CORRESPONDING RESIDUE SYSTEMS IN

ALGEBRAIC NUMBER FIELDS

Dissertation

Presented in Partial Fulfillment of the Requirements

for the Degree Doctor of Philosophy in the

Graduate School of The Ohio State

University

by

HUBERT SPENCE BUTTS, JR., B.S., M.S.

The Ohio State University

1953

Approved by:

Henry B. Mann

Adviser

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

In this paper we shall consider integral ideals in number fields, that is, in finite algebraic extensions of the field of rational numbers. Fields will be denoted by the letters F, F', F", F_1, F_2, ..., while the German letters $\mathfrak{a}$, $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{l}$, $\mathfrak{l}_1$, $\mathfrak{L}$, ... will denote ideals. Algebraic numbers in a number field F will be denoted by Greek letters and numbers of the field R of rational numbers will be denoted by lower case Latin letters.

Two ideals in the same field are said to be equal if and only if they contain the same numbers.

Let $F_1 \supset F_2$ and let $\mathfrak{a}_2$ be an ideal of F_2. The numbers of $\mathfrak{a}_2$ generate an ideal $\mathfrak{a}_1$ in F_1 and it is known that the intersection $\mathfrak{a}_1 \cap F_2 = \mathfrak{a}_2$ (see Hecke, "Theorie der algebraischen Zahlen," § 37). Also if the ideal $\mathfrak{a}$ in F and the ideal $\mathfrak{a}'$ in F' generate the same ideal in a field containing F and F', then $\mathfrak{a}$ and $\mathfrak{a}'$ generate the same ideal in $F \cup F'$ and thus in every field containing F and F'.

We shall therefore call two ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ equal if they generate the same ideal in a field containing all the numbers of $\mathfrak{a}_1$ and of $\mathfrak{a}_2$. Two such ideals may therefore be denoted by the same symbol and we shall speak of an ideal $\mathfrak{a}$ without regard to a particular field. An ideal $\mathfrak{a}$ is said to be contained in a field F if it may be generated by numbers in F, that is to say, if it has a basis in F.

Let $\mathfrak{a}$ be an ideal contained in the fields F_1 and F_2. We say that F_1 and F_2 have corresponding residue systems modulo $\mathfrak{a}$ if for every integer α_1 of F_1 there exists an integer α_2 of F_2 such that $\alpha_1 \equiv \alpha_2 (\text{mod.} \mathfrak{a})$, and for every integer α_2 of F_2 there exists an integer α_1 of F_1 such that $\alpha_1 \equiv \alpha_2 (\text{mod.} \mathfrak{a})$. The problem considered in this paper is the following one: if F_1 and F_2 are two fields containing an ideal $\mathfrak{a}$, under what conditions will F_1 and F_2 have corresponding residue systems modulo $\mathfrak{a}$. In Chapter II we show that this problem reduces to that in which the ideal $\mathfrak{a}$ is a power of a prime ideal, and a necessary and sufficient condition for F_1 and F_2 to have corresponding residue systems modulo $\mathfrak{a}$ is derived in the case that $\mathfrak{a}$ is a prime ideal. In Chapters III and IV we consider the problem for fields of the type $F(\sqrt[\ell^m]{\mu})$, where ℓ is a rational prime, μ an integer of F, and F contains a primitive ℓ^{th} root of unity.

In the remainder of Chapter I we give a list of definitions and theorems used in Chapters II and III. The proofs of the theorems may be found in "Theorie der algebraischen Zahlen" by Hecke or in "Algebraic Number Theory" by H. B, Mann.

Let $F_1 \supset F_2$ be two fields and let $\mathfrak{a}_1$ be an ideal in F_1. The numbers of $\mathfrak{a}_1$ which lie in F_2 form an ideal $\mathfrak{a}_2$ in F_2. This ideal $\mathfrak{a}_2$ is said to correspond in F_2 to the ideal $\mathfrak{a}_1$. The ideal $\mathfrak{a}_2$ depends on $\mathfrak{a}_1$ only, and not on F_1. If $\mathfrak{a}_2$ in F_2 corresponds to $\mathfrak{a}_1$ in F_1 and $\mathfrak{a}_2 = \mathfrak{a}_1^e \mathfrak{a}$ with $(\mathfrak{a}_1, \mathfrak{a}) = (1)$, then $\mathfrak{a}_1$ is said to be of order e with respect to F_2. Not every ideal has an order with respect to F_2; however, every ideal which is a prime ideal in some extension of F_2 does.

If α is a number if $F_1 \supset F_2$, we define the relative norm ${}_{F_1F_2}^{N}(\alpha)$ of α in F_1 over F_2 and the relative trace ${}_{F_1F_2}^{T}(\alpha)$ of α in F_1 over F_2 by

$$ {}_{F_1F_2}^{N}(\alpha) = \alpha \cdot \alpha^{(2)} \cdot \ldots \cdot \alpha^{(r)} $$

$$ {}_{F_1F_2}^{T}(\alpha) = \alpha + \alpha^{(2)} + \ldots + \alpha^{(r)} $$

where $\alpha, \alpha^{(2)}, \ldots, \alpha^{(r)}$ are the conjugates of α in F_1 over F_2. The relative norm ${}_{F_1F_2}^{N}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ in F_1 over F_2 is defined by

$$ {}_{F_1F_2}^{N}(\mathfrak{a}) = \mathfrak{a} \cdot \mathfrak{a}^{(2)} \ldots \cdot \mathfrak{a}^{(r)} $$

where $\mathfrak{a}^{(i)}$ is the ideal formed by the i^{th} conjugates in F_1 over F_2 of all numbers of $\mathfrak{a}$. If $F_1 \supset F_2 \supset F_3$ and $\mathfrak{a}$ is an ideal of F_1, then

$$ {}_{F_1F_3}^{N}(\mathfrak{a}) = {}_{F_2F_3}^{N}({}_{F_1F_2}^{N}(\mathfrak{a})). $$

The absolute norm of an ideal $\mathfrak{a}$ in F_1 is the relative norm of $\mathfrak{a}$ in F_1 over the field R of rational numbers and is denoted by ${}_{F_1R}^{N}(\mathfrak{a})$ or ${}_{F_1}^{N}(\mathfrak{a})$. The ideal ${}_{F_1F_2}^{N}(\mathfrak{a})$ is contained in F_2 and in case $F_2 = R$ this ideal is principal. By $|{}_{F_1R}^{N}(\mathfrak{a})|$ we mean the absolute value of the rational number that generates ${}_{F_1R}^{N}(\mathfrak{a})$.

Theorem 1.1: If $\mathfrak{a}$ is an ideal contained in the number field F, the number of residue classes modulo $\mathfrak{a}$ in F is equal to $|{}_{F}N(\mathfrak{a})|$.

Theorem 1.2: If $\mathfrak{p}_1$ is a prime ideal in $F_1 \supset F_2$, there exists a unique prime ideal $\mathfrak{p}_2$ in F_2 such that $\mathfrak{p}_2 \equiv 0 \pmod{\mathfrak{p}_1}$ and ${}_{F_1F_2}^{N}(\mathfrak{p}_1) = \mathfrak{p}_2^{f}$.

Let $F_{\mathfrak{q}}$ denote the field of residues mod. $\mathfrak{q}$ in F, where $\mathfrak{q}$ is a prime ideal in F.

Theorem 1.3: Let $\mathfrak{p}'$ be a prime ideal in $F' \supset F$ and let $\mathfrak{p}$ correspond to $\mathfrak{p}'$ in F. Then ${}_{F'}N_F(\mathfrak{p}') = \mathfrak{p}^f$ and $F'_{\mathfrak{p}'}$ is an algebraic extension of $F_{\mathfrak{p}}$ of degree f.

The number $f = (F'_{\mathfrak{p}'} \mid F_{\mathfrak{p}})$ is called the degree of $\mathfrak{p}'$ in F' over F.

Theorem 1.4: If $\mathfrak{p}_1$ is a prime ideal in $F_1 \supset F_2$ and $\mathfrak{p}_1$ is of degree one over F_2, then every residue class mod. $\mathfrak{p}_1$ in F_1 contains an integer of F_2.

Theorem 1.5: The set S of numbers ξ in $F_1 \supset F_2$ for which ${}_{F_1}T_{F_2}(\alpha\xi) \equiv 0$ (mod. (1)) for $\alpha \equiv 0$ (mod. (1)) is the reciprocal of an integral ideal ${}_{F_1}\mathfrak{d}_{F_2}$, called the relative differente of F_1 over F_2.

The relative differente of a number θ in $F_1 \supset F_2$ is defined by

$$\varphi'(\theta) = \prod_{i=2}^{m} (\theta - \theta^{(i)})$$

where the product is extended over all the relative conjugates $\theta^{(i)}$ of θ in F_1 over F_2 and $\varphi(x) = \prod_{i=1}^{m} (x - \theta^{(i)})$.

Theorem 1.6: The relative differente ${}_{F_1}\mathfrak{d}_{F_2}$ of F_1 over F_2 is the greatest common divisor of all number differentes $\varphi'(\theta)$, where θ is an integer in F_1.

If θ is an integer of $F_1 \supset F_2$, it follows from Theorem 1.6 that there exists an ideal $\mathfrak{f}$, called the relative conductor of θ in F_1 over F_2, such that

$$(\varphi'(\theta)) = \mathfrak{f}\; {}_{F_1}\mathfrak{d}_{F_2}$$

<u>Theorem</u> 1.7: If $\mathfrak{p}_1$ is a prime ideal in $F_1 \supset F_2$, then $\mathfrak{D}_{F_1 F_2} \equiv 0 \pmod{\mathfrak{p}_1}$ if and only if $\mathfrak{p}_1$ is of order greater than one with respect to F_2.

Let F' be normal over F and let $\mathfrak{G}(F' \mid F)$ denote the Galois group of F' over F. If A is any automorphism of $\mathfrak{G}(F' \mid F)$, we shall write α^A for the number into which the number α is transformed under A. If $\mathfrak{a}$ is an ideal of F', we shall write $\mathfrak{a}^A$ for the ideal into which $\mathfrak{a}$ is mapped under the automorphism A.

Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F. The <u>inertial group</u> $\mathfrak{G}_i$ of $\mathfrak{p}'$ is the subgroup of automorphisms A of $\mathfrak{G}(F' \mid F)$ for which $\alpha^A \equiv \alpha \pmod{\mathfrak{p}'}$ for every integer α in F'. The <u>inertial field</u> F_i of $\mathfrak{p}'$ is the subfield of F' corresponding to $\mathfrak{G}_i$ under the Galois correspondence.

