations on $H_q(x)$

p	matrix nullity	$H_q(x)$ †	factors of $H_q(x)$ †	exponents of factors
81	2	7	7	3
155	10	2303	75, 67	31, 31
245	6	177	13, 15	7, 7
273	2	7	7	3
303	2	7	7	3
341	5	73	73	31
375	4	23	23	15
413	6	177	13, 15	7, 7
426	2	7	7	3
441	6	103	103	63

† Polynomials are expressed by writing down their coefficients in octal notation. For example, the polynomial $x^3 + x + 1$ is denoted by 13 octal, which is 1011 binary.

Index of Notation

A_d	multiplicative group mod d of least positive residues prime to d, d odd	
B_d	$A_d/\langle 2\rangle$, group of cosets of $\langle 2\rangle$ in A_d	
δ_{ij}	Kronecker delta	
e_d	exponent of 2 mod d, d odd	p. 28
E	field $F(\sqrt{\upsilon_1}, \ldots, \sqrt{\upsilon_p})$	
F	field $Q(\zeta+\zeta^{-1})$	
$\varphi(d)$	Euler phi function	
$\varphi_{\mathfrak{p}}$	reciprocity map	p. 44
Φ	mapping from U/U^2 to $G(E/F)$	p. 53
g. c. d.	greatest common divisor in $GF(2)[x]$	
GF(2)	Galois field of two elements	
G(L/K)	Galois group of L over K	
$G_{\mathfrak{p}}(L/K)$	decomposition group at $\mathfrak{p}$	p. 42
$GF(2)[G(F/Q)]$	group ring of $G(F/Q)$ over $GF(2)$	
$H_q(x)$	see definition	p. 32
$k_{\mathfrak{p}}$	completion of field K at prime $\mathfrak{p}$	
K^*	non zero elements of field K	
$\ell g_\ell k$	see definition	p. 31
M_q	matrix of cyclotomic signatures	p. 8
M_q'	see definition	p. 16
N	units in F which are norms	p. 9
$N\mathfrak{p}$	absolute norm of prime $\mathfrak{p}$	p. 56
$N(L/K, \mathfrak{p})$	local norm group	p. 44
$N_{L/K}$	norm map	
p	$(q-1)/2$	

Index of Notation - cont'd.

p, q	primes	
q	odd rational prime integer	
Q	field of rational numbers	
R	field of real numbers	
R^+	positive real numbers	
S	units in F which are squares	p. 9
$\mathrm{sign}_\sigma(\alpha)$	σ - sign of α	p. 8
$\mathrm{sgn}_\sigma(\alpha)$	σ - signature of α	p. 8
$\mathrm{sgn}(\mu)$	see definition	p. 10
$\overline{\mathrm{sgn}}(\mu)$	see definition	p. 30
T	units in F which are totally positive	p. 9
υ_i	cyclotomic unit	pp. 7-8
U	group generated by cyclotomic units	
$(U/U^2)^\#$	dual group of U/U^2	
V	group of units in F	
$\Psi_d(x)$	dth cyclotomic polynomial	
ζ	primitive qth root of unity	
ζ_d	primitive dth root of unity	
$\tilde{x}$	the coset $x + \langle x^p+1\rangle$	
Z	rational integers	
$\lvert\cdot\rvert$	ordinary absolute value or set cardinality	
$[\![\cdot]\!]$	least positive residue mod q	
$\langle\!\langle\cdot\rangle\!\rangle$	see definition	p. 59
$(\cdot,\cdot)_p$	Hilbert symbol	p. 54
$(\div)$	Legendre symbol	

References

[1] Albert, A. A., Fundamental Concepts of Higher Algebra, University of Chicago Press, Chicago, 1956.

[2] Artin, E., Algebraic Numbers and Algebraic Functions, Gordon and Breach, New York, 1967.

[3] Bass, H., Generators and Relations for Cyclotomic Units, Nagoya Math. J. 27, (1966), pp. 401-407.

[4] Berlekamp, E. R., Factoring Polynomials over Finite Fields, Bell Systems Technical Journal, 46, (1967) pp. 1853-1859.

[5] Borevich, Z. I. and Shafarevich, I. R., Number Theory (translation by Newcomb Greenleaf), Pure and Applied Mathematics, Academic Press, New York, 1966.

[6] Cassels, J. W. S. and Fröhlich, A., Algebraic Number Theory, Thompson Book Co. Inc., Washington, D. C., 1967.

[7] Hardy, G. H., and Wright, E. M., Introduction to the Theory of Numbers, 4th ed. Oxford University Press, London, 1965.

[8] Hasse, H., Über die Klassenzahl Abelscher Zahlkörper, Akademie Verlag, Berlin, 1952.

[9] Hilbert, David, Gesammelte Abhandlungen, v. 1. Zahlentheorie, Springer Verlag, Berlin, 1932.

[10] Jacobson, Nathan, Lectures in Abstract Algebra, v. III, D. Van Nostrand Co., Princeton, N. J., 1964.

[11] O'Meara, O. T., Introduction to Quadratic Forms, Die Grundlehren der Math. Wissenschaften, 117, Springer Verlag, Academic Press, New York, 1963.

[12] Serre, J. P., Corps Locaux, Hermann, Paris, 1962.

[13] Taussky, O., Unimodular Integral Circulants, Math. Zeitschrift. 63 (1955) pp. 285-289.

[14] Van der Waerden, B. L., Modern Algebra, v. 1., rev. English ed., Frederick Ungar Publ. Co., New York, 1966.

[15] Weiss, Edwin, Algebraic Number Theory, McGraw Hill, Inc., New York, 1963.

[16] Weyl, H., Algebraic Theory of Numbers, Annals of Mathematics Studies No. 1., Princeton University Press, Princeton, N. J., 1940.