<u>Theorem</u> 1.8: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F. If f denotes the degree, e the order, and g the number of conjugates of $\mathfrak{p}'$ in F' over F, then $efg = (F' \mid F)$.

<u>Theorem</u> 1.9: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F, and let F_i be the inertial field of $\mathfrak{p}'$ in F' over F. Then $\mathfrak{p}'$ is of order $(F' \mid F_i)$ with respect to F_i.

<u>Theorem</u> 1.10: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F, $\mathfrak{G}$ the Galois group of F' over F, and let $\mathfrak{p}'$ correspond to $\mathfrak{p}$ in F. There exists an automorphism A in $\mathfrak{G}$ such that

$$\alpha^A \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{p}'}$$

for every integer α in F', where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in F' over the rational field.

The j^{th} ramification group $\mathcal{G}_j$ of a prime ideal $\mathfrak{p}'$ in a field F' normal over F is the subgroup of automorphisms A of $\mathcal{G}(F' \mid F)$ for which $\alpha^A \equiv \alpha \pmod{\mathfrak{p}'^j}$ for all integers α in F'. We have

$$\mathcal{G}_i = \mathcal{G}_1 \supset \mathcal{G}_2 \supset \mathcal{G}_3 \supset \ldots$$

Theorem 1.11: The sequence $\mathcal{G}_i = \mathcal{G}_1 \supset \mathcal{G}_2 \supset \ldots$ ends with the unit element.

If v is the first integer such that $\mathcal{G}_{v+1}$ is the unit element, then v is called the order of ramification of the ideal $\mathfrak{p}'$ in F' over F.

Theorem 1.12: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F, let p be the rational prime corresponding to $\mathfrak{p}'$, and let e denote the order of $\mathfrak{p}'$ in F' over F. If $e = e_0 p^r$ with $(e_0, p) = 1$, then $\mathcal{G}_1 / \mathcal{G}_2$ is cyclic of order e_0 and $\mathcal{G}_{j-1} / \mathcal{G}_j$ is Abelian of type $(p, \ldots, p)$ and order p^{r_j} for $j > 2$.

Theorem 1.13: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F, and let π be a number of F' exactly divisible by $\mathfrak{p}'$. Then an automorphism A in $\mathcal{G}_1$ is in $\mathcal{G}_j$ if and only if $\pi^A \equiv \pi \pmod{\mathfrak{p}'^j}$

Theorem 1.14: Let $\mathfrak{p}'$ be a prime ideal in the field F' normal over F and let p^{r_j} be the order of $\mathcal{G}_j$ for $j \geq 2$. Then ${}_{F'}\mathfrak{d}_F$ is exactly divisible by

$$\mathfrak{p}'^{\,e-1 + \sum_{2}^{v} (p^{r_j} - 1)}$$

where e is the order of $\mathfrak{p}'$ in F' over F and v is the order of ramification.

Let ℓ be a positive rational prime, $\zeta \neq 1$ an ℓ^{th} root of unity, and F a number field containing ζ. Let μ be a number of F which is not the ℓ^{th} power of a number in F. The following three theorems (see Hecke, "Theorie der algebraischen Zahlen," §39) give the prime decomposition of a prime ideal of F in F($\sqrt[\ell]{\mu}$).

Theorem 1.15: If $\mathfrak{p}$ is a prime ideal in F, one of the following three possibilities must hold: 1.) $\mathfrak{p}$ remains a prime ideal in F($\sqrt[\ell]{\mu}$). 2.) $\mathfrak{p}$ is the ℓ^{th} power of a prime ideal in F($\sqrt[\ell]{\mu}$). 3.) $\mathfrak{p}$ is the product of ℓ different prime ideals in F($\sqrt[\ell]{\mu}$).

Theorem 1.16: Let $\mathfrak{p}$ be a prime ideal in F and suppose $(\mu) = \mathfrak{p}^a\mathfrak{a}$ with $a \geq 0$ and $(\mathfrak{a}, \mathfrak{p}) = (1)$. If $(a, \ell) = 1$, $\mathfrak{p}$ is the ℓ^{th} power of a prime ideal in F($\sqrt[\ell]{\mu}$). If $a = 0$ and $(\mathfrak{p}, \ell) = (1)$, then $\mathfrak{p}$ is the product of ℓ different prime ideals in F($\sqrt[\ell]{\mu}$) in case the congruence

$$\mu \equiv \xi^{\ell} \pmod{\mathfrak{p}}$$

is solvable for ξ in F, and $\mathfrak{p}$ remains a prime ideal in F($\sqrt[\ell]{\mu}$) in case this congruence is not solvable.

Theorem 1.17: Let $\mathfrak{l}$ be a prime divisor of $(1 - \zeta)$ in F such that $(\mathfrak{l}, \mu) = (1)$. Suppose $(1 - \zeta) = \mathfrak{l}^a \mathfrak{l}_1$ with $(\mathfrak{l}, \mathfrak{l}_1) = (1)$. Then 1.) $\mathfrak{l}$ is the product of ℓ different prime ideals in F($\sqrt[\ell]{\mu}$) in case the congruence

$$\mu \equiv \xi^{\ell} \pmod{\mathfrak{l}^{a\ell+1}}$$

is solvable for ξ in F. 2.) $\mathfrak{l}$ remains a prime ideal in F($\sqrt[\ell]{\mu}$) in case the congruence of 1.) is not solvable and the congruence

$$\mu \equiv \xi^{\ell} \pmod{\mathfrak{l}^{a\ell}}$$

is solvable for ξ in F. 3.) $\mathfrak{l}$ is the ℓ^{th} power of a prime ideal in

$F(\sqrt[l]{\mu})$ in case the congruence of 2.) is not solvable.

CHAPTER II

GENERAL THEOREMS

In this chapter we consider the problem of corresponding residue systems mod. an ideal $\mathfrak{a}$ for two general number fields, and also for two number fields F_1 and F_2 each normal over their intersection $F_1 \cap F_2$. The main result of this chapter is Theorem 2.5 which gives a necessary and sufficient condition for two number fields to have corresponding residue systems mod. an ideal which is a prime ideal in both fields.

We first show that we need only to consider the case in which the modulus $\mathfrak{a}$ is a power of a prime ideal.

Theorem 2.1: Let $\mathfrak{a}$ be an ideal in the two number fields F_1 and F_2, and suppose F_1 and F_2 have corresponding residue systems mod. $\mathfrak{a}$. Then $\mathfrak{a}$ has the same prime ideal decomposition in F_1 and in F_2.

Proof: Let

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r} \quad \text{in } F_1$$

$$\mathfrak{a} = \mathfrak{q}_1^{f_1} \cdot \ldots \cdot \mathfrak{q}_s^{f_s} \quad \text{in } F_2$$

where the $\mathfrak{p}_i$ are prime ideals in F_1 and the $\mathfrak{q}_i$ are prime ideals in F_2. Let α be an integer in F_1 such that α is exactly divisible by $\mathfrak{p}_1$ and $(\alpha, \mathfrak{p}_i) = (1)$ for $i = 2, \ldots, r$. There exists an integer β in F_2 such that

$$\alpha \equiv \beta \pmod{\mathfrak{a}}$$

and thus in $F_1 \cup F_2$ we have $(\beta, \mathfrak{a}) = \mathfrak{p}_1$. Since β is in F_2 and $\mathfrak{a} \subset F_2$, it follows that

$$\mathfrak{p}_1 \subset F_2.$$

In the same manner it follows that

$$\mathfrak{p}_i \subset F_2 \qquad i = 1, \ldots, r$$

and also that

$$\mathfrak{q}_i \subset F_1 \qquad i = 1, \ldots, s.$$

Therefore in F_1 and in F_2 we have

$$\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r} = \mathfrak{q}_1^{f_1} \cdot \ldots \cdot \mathfrak{q}_s^{f_s}.$$

In F_2 the $\mathfrak{q}_i$ are prime ideals and hence

$$\mathfrak{q}_1 \mid \mathfrak{p}_j$$

in F_2 for some j. In F_1 the $\mathfrak{p}_i$ are prime ideals and therefore

$$\mathfrak{p}_k \mid \mathfrak{q}_1$$

in F_1 for some k. Thus in $F_1 \cup F_2$ we have

$$\mathfrak{p}_k \mid \mathfrak{p}_j$$

which implies that

$$\mathfrak{p}_k = \mathfrak{p}_j = \mathfrak{q}_1$$

in F_1 and in F_2. By renumbering and repeated application of the above argument we obtain r = s and

$$\mathfrak{p}_i = \mathfrak{q}_i$$

for i = 1, ..., r = s in F_1 and in F_2. Hence $\mathfrak{a}$ has the same prime ideal decomposition in F_1 and in F_2.

<u>Theorem</u> 2.2: Let $\mathfrak{a}$ be an ideal in the two number fields F_1 F_2. Then F_1 and F_2 have corresponding residue systems mod. $\mathfrak{a}$ if and only if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i$ is a prime ideal in F_1 and in F_2, and F_1 and F_2 have corresponding residue systems

mod. $\mathfrak{p}_i^{e_i}$ for $i = 1, \ldots, r$.

<u>Proof</u>: Suppose F_1 and F_2 have corresponding residue systems mod. $\mathfrak{a}$. By Theorem 2.1 we have

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

in F_1 and in F_2, where $\mathfrak{p}_i$ is a prime ideal in F_1 and in F_2. It follows that F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}_i^{e_i}$ for $i = 1, \ldots, r$.

Conversely, suppose $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ in F_1 and in F_2, where $\mathfrak{p}_i$ is a prime ideal in F_1 and in F_2, and that F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}_i^{e_i}$ for $i = 1, \ldots, r$. Let α be any integer of F_1. There exist integers β_i in F_2 such that

$$\alpha \equiv \beta_i \pmod{\mathfrak{p}_i^{e_i}} \qquad i = 1, \ldots, r.$$

By the Chinese remainder theorem applied in F_2 there exists an integer β in F_2 such that

$$\beta \equiv \beta_i \pmod{\mathfrak{p}_i^{e_i}} \qquad i = 1, \ldots, r$$

and hence

$$\alpha \equiv \beta \quad (\mathfrak{a}) .$$

It follows that F_1 and F_2 have corresponding residue systems mod. $\mathfrak{a}$.

In order to prove the main result (Theorem 2.5) of this chapter we first prove two preliminary theorems.

<u>Theorem</u> 2.3: Let F_1 and F_2 be two number fields, $F = F_1 \cap F_2$, and let $\mathfrak{p}$ be a prime ideal in both F_1 and F_2. Suppose F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}^j$ and let F_n be the smallest normal extension containing F_1 and F_2. Then for every automorphism A in $\mathfrak{G}(F_n \mid F)$ we have

$$\alpha_1^A \equiv \alpha_1 \quad (\text{mod. } \mathcal{J}^j)$$

$$\alpha_2^A \equiv \alpha_2 \quad (\text{mod. } \mathcal{J}^j)$$

for every integer α_1 in F_1 and α_2 in F_2.

Proof: Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be the subgroups of $\mathcal{G}(F_n | F)$ which leave F_1 and F_2 fixed respectively. Since the ideal $\mathcal{J}$ is contained in F_1 and in F_2, we have

$$(\mathcal{J}^j)^A = \mathcal{J}^j$$

for every automorphism A in the group $\mathcal{G}_1 \cup \mathcal{G}_2$. Since $F = F_1 \cap F_2$, we have by Galois theory that $\mathcal{G}_1 \cup \mathcal{G}_2$ corresponds to F under the Galois correspondence between subgroups and subfields. Hence

$$\mathcal{G}_1 \cup \mathcal{G}_2 = \mathcal{G}(F_n | F).$$

Denote by S_i ($i = 1, 2$) the set of automorphisms A in $\mathcal{G}(F_n | F)$ such that

$$\alpha_i^A \equiv \alpha_i \ (\text{mod. } \mathcal{J}^j) \qquad i = 1, 2$$

for all integers α_i in F_i for $i = 1, 2$. The sets S_i are subgroups of $\mathcal{G}(F_n | F)$. Furthermore the sets S_i contain $\mathcal{G}_i$ for $i = 1, 2$.

Let A be an automorphism of S_2. For every integer α_1 in F_1 there exists an integer α_2 in F_2 such that

$$\alpha_1 \equiv \alpha_2 \quad (\text{mod. } \mathcal{J}^j).$$

Therefore

$$(\alpha_1 - \alpha_2)^A \equiv 0 \ (\text{mod. } \mathcal{J}^j)$$

$$\alpha_1^A \equiv \alpha_2^A \ (\text{mod. } \mathcal{J}^j)$$

$$\alpha_1^A \equiv \alpha_2 \quad (\text{mod. } \mathcal{J}^j)$$

$$\alpha_1^A \equiv \alpha_1 \quad (\text{mod. } \mathcal{J}^j) \ .$$

Hence the automorphism A is also in S_1 and it follows that

$$S_2 \subset S_1.$$

Similarly $S_1 \subset S_2$ and therefore

$$S_1 = S_2.$$

Thus

$$S_1 = S_2 = \mathcal{G}(F_n \mid F)$$

since $S_i \supset \mathcal{G}_i$ for $i = 1, 2$ and $\mathcal{G}_1 \cup \mathcal{G}_2 = \mathcal{G}(F_n \mid F)$.

Corollary 2.3.1: Under the conditions of Theorem 2.3 it follows that

$$\mathfrak{d}_{F_1 F} \equiv 0 \ (\mathfrak{p}^{n_1 j}) \qquad \mathfrak{d}_{F_2 F} \equiv 0 \ (\mathfrak{p}^{n_2 j})$$

where $n_1 + 1 = (F_1 \mid F)$ and $n_2 + 1 = (F_2 \mid F)$.

Proof: The corollary follows from Theorem 1.6 and Theorem 2.3.

Theorem 2.4: Let $F_1 \supset F$ be two number fields and let $\mathfrak{P}$ be a prime ideal in F_1. Suppose that for every integer α in F_1 we have

$$\alpha \equiv \alpha^{(i)} \ (\text{mod. } \mathfrak{P}) \qquad i = 1, \ldots, k = (F_1 \mid F)$$

Then $\mathfrak{P}$ is of order $k = (F_1 \mid F)$ with respect to F.

Proof: It is clear that $\mathfrak{P}$ coincides with all of its conjugates. Let F_n denote the smallest normal extension containing F_1. Let $\mathfrak{P}_n$ be a prime divisor of $\mathfrak{P}$ in F_n and let $\mathfrak{p}$ in F correspond to $\mathfrak{P}$.

The residue field mod. $\mathfrak{P}$ in F_1 is an algebraic extension of the residue field mod. $\mathfrak{p}$ in F by Theorem 1.3. Its Galois group is generated by the automorphism $\alpha \to \alpha^{N(\mathfrak{p})}$ where $N(\mathfrak{p})$ is the absolute norm of $\mathfrak{p}$ in F. Let ω be a primitive root mod. $\mathfrak{P}$ in F_1. By Theorem 1.10 there exists an automorphism A such that

$$\omega^{N(\mathfrak{p})} \equiv \omega^{A} \quad (\mathfrak{P}_n).$$

But

$$\omega^{A} = \omega^{(i)} \equiv \omega \quad (\text{mod. } \mathfrak{P}).$$

Hence

$$\omega^{N(\mathfrak{f})} \equiv \omega \ (\text{mod. } \mathfrak{P}_n)$$
$$\omega^{N(\mathfrak{f})} \equiv \omega \ (\text{mod. } \mathfrak{P}).$$

But this means that ω is in the field of residues mod. $\mathfrak{f}$ in F or

$$\omega \equiv \xi \ (\text{mod. } \mathfrak{P}) \qquad \xi \text{ in } F.$$

Hence $\mathfrak{P}$ is of degree one over $\mathfrak{f}$ and therefore by Theorem 1.8 of order $k = (F_1 | F)$.

<u>Theorem</u> 2.5: Let F_1 and F_2 be two number fields and $\mathfrak{f}$ be a prime ideal in both fields. Then F_1 and F_2 have corresponding residue systems mod. $\mathfrak{f}$ if and only if $\mathfrak{f}$ is of order $(F_1 | F_1 \cap F_2)$ in F_1 over $F_1 \cap F_2$ and of order $(F_2 | F_1 \cap F_2)$ in F_2 over $F_1 \cap F_2$.

<u>Proof</u>: If F_1 and F_2 have corresponding residue systems mod. $\mathfrak{f}$, it follows immediately from Theorems 2.3 and 2.4 that the order of $\mathfrak{f}$ satisfies the conditions of the theorem.

The converse is clear since $\mathfrak{f}$ is of degree one over $F_1 \cap F_2$ by Theorem 1.8, and therefore by Theorem 1.4 every residue class mod. $\mathfrak{f}$ contains an integer of $F_1 \cap F_2$.

<u>Corollary</u> 2.5.1: Let $\mathfrak{a}$ be an ideal in the number fields F_1 and F_2. If F_1 and F_2 have corresponding residue systems mod. $\mathfrak{a}$, then

$$(F_1 | F_1 \cap F_2) = (F_2 | F_1 \cap F_2).$$

<u>Proof</u>: The corollary follows from Theorems 2.2 and 2.5.

In the remainder of Chapter II we consider the case in which the two number fields F_1 and F_2 are normal over their intersection $F_1 \cap F_2$.

<u>Theorem</u> 2.6: Let F_1 and F_2 be two number fields each normal over $F = F_1 \cap F_2$ and let $\mathfrak{p}$ be a prime ideal in F_1 and in F_2. In order that F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}$ it is necessary and sufficient that the inertial group of $\mathfrak{p}$ in F_j over F be equal to the Galois group of F_j over F for $j = 1, 2$.

<u>Proof</u>: The condition is sufficient since by Theorem 1.9 $\mathfrak{p}$ is of degree one in F_j over F $(j = 1, 2)$ if the inertial group of $\mathfrak{p}$ in F_j over F is equal to the Galois group of F_j over F $(j = 1, 2)$.

Suppose F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}$ and let F_i denote the inertial field of $\mathfrak{p}$ in F_1 over F. By Theorem 1.9 the order of $\mathfrak{p}$ in F_1 over F is equal to $(F_1 \mid F_i)$, and hence from Theorem 2.5 we have

$$(F_1 \mid F_i) = (F_1 \mid F) .$$

It follows that $F_i = F$, and hence the Galois group of F_1 over F is equal to the inertial group of $\mathfrak{p}$ in F_1 over F. In the same way it follows that the Galois group of F_2 over F is equal to the inertial group of $\mathfrak{p}$ in F_2 over F.

We were not able to obtain a necessary and sufficient condition for two number fields to have corresponding residue systems mod. a power of a prime ideal. However, if F_1 and F_2 are normal over $F_1 \cap F_2$, the following theorem gives a necessary condition for F_1 and F_2 to have corresponding residue systems mod. a power of a prime ideal.

<u>Theorem</u> 2.7: Let F_1 and F_2 be two number fields each normal over $F = F_1 \cap F_2$, and let $\mathfrak{p}$ be a prime ideal in F_1 and in F_2. If F_1 and

F_2 have corresponding residue systems mod. $\mathfrak{p}^j$, then the j^{th} ramification group of $\mathfrak{p}$ in F_k over F is equal to the Galois group of F_k over F for $k = 1, 2$.

Lemma: Let F_1 and F_2 be two fields normal over $F = F_1 \cap F_2$. Then every automorphism of $\mathcal{G}(F_i \mid F)$ can be continued to an automorphism of $\mathcal{G}(F_1 \cup F_2 \mid F)$ for $i = 1, 2$.

Proof: The lemma follows directly from Galois theory and the fact that $\mathcal{G}(F_1 \cup F_2 \mid F)$ is the direct product of $\mathcal{G}(F_1 \mid F)$ and $\mathcal{G}(F_2 \mid F)$.

Proof of the theorem: Let A be any automorphism of $\mathcal{G}(F_1 \cup F_2 \mid F)$. It follows from Theorem 2.3 that

$$\alpha_i^A \equiv \alpha_i (\text{mod. } \mathfrak{p}^j)$$

for every integer α_i in F_i for $i = 1, 2$. Hence if A_i is an automorphism of $\mathcal{G}(F_i \mid F)$ it follows from the lemma that

$$\alpha_i^{A_i} \equiv \alpha_i \ (\text{mod. } \mathfrak{p}^j)$$

for every integer α_i in F_i for $i = 1, 2$. Thus the j^{th} ramification group of $\mathfrak{p}$ in F_i over F is equal to the Galois group of F_i over F for $i = 1, 2$.

Corollary 2.7.1: Let F_1 and F_2 be two number fields normal over $F = F_1 \cap F_2$, and let $\mathfrak{p}$ be a prime ideal in F_1 and in F_2. If F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}^j$ for $j > 1$, then $(F_1 \mid F) = (F_2 \mid F) = p^r$ where p is the rational prime belonging to $\mathfrak{p}$.

Proof: By Theorem 2.7 we have

$$\mathcal{G}(F_1 \mid F) = \mathcal{G}_1 = \dots = \mathcal{G}_j$$

where $\mathcal{G}_j$ is the j^{th} ramification group of $\mathfrak{P}$ in F_1 over F. By Theorem 2.5 the order e of $\mathfrak{P}$ in F_1 over F is equal to $(F_1 | F)$. By Theorem 1.12 we have $\mathcal{G}_1 / \mathcal{G}_2$ cyclic of order e_o where

$$e = e_o\, p^r \qquad (e_o, p) = 1$$

and p is the rational prime belonging to the ideal $\mathfrak{P}$. Therefore

$$(F_1 | F) = e_o p^r.$$

Since $\mathcal{G}_1 = \mathcal{G}_2$, $e_o = 1$ and

$$(F_1 | F) = p^r .$$

By Corollary 2.5.1

$$(F_1 | F) = (F_2 | F) = p^r.$$

Corollary 2.7.2: Let F_1 and F_2 be two number fields normal over $F = F_1 \cap F_2$, let $\mathfrak{A}$ be an ideal in F_1 and in F_2, and suppose F_1 and F_2 have corresponding residue systems mod. $\mathfrak{A}$. Then $\mathfrak{A}$ is not divisible by the square of a prime ideal if $(F_1 | F) = (F_2 | F)$ is not a prime power. If $(F_1 | F) = (F_2 | F) = p^k$ is a prime power, then $\mathfrak{A} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r \cdot \mathfrak{A}'$ where $\mathfrak{P}_i \neq \mathfrak{P}_j$ are prime ideals and $\mathfrak{A}'$ divides a power of p.

Proof: The corollary follows directly from Theorem 2.2 and Corollary 2.7.1.

Corollary 2.7.3: Let F_1 and F_2 be two number fields each normal over $F = F_1 \cap F_2$, and let $\mathfrak{P}$ be a prime ideal in F_1 and in F_2. Let v_i denote the order of ramification of $\mathfrak{P}$ in F_i over F for $i = 1, 2$ and suppose $v_1 \geq v_2 \geq 2$. If F_1 and F_2 have corresponding residue systems mod. $\mathfrak{P}^{v_2}$, $\mathcal{G}(F_2 | F)$ is Abelian of type (p, ..., p) where p is the rational prime belonging to $\mathfrak{P}$.

<u>Proof</u>: If F_1 and F_2 have corresponding residue systems mod. $\mathfrak{p}^{v_2}$, it follows that from Theorem 2.7

$$\mathfrak{T}(F_2 \mid F) = \mathfrak{T}_1 = \mathfrak{T}_2 = \dots = \mathfrak{T}_{v_2}$$

where $\mathfrak{T}_j$ is the j^{th} ramification group of $\mathfrak{p}$ in F_2 over F. By the definition of v_2 we have

$$\mathfrak{T}_{v_2+1} = I,$$

the group identity. By Theorem 1.12 we have $\mathfrak{T}_{v_2} \mid \mathfrak{T}_{v_2+1}$ Abelian of type (p, ..., p) where p is the rational prime belonging to $\mathfrak{p}$. It follows that $\mathfrak{T}(F_2 \mid F)$ is Abelian of type (p, ..., p).

In case $v_2 = 1$ in Corollary 2.7.3 the group $\mathfrak{T}(F_2 \mid F)$ is cyclic of order e_0 where $(F_2 \mid F) = e_0 p^r$, $(e_0, p) = 1$, p the rational prime belonging to $\mathfrak{p}$.

The condition of Theorem 2.7 is not sufficient as the following example shows. Denote by R the field of rational numbers and let $F_1 = R(\sqrt{2})$, $F_2 = R(\sqrt{3})$, $\mathfrak{p} = (\sqrt{2})$. It is clear that the second ramification of the ideal $(\sqrt{2})$ in F_2 over R is equal to the Galois group of F_1 over R, and likewise for F_2. However, F_1 and F_2 do not have corresponding residue systems mod. $(\sqrt{2})^2$. For suppose

$$\sqrt{2} \equiv a + b\sqrt{3} \pmod{2}$$

in the field $R(\sqrt{2}, \sqrt{3})$ where a and b are rational integers. We may suppose that both a and b are odd, for otherwise $2 \mid \sqrt{2}$. Therefore both a and b may be replaced by 1. Hence

$$\sqrt{2} \equiv 1 + \sqrt{3} \pmod{2}$$

and

$$\frac{\sqrt{2} - 1 - \sqrt{3}}{2}$$

is an integer. Thus

$$\left(\frac{\sqrt{2} - 1 - \sqrt{3}}{2}\right)\left(\frac{\sqrt{2} - 1 + \sqrt{3}}{2}\right) = - \frac{\sqrt{2}}{2}$$

must be an integer, which is a contradiction.

CHAPTER III

CORRESPONDING RESIDUE SYSTEMS IN FIELDS $F(\sqrt[\ell]{\mu})$

Let ℓ be a rational prime, $\zeta \neq 1$ an ℓ^{th} root of unity, and F a number field containing ζ. In this chapter we shall consider fields of the type $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$, ... where μ_i is an integer of F and not the ℓ^{th} power of an integer in F.

Let $\mathfrak{P}$ be a prime ideal in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$. By Theorem 2.5 in order that $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{P}$ it is necessary and sufficient that $\mathfrak{P}$ be of order ℓ in $F(\sqrt[\ell]{\mu_1})$ over F and in $F(\sqrt[\ell]{\mu_2})$ over F. Therefore by Theorem 1.7 it is necessary and sufficient that $\mathfrak{P}$ divide the relative differente

$$\underset{F(\sqrt[\ell]{\mu_i})\;F}{\mathfrak{D}}$$

of $F(\sqrt[\ell]{\mu_i})$ over F for i = 1, 2. If $\mathfrak{C}_i$ denotes the relative conductor of $\sqrt[\ell]{\mu_i}$ (i = 1, 2), then

$$(\sqrt[\ell]{\mu_i})^{\ell-1}\,\ell = \mathfrak{C}_i \cdot \underset{F(\sqrt[\ell]{\mu_i})\;F}{\mathfrak{D}}$$

for i = 1, 2 since $(\sqrt[\ell]{\mu_i})^{\ell-1}\,\ell$ is the relative number differente of $\sqrt[\ell]{\mu_i}$ over F (see Theorem 1.6). It follows that $\mathfrak{P}$ must divide $(\sqrt[\ell]{\mu_i})^{\ell-1}\,\ell$ for i = 1, 2 if $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{P}$.

Denote by $\mathfrak{q}$ the prime ideal corresponding to $\mathfrak{P}$ in F. By Theorem 1.16, if $\mathfrak{q}$ divides μ_i then $\mathfrak{q} = \mathfrak{P}^{\ell}$ in $F(\sqrt[\ell]{\mu_i})$ if and only if

$$(\mu_i) = \mathfrak{f}^{a_i}\,\mathfrak{a}_i \qquad i = 1, 2$$

where $(a_i, \ell) = 1$ and $(\mathfrak{a}_i, \mathfrak{f}) = (1)$. Thus we have the following theorem.

<u>Theorem</u> 3.1: If $(\mathfrak{p}, \ell) = 1$, then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{p}$ if and only if

$$(\mu_i) = \mathfrak{f}^{a_i}\,\mathfrak{a}_i$$

with $(a_i, \ell) = 1$ and $(\mathfrak{a}_i, \mathfrak{f}) = (1)$ for $i = 1, 2$.

From Corollary 2.7.1 it follows that $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ do not have corresponding residue systems mod. $\mathfrak{p}^j$ for $j > 1$ in case $(\mathfrak{p}, \ell) = (1)$.

We now consider prime ideals in $F(\sqrt[\ell]{\mu})$ which divide ℓ, that is, prime ideals which divide the ideal $(1 - \zeta)$ since $\ell = (1 - \zeta)^{\ell-1}$ in F. Let

$$(1 - \zeta) = \mathfrak{L}^a\,\mathfrak{a}$$

in F, where $(\mathfrak{L}, \mathfrak{a}) = (1)$ and $\mathfrak{L}$ is a prime ideal in F, and let $\mathfrak{l}$ be a prime ideal of $F(\sqrt[\ell]{\mu})$ which divides $\mathfrak{L}$. By Theorem 2.5 we are concerned only with the case in which $\mathfrak{l}$ is of order ℓ in $F(\sqrt[\ell]{\mu})$ over F, that is

$$\mathfrak{L} = \mathfrak{l}^{\ell}$$

in $F(\sqrt[\ell]{\mu})$. We may suppose without loss of generality that either $(\mu, \mathfrak{L}) = (1)$ or $(\mu, \mathfrak{L}^2) = \mathfrak{L}$ (see Hecke, Theorie der algebraischen Zahlen, page 151). By Theorem 1.16 $\mathfrak{L}$ becomes the ℓ^{th} power of a prime ideal in $F(\sqrt[\ell]{\mu})$ in case $(\mu, \mathfrak{L}^2) = \mathfrak{L}$. In case $(\mu, \mathfrak{L}) = (1)$, by Theorem 1.17 $\mathfrak{L}$ becomes an ℓ^{th} power of a prime ideal in $F(\sqrt[\ell]{\mu})$ if the congruence

$$\mu \equiv \xi^{\ell} \pmod{\mathfrak{L}^{a\ell}}$$

is not solvable for ξ in F.

The main result of this chapter is the following: if μ_1, μ_2 are two integers of F such that $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$, and $\mathfrak{l}$ has ramification orders $\geq v > a$ in $F(\sqrt[\ell]{\mu_1}), F(\sqrt[\ell]{\mu_2})$ over F, then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{v-a}$.

We consider first the case in which $(\mu, \mathfrak{L}^2) = \mathfrak{L}$.

<u>Theorem</u> 3.2: If $(\mu, \mathfrak{L}^2) = \mathfrak{L}$ and n is a positive integer, then $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu})$ and every integer α in $F(\sqrt[\ell]{\mu})$ satisfies the congruence

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu} + \dots + \alpha_{n-1} \sqrt[\ell]{\mu^{n-1}} \pmod{\mathfrak{l}^n}$$

where the α_i are integers in F. Furthermore the order of ramification v of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu})$ over F is equal to $a\ell + 1$.

<u>Proof</u>: Since $(\mu, \mathfrak{L}^2) = \mathfrak{L}$, we have $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu})$ where $\mathfrak{l}$ is a prime ideal. It follows that $\sqrt[\ell]{\mu}$ is exactly divisible by $\mathfrak{l}$. Let n be any positive integer. If α is any integer of F we have

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu} + \dots + \alpha_{n-1} \sqrt[\ell]{\mu^{n-1}} \pmod{\mathfrak{l}^n}$$

where the α_i are residues mod. $\mathfrak{l}$ and may be chosen in F since $\mathfrak{l}$ is of degree 1 with respect to F.

By Theorem 1.13 the order of ramification of $\mathfrak{l}$ is equal to v if and only if

$$\sqrt[\ell]{\mu} \equiv \zeta \sqrt[\ell]{\mu} \pmod{\mathfrak{l}^{v}}, \qquad \sqrt[\ell]{\mu} \not\equiv \zeta \sqrt[\ell]{\mu} \pmod{\mathfrak{l}^{v+1}}.$$

Hence $v = a\,\ell + 1$ since $(1 - \zeta) = \mathfrak{n}\,\mathfrak{L}^{a}$, $\mathfrak{L} = \mathfrak{l}^{\ell}$, and $(\mathfrak{L}, \mathfrak{n}) = (1)$.

Theorem 3.3: If μ_1, μ_2 are two integers of F each exactly divisible by $\mathfrak{L}$, then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1-a}$.

Proof: Choose a fixed residue system mod. $\mathfrak{L}$ in F consisting of ℓ^{th} powers, which is possible since $\mathfrak{L}$ is a prime ideal in F. Represent the residue class 0 by 0 and let $n = a(\ell - 1)$. Since μ_1 is exactly divisible by $\mathfrak{L}$ we have

$$\mu_2 \equiv \alpha_1^{\ell}\,\mu_1 + \dots + \alpha_n^{\ell}\,\mu_1^{n} \pmod{\mathfrak{L}^{n+1}}$$

where the α_i^{ℓ} belong to the fixed residue systems mod. $\mathfrak{L}$ chosen above.

Hence

$$(\sqrt[\ell]{\mu_2} - \alpha_1\sqrt[\ell]{\mu_1} - \dots - \alpha_n\sqrt[\ell]{\mu_1^{n}})^{\ell} \equiv \mu_2 - \alpha_1^{\ell}\mu_1 - \dots - \alpha_n^{\ell}\mu_1^{n} \pmod{\mathfrak{L}^{n+1}}$$

$$\equiv 0 \pmod{\mathfrak{L}^{n+1}}$$

since all mixed terms are divisible by $\ell\,\mathfrak{L}$. It follows that

$$\sqrt[\ell]{\mu_2} \equiv \alpha_1 \sqrt[\ell]{\mu_1} + \dots + \alpha_n \sqrt[\ell]{\mu_1^{n}} \pmod{\mathfrak{l}^{n+1}},$$

and by Theorem 3.2 $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1-a}$.

By Theorem 2.7 the two fields $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ do not have corresponding residue systems mod. $\mathfrak{l}^{v+1}$ where v is the order of ramification of $\mathfrak{l}$. The following theorem gives a sufficient condition for $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ to have corresponding residue systems mod. $\mathfrak{l}^{v}$.

<u>Theorem</u> 3.4: Let μ_1, μ_2 be two integers of F each exactly divisible by $\mathfrak{L}$. If

$$\mu_1 \equiv \mu_2 \quad (\text{mod. } \mathfrak{L}^{a\ell+1})$$

then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1}$, that is, mod. $\mathfrak{l}^{v}$ where v is the order of ramification of $\mathfrak{l}$.

<u>Proof</u>: Since $\mu_1 \equiv \mu_2$ (mod. $\mathfrak{L}^{a\ell+1}$) and

$$(\sqrt[\ell]{\mu_1} - \sqrt[\ell]{\mu_2})^{\ell} \equiv \mu_1 - \mu_2 \quad (\text{mod. } \ell),$$

it follows that

$$\sqrt[\ell]{\mu_1} \equiv \sqrt[\ell]{\mu_2} \ (\text{mod. } \mathfrak{l}^{a(\ell-1)}).$$

Suppose

1.) $\sqrt[\ell]{\mu_1} \equiv \sqrt[\ell]{\mu_2}$ (mod. $\mathfrak{l}^{m}$) and $\sqrt[\ell]{\mu_1} \not\equiv \sqrt[\ell]{\mu_2}$ (mod. $\mathfrak{l}^{m+1}$).

For any polynomial $P(x, y)$ with integral coefficients such that both x and y occur in every term we have

$$P(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2}) \equiv P(\sqrt[\ell]{\mu_2}, \sqrt[\ell]{\mu_2}) \ (\text{mod. } \mathfrak{l}^{m}\mathfrak{l}).$$

Thus

$$(\sqrt[\ell]{\mu_1} - \sqrt[\ell]{\mu_2})^{\ell} \equiv \mu_1 - \mu_2 \ (\text{mod. } \ell\, \mathfrak{l}^{m}\mathfrak{l})$$

2.) $$(\sqrt[\ell]{\mu_1} - \sqrt[\ell]{\mu_2})^{\ell} \equiv \mu_1 - \mu_2 \ (\text{mod. } \mathfrak{L}^{a(\ell-1)}\mathfrak{l}^{m}\mathfrak{l}).$$

If

$$\mu_1 - \mu_2 \not\equiv 0 \quad (\text{mod. } \mathfrak{L}^{a(\ell-1)}\mathfrak{l}^{m}\mathfrak{l})$$

Then

$$\ell(a\ell + 1) < a\ell(\ell - 1) + m + 1$$

since $\mu_1 \equiv \mu_2$ (mod. $\mathfrak{L}^{a\ell+1}$). Therefore $\ell < -a\ell + m + 1$ and

$$a\ell + \ell - 1 < m$$

$$m \geq a\ell + 1.$$

On the other hand if

$$\mu_1 \equiv \mu_2 \ (\text{mod. } \mathfrak{L}^{a(\ell-1)} \ \mathfrak{l}^m \mathfrak{l})$$

then

$$(\sqrt[\ell]{\mu_1} - \sqrt[\ell]{\mu_2}) \equiv 0 \ (\text{mod. } \mathfrak{L}^{a(\ell-1)} \mathfrak{l}^m \mathfrak{l})$$

from 2.). Thus by 1.)

$$m\ell \geq a\ell(\ell - 1) + m + 1$$

$$m(\ell - 1) \geq a\ell(\ell - 1) + 1$$

$$m(\ell - 1) > a\ell(\ell - 1)$$

$$m > a\ell$$

and hence $m \geq a\ell + 1$. Therefore in either case $m \geq a\ell + 1$ and we have by 1.)

$$\sqrt[\ell]{\mu_1} - \sqrt[\ell]{\mu_2} \equiv 0 \ (\text{mod. } \mathfrak{l}^{a\ell+1}).$$

Let α be any integer of $F(\sqrt[\ell]{\mu_1})$ and v the order of ramification of $\mathfrak{l}$, that is, $v = a\ell + 1$. By Theorem 3.2

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu_1} + \dots + \alpha_{v-1} \sqrt[\ell]{\mu_1^{v-1}} \ (\text{mod. } \mathfrak{l}^v)$$

where the α_i are integers in F. Let

$$\beta \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu_2} + \dots + \alpha_{v-1} \sqrt[\ell]{\mu_2^{v-1}}.$$

then

$$\alpha \equiv \beta \quad (\text{mod. } \mathfrak{l}^v)$$

and $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^v$.

We now consider the case in which $(\mu, \mathfrak{L}) = (1)$ and the congruence $\mu \equiv \xi^{\ell}$ (mod. $\mathfrak{L}^{a\ell}$) is not solvable for ξ in F, that is, $(\mu, \mathfrak{L}) = (1)$ and $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu})$. Let k be the largest positive integer such that the congruence

$$\mu \equiv \xi^{\ell} \pmod{\mathfrak{L}^{k}}$$

is solvable for ξ in F. Clearly $0 < k < a\ell$ and k is the largest positive integer such that the congruence

$$\sqrt[\ell]{\mu} \equiv \xi \pmod{\mathfrak{l}^{k}}$$

is solvable for ξ in F.

Theorem 3.5: Let μ be an integer of F such that $(\mu, \mathfrak{L}) = (1)$ and $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu})$. Let k be the largest integer such that $\mu \equiv \xi^{\ell}$ (mod. $\mathfrak{L}^{k}$) is solvable for ξ in F. Then the order of ramification v of $\mathfrak{l}$ with respect to F is equal to $a\ell + 1 - k$.

Proof: Let α in F be a solution of the congruence $\mu \equiv \xi^{\ell}$ (mod. $\mathfrak{L}^{k}$) with k maximal. Since $\mu - \alpha^{\ell}$ is exactly divisible by $\mathfrak{L}^{k}$, it follows that $\sqrt[\ell]{\mu} - \alpha$ is exactly divisible by $\mathfrak{l}^{k}$. Furthermore we have $(k, \ell) = 1$ (see Hecke, Theorie der algebraischen Zahlen, page 153). Thus there exist positive integers x and y such that $kx = 1 + \ell y$.

Let π be an integer of F exactly divisible by $\mathfrak{L}$, that is $(\pi) = \mathfrak{a}\mathfrak{L}$ where $(\mathfrak{a}, \mathfrak{L}) = (1)$ and $\mathfrak{a}$ is an ideal of F. There exists an ideal $\mathfrak{c}$ in F such that $\mathfrak{a}\mathfrak{c} = (\omega)$ is principal and $\mathfrak{c}$ is prime to $\mathfrak{L}$.

Now, let

$$\rho = \frac{(\sqrt[\ell]{\mu} - \alpha)^{x}}{\pi^{y}} .$$

Then

$$(\rho) = \frac{(\sqrt[\ell]{\mu} - \alpha)^x}{\sigma^y \; \mathfrak{L}^y} = \frac{(\sqrt[\ell]{\mu} - \alpha)^x \tau^y}{\sigma^y \; \mathfrak{L}^y \tau^y}$$

$$(\rho) = \frac{(\sqrt[\ell]{\mu} - \alpha)^x \tau^y}{(\omega^y) \; \mathfrak{L}^y}$$

Hence

$$(\omega^y \rho) = \frac{(\sqrt[\ell]{\mu} - \alpha)^x \tau^y}{\mathfrak{L}^y} \quad .$$

The ideal fraction on the right in the last equation is an integral ideal exactly divisible by $\mathfrak{l}$. It follows that $\omega^y \rho$ is an integer of $F(\sqrt[\ell]{\mu})$ exactly divisible by $\mathfrak{l}$. Let

$$\theta = \omega^y \rho = \frac{\omega^y (\sqrt[\ell]{\mu} - \alpha)^x}{\pi^y} \quad .$$

Since θ is exactly divisible by $\mathfrak{l}$ it follows from Theorem 1.13 that the order of ramification of $\mathfrak{l}$ is equal to v if and only if $\theta - \theta^A$ is exactly divisible by $\mathfrak{l}^v$ where A is the automorphism $\sqrt[\ell]{\mu} \to \zeta \sqrt[\ell]{\mu}$, that is, if and only if

$$\frac{\omega^y (\sqrt[\ell]{\mu} - \alpha)^x}{\pi^y} - \frac{\omega^y (\zeta \sqrt[\ell]{\mu} - \alpha)^x}{\pi^y}$$

is exactly divisible by $\mathfrak{l}^v$. Since $(\omega, \mathfrak{L}) = (1)$ this is true if and only if

$$(\sqrt[\ell]{\mu} - \alpha)^x - (\zeta \sqrt[\ell]{\mu} - \alpha)^x$$

is exactly divisible by $\mathfrak{L}^y \mathfrak{l}^v = \mathfrak{l}^{kx-1} \mathfrak{l}^v$. Now

$$(\zeta \sqrt[\ell]{\mu} - \alpha)^x = \left[(\zeta \sqrt[\ell]{\mu} - \sqrt[\ell]{\mu}) + (\sqrt[\ell]{\mu} - \alpha) \right]^x$$

$$= (\sqrt[\ell]{\mu} - \alpha)^x + x (\sqrt[\ell]{\mu} - \alpha)^{x-1} (\zeta \sqrt[\ell]{\mu} - \sqrt[\ell]{\mu}) + \dots$$

Therefore

$$(\zeta \sqrt[\ell]{\mu} - \alpha)^x \equiv (\sqrt[\ell]{\mu} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{k(x-1)}(1-\zeta))$$
$$\equiv (\sqrt[\ell]{\mu} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{k(x-1)} \mathfrak{l}^{a\ell})$$

since $0 < k < a\ell$ and $(1 - \zeta) = \mathfrak{L}^a \mathfrak{a}$ with $(\mathfrak{L}, \mathfrak{a}) = (1)$. Furthermore this congruence holds exactly mod. $\mathfrak{l}^{k(x-1)}\mathfrak{l}^{a\ell}$. It follows that

$$kx - 1 + v = k(x-1) + a\ell$$
$$v = a\ell + 1 - k\,.$$

Theorem 3.6: Let μ_1, μ_2 be two integers of F each prime to $\mathfrak{L}$ and such that $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$. Let k_i be the largest integer such that the congruence $\mu_i \equiv \xi_i^{\ell}$ (mod. $\mathfrak{L}^{k_i}$) is solvable for ξ_i an integer in F($i = 1, 2$). Let $v_i = a\ell + 1 - k_i$ for $i = 1, 2$ and suppose $v_1 \geq v_2 > a$. Then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{v_2 - a}$.

Proof: Since $\mu_i - \xi_i^{\ell}$ is exactly divisible by $\mathfrak{L}^{k_i}$, then $\sqrt[\ell]{\mu_i} - \xi_i$ is exactly divisible by $\mathfrak{l}^{k_i}(i = 1, 2)$. Since $(k_i, \ell) = 1$ we have positive integers x_i and y_i such that $k_i x_i = 1 + \ell y_i (i = 1,2)$. Let π be an integer of F exactly divisible by $\mathfrak{L}$. Using the method of Theorem 3.5 we obtain an integer of $F(\sqrt[\ell]{\mu_i})$

$$\theta_i = \frac{\omega^{y_i}(\sqrt[\ell]{\mu_i} - \xi_i)^{x_i}}{\pi^{y_i}} \qquad i = 1, 2$$

which is exactly divisible by $\mathfrak{l}$.

We now show that θ_i^{ℓ} is congruent to an integer in F mod. $\mathfrak{L}^{v_i - a}$ for $i = 1, 2$. We have

$$\theta_i^{\ell} = \frac{\omega^{y_i \ell}(\sqrt[\ell]{\mu_i} - \xi_i)^{x_i \ell}}{\pi^{y_i \ell}} = \frac{\omega^{y_i \ell}(\lambda_i + \rho_i \ell)^{x_i}}{\pi^{y_i \ell}}$$

where λ_i is an integer of F and $\lambda_i \equiv 0 \pmod{\mathfrak{L}^{k_i}}$. Hence

$$\theta_i^{\ell} = \frac{\omega^{y_i \ell}(\lambda_i^{x_i} + x_i \lambda_i^{x_i - 1}\rho_i \ell + \ldots)}{\pi^{y_i \ell}}$$

$$= \frac{\omega^{y_i \ell}\lambda_i^{x_i}}{\pi^{y_i \ell}} + \frac{(\omega^{y_i \ell} x_i \lambda_i^{x_i - 1}\rho_i \ell + \ldots)}{\pi^{y_i \ell}}$$

$$\equiv \frac{\omega^{y_i \ell}\lambda_i^{x_i}}{\pi^{y_i \ell}} \quad (\text{mod. } \mathfrak{L}^{a\ell + 1 - k_i - a})$$

$$\equiv \frac{\omega^{y_i \ell}\lambda_i^{x_i}}{\pi^{y_i \ell}} \quad (\text{mod. } \mathfrak{L}^{v_i - a}).$$

But $\nu_i = \frac{\omega^{y_i \ell}\lambda_i^{x_i}}{\pi^{y_i \ell}}$ is an integer of F, so that θ_i^{ℓ} is congruent to an integer ν_i of F mod. $\mathfrak{L}^{v_i - a}$ for $i = 1, 2$.

We now show that the ℓ^{th} power of every integer of $F(\sqrt[\ell]{\mu_i})$ is congruent to an integer of F mod. $\mathfrak{L}^{v_i - a}$ for $i = 1, 2$.

Let β be any integer of $F(\sqrt[\ell]{\mu_1})$ and let $n = v_1 - a$. Since θ_1 is exactly divisible by $\mathfrak{l}$

$$\beta \equiv \beta_o + \beta_1 \theta_1 + \ldots + \beta_{n-1}\theta_1^{n-1} \quad (\text{mod. } \mathfrak{l}^n)$$

where the β_i are residues mod. $\mathfrak{l}$ and may be chosen in F since $\mathfrak{l}$ is of degree 1 over F. Hence

$$\left[\beta - (\beta_o + \ldots + \beta_{n-1}\theta_1^{n-1})\right]^{\ell} \equiv \beta^{\ell} - (\beta_o + \ldots + \beta_{n-1}\theta_1^{n-1})^{\ell} (\text{mod } .\ell)$$

$$\equiv \beta^{\ell} - (\beta_o^{\ell} + \ldots + \beta_{n-1}^{\ell}\theta_1^{\ell(n-1)}) \quad (\text{mod. } \ell)$$

$$\equiv \beta^{\ell} - \sigma \quad (\text{mod. } \mathfrak{L}^{v_1 - a})$$

where σ is an integer of F. It follows that

$$\beta^{\ell} \equiv \sigma \pmod{\lambda^{v_1-a}}.$$

If β and β' are two integers of $F(\sqrt[\ell]{\mu_1})$ such that

$$\beta^{\ell} \equiv \sigma \pmod{\lambda^{v_1-a}} \text{ and } \beta'^{\ell} \equiv \sigma \pmod{\lambda^{v_1-a}}$$

then

$$\beta \equiv \beta' \pmod{\mathfrak{l}^{v_1-a}}.$$

Also if

$$\beta^{\ell} \equiv \sigma \pmod{\lambda^{v_1-a}} \text{ and } \beta \equiv \sigma' \pmod{\lambda^{v_1-a}}$$

where σ, σ' are integers of F, then $\sigma \equiv \sigma' \pmod{\lambda^{v_1-a}}$.

The number of residue classes mod. $\mathfrak{l}^{v_1-a}$ in $F(\sqrt[\ell]{\mu_1})$ is equal to the number of residue classes mod. λ^{v_1-a} in F. It follows that if σ is any integer of F there exists an integer β of $F(\sqrt[\ell]{\mu_1})$ such that

$$\beta^{\ell} \equiv \sigma \pmod{\lambda^{v_1-a}}.$$

In the same way, if γ is any integer of $F(\sqrt[\ell]{\mu_2})$ there exists an integer τ of F such that

$$\gamma^{\ell} \equiv \tau \pmod{\lambda^{v_2-a}}.$$

There exists an integer β of $F(\sqrt[\ell]{\mu_1})$ such that

$$\beta^{\ell} \equiv \tau \pmod{\lambda^{v_1-a}}.$$

Since $v_1 \geq v_2$

$$\beta^{\ell} \equiv \gamma^{\ell} \pmod{\lambda^{v_2-a}}.$$

But

$$(\beta - \gamma)^{\ell} \equiv \beta^{\ell} - \gamma^{\ell} \pmod{\ell}$$

and therefore

$$\beta \equiv \gamma \pmod{\mathfrak{l}^{v_2-a}}.$$

Thus $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{v_2-a}$.

By combining Theorems 3.3 and 3.6 we have the following result.

<u>Theorem</u> 3.7: If μ_1, μ_2 are two integers of F such that $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$, and $\mathfrak{l}$ has ramification orders $\geq v > a$ in $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ over F, then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{v-a}$.

<u>Proof</u>: We need only to consider the case in which μ_1 is exactly divisible by $\mathfrak{L}$ and μ_2 is prime to $\mathfrak{L}$, the other two cases following from Theorems 3.3 and 3.6. Let $v_1 = a\,\ell + 1$ be the order of ramification of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu_1})$ over F, and let v_2 be the order of ramification of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu_2})$ over F. From Theorem 3.5 it follows that $v_1 - 1 = a\,\ell \geq v_2$.

Let α be any integer of $F(\sqrt[\ell]{\mu_1})$ and let $n = a\,\ell - a$. Since $\sqrt[\ell]{\mu_1}$ is exactly divisible by $\mathfrak{l}$, it follows that

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu_1} + \cdots + \alpha_{n-1} \sqrt[\ell]{\mu_1^{n-1}} \quad (\text{mod. } \mathfrak{l}^n)$$

where the α_i are integers of F. Hence

$$\alpha^\ell \equiv \alpha_0^\ell + \alpha_1^\ell\ \mu_1 + \cdots + \alpha_{n-1}^\ell\ \mu_1^{n-1} \quad (\text{mod. } \mathfrak{L}^n)$$

$$\alpha^\ell \equiv \sigma \quad (\text{mod. } \mathfrak{L}^{a\,\ell - a})$$

where σ is an integer of F. Using the method of Theorem 3.6, there exists an integer β of $F(\sqrt[\ell]{\mu_2})$ such that

$$\beta^\ell \equiv \sigma \quad (\text{mod. } \mathfrak{L}^{v_2-a}).$$

Therefore

$$\alpha^\ell \equiv \beta^\ell \quad (\text{mod. } \mathfrak{L}^{v_2-a}).$$

$$\alpha \equiv \beta \quad (\text{mod. } \mathfrak{l}^{v_2 - a}).$$

Thus $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{v-a}$ where $v_2 \geq v > a$.

<u>Theorem</u> 3.8: Let μ_1, μ_2 be two integers of F, each prime to $\mathfrak{L}$, such that $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$. Suppose $\mu_1 \equiv \mu_2$ (mod. $\mathfrak{L}^{a\ell}$) and let k be the largest integer such that the congruences $\mu_1 \equiv \alpha^{\ell}$ (mod. $\mathfrak{L}^k$) and $\mu_2 \equiv \alpha^{\ell}$ (mod. $\mathfrak{L}^k$) are solvable for α an integer of F. Then $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^v$ where $v = a\ell + 1 - k$.

<u>Proof</u>: Since $\mu_1 \equiv \mu_2$ (mod. $\mathfrak{L}^{a\ell}$), it follows that

$$\sqrt[\ell]{\mu_1} \equiv \sqrt[\ell]{\mu_2} \quad (\text{mod. } \mathfrak{L}^a)$$

using the method of Theorem 3.4. We have $k\,x = 1 + \ell\,y$ and following Theorem 3.5 it is sufficient to show that

$$(\sqrt[\ell]{\mu_1} - \alpha)^x \equiv (\sqrt[\ell]{\mu_2} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{v+\ell y}).$$

We have

$$(\sqrt[\ell]{\mu_2} - \alpha)^x = \left[(\sqrt[\ell]{\mu_1} - \alpha) + (\sqrt[\ell]{\mu_2} - \sqrt[\ell]{\mu_1}) \right]^x$$

$$= (\sqrt[\ell]{\mu_1} - \alpha)^x + x(\sqrt[\ell]{\mu_1} - \alpha)^{x-1}(\sqrt[\ell]{\mu_2} - \sqrt[\ell]{\mu_1}) + \cdots$$

$$\equiv (\sqrt[\ell]{\mu_1} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{k(x-1)}\ \mathfrak{l}^{a\ell})$$

$$\equiv (\sqrt[\ell]{\mu_1} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{1+\ell y - k}\ \mathfrak{l}^{a\ell})$$

$$\equiv (\sqrt[\ell]{\mu_1} - \alpha)^x \quad (\text{mod. } \mathfrak{l}^{v+\ell y}).$$

Thus $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^v$ where $v = a\ell + 1 - k$ is the order of ramification of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$.

We remark that if $F(\sqrt[\ell]{\mu_1}) \neq F(\sqrt[\ell]{\mu_2})$ then $\sqrt[\ell]{\mu_1} \not\equiv \sqrt[\ell]{\mu_2} \pmod{\mathfrak{l}^{a\ell+1}}$, for otherwise we would have corresponding residue systems mod. $\mathfrak{l}^{v+1}$ contrary to Theorem 2.7.

A necessary and sufficient condition for $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ to have corresponding residue systems mod. $\mathfrak{l}^{v}$ is not known to the author (where v is the smaller of the ramification orders of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ over F). The following theorem shows that in case $v = a\ell$ $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell}$ if and only if μ_1 and μ_2 satisfy a system of congruences and an example is given to show that this system is not always solvable.

<u>Theorem</u> 3.9: If $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a}$ then the following congruences must be solvable

1) $\mu_1 \equiv \alpha_0^\ell + \alpha_1^\ell \mu_2 + \cdots + \alpha_{\ell-1}^\ell \mu_2^{\ell-1} \pmod{\mathfrak{l}^{a\ell-a}}$

2) $$\frac{1}{\ell}\left\{\mu_1 - (\alpha_0^\ell + \cdots + \alpha_{\ell-1}^\ell \mu_2^{\ell-1})\right\} \equiv \sum_{\substack{e_0+\cdots+e_{\ell-1}=\ell,\ e_j \neq \ell,\ j=0,\ldots,\ell-1 \\ e_1+2e_2+\cdots+(\ell-1)e_{\ell-1}=m\ell}} \frac{(\ell-1)!}{e_0!\cdots e_{\ell-1}!}\alpha_0^{e_0}\cdots\alpha_{\ell-1}^{e_{\ell-1}}\mu_2^{m} \pmod{\mathfrak{l}^{a}}$$

3) $$\sum_{\substack{e_0+\cdots+e_{\ell-1}=\ell,\ e_j \neq \ell,\ j=0,\ldots,\ell-1 \\ e_1+2e_2+\cdots+(\ell-1)e_{\ell-1}=m\ell+i}} \frac{(\ell-1)!}{e_0!\cdots e_{\ell-1}!}\alpha_0^{e_0}\cdots\alpha_{\ell-1}^{e_{\ell-1}}\mu_2^{m} \equiv 0 \pmod{\mathfrak{l}^{a}}$$

where $\alpha_0, \ldots, \alpha_{\ell-1}$ are integers of F and $e_1, \ldots, e_{\ell-1}$, m are positive integers and $i = 1, \ldots, \ell - 1$, and conversely.

<u>Proof</u>: Since $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a}$ it follows that $1, \sqrt[\ell]{\mu_2}, \ldots, \sqrt[\ell]{\mu_2^{\ell-1}}$ is a basis for the residue system mod. $\mathfrak{l}^{a}$ in $F(\sqrt[\ell]{\mu_2})$. Thus

$$\sqrt[\ell]{\mu_1} \equiv \alpha_0 + \alpha_1 \sqrt[\ell]{\mu_2} + \cdots + \alpha_{\ell-1} \sqrt[\ell]{\mu_2^{\ell-1}} \pmod{\mathfrak{L}^a}$$

where the α_i are integers of F. Therefore

$$\mu_1 \equiv (\alpha_0 + \alpha_1 \sqrt[\ell]{\mu_2} + \cdots + \alpha_{\ell-1} \sqrt[\ell]{\mu_2^{\ell-1}})^\ell \pmod{\mathfrak{L}^{a\ell}}$$

and it follows that

$$\frac{1}{\ell}\left\{(\alpha_0+\alpha_1 \sqrt[\ell]{\mu_2}+\cdots+\alpha_{\ell-1} \sqrt[\ell]{\mu_2^{\ell-1}})^\ell - (\alpha_0^\ell+\alpha_1^\ell \mu_2+\cdots+\alpha_{\ell-1}^\ell \mu_2^{\ell-1})\right\}$$

is congruent to a number of F mod. $\mathfrak{L}^a$. Since $1, \sqrt[\ell]{\mu_2}, \ldots, \sqrt[\ell]{\mu_2^{\ell-1}}$ is a basis for the residue system mod. $\mathfrak{L}^a$, the coefficients of $\sqrt[\ell]{\mu_2^i}$ must vanish mod. $\mathfrak{L}^a$. Thus the congruences

$$\sum_{\substack{e_0+\cdots+e_{\ell-1}=\ell,\ e_j\neq\ell,\ j=0,\ldots,\ell-1 \\ e_1+2e_2+\cdots+(\ell-1)e_{\ell-1}=m\ell+i}} \frac{(\ell-1)!}{e_0!\cdots e_{\ell-1}!}\alpha_0^{e_0}\cdots\alpha_{\ell-1}^{e_{\ell-1}}\mu_2^m \equiv \begin{cases} \frac{1}{\ell}\{\mu_1-(\alpha_0^\ell+\alpha_1^\ell\mu_2+\cdots+\alpha_{\ell-1}^\ell\mu_2^{\ell-1})\}, & i=0 \\ 0 \quad \text{for} \quad i=1,\ldots,\ell-1 \end{cases}$$

are solvable for $i = 1, \ldots, \ell - 1$ and $i = 0$ mod. $\mathfrak{L}^a$.

In Theorem 3.10 we consider a special case of Theorem 3.9 in which $F = R(\zeta)$ and $\ell = 3$.

<u>Theorem</u> 3.10: If $F = R(\zeta)$, $\ell = 3$, and $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $(1 - \zeta)$, then either

$$\mu_1 \equiv \alpha^3 \mu_2^\epsilon \pmod{3(1-\zeta)}$$

for α in $R(\zeta)$ and $\epsilon = 1$ or 2, or

$$\mu_1 \equiv \mu_2 \equiv 0 \pmod{(1-\zeta)}.$$

<u>Proof</u>: In $R(\zeta)$ the ideal $(1 - \zeta)$ is a prime ideal, that is, $(1 - \zeta) = \mathfrak{L}$. Since $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $(1 - \zeta)$ we have $(1 - \zeta) = \mathfrak{l}^\ell$ and the orders of ramification of $\mathfrak{l}$ in $F(\sqrt[\ell]{\mu_1})$, $F(\sqrt[\ell]{\mu_2})$ over $R(\zeta)$ are $\geq \ell$ and

hence either ℓ or $\ell + 1$. If the order of ramification of l in $F(\sqrt[\ell]{\mu_1})$ over $R(\zeta)$ is $\ell + 1$, then μ_1 may be chosen exactly divisible by $\mathcal{L} = (1 - \zeta)$ and $1, \sqrt[3]{\mu_1}, \sqrt[3]{\mu_1^2}$ is a basis for the residue system mod. $(1 - \zeta)$ in $F(\sqrt[\ell]{\mu_1})$. If the order of ramification of l in $F(\sqrt[\ell]{\mu_1})$ over $R(\zeta)$ is equal to ℓ, then $k = 1$ is the largest integer such that the congruence $\mu_1 \equiv \xi^{\ell}$ (mod. $\mathcal{L}^k$) has a solution ξ in $R(\zeta)$. In this case $\sqrt[\ell]{\mu_1} - \xi$ is exactly divisible by l, and again $1, \sqrt[3]{\mu_1}, \sqrt[3]{\mu_1^2}$ is a basis for the residue system mod. $(1 - \zeta)$ in $F(\sqrt[\ell]{\mu_1})$ over $R(\zeta)$. The same statements are valid for $\sqrt[\ell]{\mu_2}$.

Since $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $(1 - \zeta)$, we must have

1.) $\sqrt[3]{\mu_1} \equiv \alpha_0 + \alpha_1 \sqrt[3]{\mu_2} + \alpha_2 \sqrt[3]{\mu_2^2}$ (mod. $(1-\zeta)$)

2.) $\mu_1 \equiv \alpha_0^3 + \alpha_1^3 \mu_2 + \alpha_2^3 \mu_2^2 + 3\, P(\sqrt[3]{\mu_2})$ (mod. $3(1-\zeta)$)

where $P(x)$ is a polynomial with coefficients in $R(\zeta)$. It follows that $P(\sqrt[3]{\mu_2})$ is congruent to a number in $R(\zeta)$ mod. $(1 - \zeta)$. Since $1, \sqrt[3]{\mu_2}, \sqrt[3]{\mu_2^2}$ is a basis of the residue system mod. $(1 - \zeta)$ in $F(\sqrt[3]{\mu_2})$ the coefficients of $\sqrt[3]{\mu_2}$ and $\sqrt[3]{\mu_2^2}$ must vanish. Hence

3.) $\alpha_0^2 \alpha_1 + \alpha_0 \alpha_2^2 \mu_2 + \alpha_1^2 \alpha_2 \mu_2 \equiv 0$ (mod. $(1-\zeta)$)

4.) $\alpha_0 \alpha_1^2 + \alpha_1 \alpha_2^2 \mu_2 + \alpha_0^2 \alpha_2 \equiv 0$ (mod. $(1-\zeta)$)

We consider two cases: $\mu_2 \equiv 0$ (mod. $(1-\zeta)$) and $\mu_2 \not\equiv 0$ (mod. $(1-\zeta)$).

Suppose $\mu_2 \equiv 0$ (mod. $(1-\zeta)$). This implies that α_0 or $\alpha_1 \equiv 0$ (mod. $(1-\zeta)$) from 3.). If $\alpha_0 \equiv 0$ (mod. $(1-\zeta)$), then $\mu_1 \equiv 0$ (mod. $(1-\zeta)$) from 2.). If $\alpha_0 \not\equiv 0$ (mod. $(1-\zeta)$) and

$\alpha_1 \equiv 0$ (mod. $(1-\zeta)$), then $\alpha_2 \equiv 0$ (mod. $(1-\zeta)$) by 4.) and therefore from 2.) we have $\mu_1 \equiv \alpha_o^3$ (mod. $3(1-\zeta)$). But the last congruence means that $(1-\zeta)$ is not an ℓ^{th} power in $F(\sqrt[\ell]{\mu_1})$ and hence we can't have corresponding residue systems mod. $\mathfrak{l}$. Thus if $\mu_2 \equiv 0$ (mod. $(1-\zeta)$), then $\mu_1 \equiv 0$ (mod. $(1-\zeta)$) - provided we have corresponding residue systems mod. $(1-\zeta)$.

Suppose $\mu_2 \not\equiv 0$ (mod. $(1-\zeta)$). If $\alpha_o \equiv 0$ (mod. $(1-\zeta)$) then either α_1 or $\alpha_2 \equiv 0$ (mod. $(1-\zeta)$) from 3.). It follows from 1.) that $\sqrt[3]{\mu_1} \equiv \alpha \sqrt[3]{\mu_2^{\epsilon}}$ (mod. $(1-\zeta)$) where $\alpha = \alpha_1$ or α_2 is in $R(\zeta)$ and $\epsilon = 1$ or 2. Hence $\mu_1 \equiv \alpha^3 \mu_2^{\epsilon}$ (mod. $3(1-\zeta)$). We note that if both α_1 and $\alpha_2 \equiv 0$ (mod. $(1-\zeta)$), then $\mu_1 \equiv 0$ (mod. $(1-\zeta)$) from 2.) which is impossible by the first case.

If $\alpha_o \not\equiv 0$ (mod. $(1-\zeta)$) and either $\alpha_1 \equiv 0$ (mod. $(1-\zeta)$) or $\alpha_2 \equiv 0$ (mod. $(1-\zeta)$), then from 3.) it follows that $\alpha_1 \equiv \alpha_2 \equiv 0$ (mod. $(1-\zeta)$). Hence from 2.) we have $\mu_1 \equiv \alpha_o^3$ (mod. $3(1-\zeta)$) which is impossible as in the first case.

If $\alpha_o \not\equiv 0$ (mod. $(1-\zeta)$), $\alpha_1 \not\equiv 0$ (mod. $(1-\zeta)$), and $\alpha_2 \not\equiv 0$ (mod. $(1-\zeta)$), then $\alpha_o^2 \equiv \alpha_1^2 \equiv \alpha_2^2 \equiv \mu_2^2 \equiv 1$ (mod. $(1-\zeta)$) and it follows from 4.) that $\alpha_o + \alpha_1 \mu_2 + \alpha_2 \mu_2^2 \equiv 0$ (mod. $(1-\zeta)$). Hence $\alpha_o + \alpha_1 \sqrt[3]{\mu_2} + \alpha_2 \sqrt[3]{\mu_2^2} \equiv 0$ (mod. $\mathfrak{l}$). It follows from 1.) that $\sqrt[3]{\mu_1} \equiv 0$ (mod. $\mathfrak{l}$) and therefore $\mu_1 \equiv 0$ (mod. $(1-\zeta)$). It follows from the first case that $\mu_2 \equiv 0$ (mod. $(1-\zeta)$) since the roles of μ_1 and μ_2 in case one may be interchanged, which completes the proof.

If $F = R(\zeta)$, $\ell = 3$, $\mu_1 = 2$ and $\mu_2 = 5$, the congruences of Theorem 3.10 are not solvable. For if

$$5 \equiv 2\alpha^3 \pmod{3(1-\zeta)}$$

then

$$5 = 2a + 2b\zeta + 2c\zeta^2 + (d + e\zeta + f\zeta^2)(3)(1-\zeta)$$

where a, b, ..., f are rational integers. This means that

$$3d - 3f + 2a = 5$$

$$-3d + 3e + 2b = 0$$

$$3f - 3e + 2c = 0 \ .$$

Thus, from the last two equations,

$$3f - 3d \equiv 0 \pmod{4}$$

which is impossible by the first equation. Thus $5 \not\equiv 2\alpha^3 \pmod{3(1-\zeta)}$ and in the same manner it follows that $5 \not\equiv 4\alpha^3 \pmod{3(1-\zeta)}$. It follows that the congruences of Theorem 3.9 are not solvable.

CHAPTER IV

CORRESPONDING RESIDUE SYSTEMS IN FIELDS $F(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_r})$ AND $F(\sqrt[\ell^m]{\mu})$

Let ℓ be a rational prime, $\zeta \neq 1$ an ℓ^{th} root of unity, and F a number field containing ζ. In this chapter we consider the problem of corresponding residue systems for fields of the type $F(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_r})$ and $F(\sqrt[\ell^m]{\mu})$ where $\mu, \mu_1, \ldots, \mu_r$ are integers of F (but not ℓ^{th} powers of integers of F). As in Chapter III let $(1 - \zeta) = \mathfrak{L}^a \mathfrak{a}$ where $\mathfrak{L}$ is a prime ideal in F, $\mathfrak{a}$ is an ideal of F, and $(\mathfrak{L}, \mathfrak{a}) = (1)$.

Theorem 4.1: Let $F' = F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$ where μ_1, μ_2 are integers of F, and let $\mathfrak{f}$ be a prime ideal of F' such that $(\mathfrak{f}, \ell) = (1)$. Then $\mathfrak{f}$ is not of order ℓ^2 with respect to F.

Proof: Let $\mathfrak{f}$ in F' correspond to the prime ideal $\mathfrak{p}$ in F. If either μ_1 or μ_2 is prime to $\mathfrak{p}$, then by Theorem 1.16 $\mathfrak{f}$ is not of order ℓ^2 with respect to F.

Suppose both μ_1, μ_2 are exactly divisible by $\mathfrak{p}$. Then $\mathfrak{p} = \mathfrak{p}_1^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ where $\mathfrak{p}_1$ is a prime ideal in $F(\sqrt[\ell]{\mu_1})$. Thus μ_2 is exactly divisible by $\mathfrak{p}_1^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$. Hence there exists an integer μ_2' in $F(\sqrt[\ell]{\mu_1})$ such that $(\mathfrak{p}_1, \mu_2') = (1)$ and $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2}) = F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2'})$ (See Hecke, Theorie der algebraischen Zahlen, page 151). It follows from Theorem 1.16 that $\mathfrak{p}_1$ is not an ℓ^{th} power in $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2'}) = F'$. Therefore $\mathfrak{f}$ is not of order ℓ^2 with respect to F.

Corollary 4.1.1: Let $F' = F(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_r})$ where $\mu_1, \ldots, \mu_r$ are integers of F and let $\mathfrak{q}$ be a prime ideal in F' such that $(\mathfrak{q}, \ell) = (1)$. Suppose $(F' \mid F) = \ell^r$ with $r > 1$ and let F'' be a number field such that $F'' \cap F' = F$. Then F' and F'' do not have corresponding residue systems mod. $\mathfrak{q}$.

Proof: The corollary follows from Theorem 2.5 and Theorem 4.1.

Let $F' \supset F$, $(F' \mid F) = \ell^2$, and let $\mathfrak{q}$ be a prime ideal in F' such that $(\mathfrak{q}, \ell) = (1)$. It is interesting to note that while $\mathfrak{q}$ is not of order ℓ^2 with respect to F in case $F' = F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$, $\mathfrak{q}$ may be of order ℓ^2 with respect to F in case $F' = F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\theta})$ where θ is an integer of $F(\sqrt[\ell]{\mu_1})$. For example let $\mathfrak{p}$ be a prime ideal of F such that $(\mathfrak{p}, \ell) = (1)$ and let μ be an integer of F exactly divisible by $\mathfrak{p}$. From Theorem 1.16 it follows that $\mathfrak{p} = \mathfrak{p}_1^{\ell}$ in $F(\sqrt[\ell]{\mu})$ and $\mathfrak{p}_1 = \mathfrak{p}_2^{\ell}$ in $F(\sqrt[\ell]{\mu}, \sqrt[\ell^2]{\mu}) = F(\sqrt[\ell^2]{\mu})$, so that $\mathfrak{p}_2$ is of order ℓ^2 with respect to F.

Theorem 4.2: Let μ_1, μ_2 be integers of F such that $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{L}^a$. If $\mathfrak{l}_1$ is a prime divisor of $\mathfrak{L}$ in $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$, then $\mathfrak{l}_1$ is not of order ℓ^2 with respect to F.

Proof: We may assume that $F(\sqrt[\ell]{\mu_1}) \neq F(\sqrt[\ell]{\mu_2})$. Since $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{L}^a$, it follows that $\mathfrak{L} = \mathfrak{l}^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and in $F(\sqrt[\ell]{\mu_2})$. Suppose $(\mu_2, \mathfrak{L}) = (1)$. There exists an integer α of $F(\sqrt[\ell]{\mu_1})$ such that $\sqrt[\ell]{\mu_2} \equiv \alpha \pmod{\mathfrak{L}^a}$. Since

$$(\sqrt[\ell]{\mu_2} - \alpha)^{\ell} = \mu_2 - \alpha^{\ell} \quad (\text{mod. } \ell \mathfrak{L}^a)$$

it follows that

$$\mu_2 \equiv \alpha^{\ell} \quad (\text{mod. } \mathfrak{l}^{a\ell^2}) .$$

But this means that $\mathfrak{l}$ is not an ℓ^{th} power in $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$ by Theorem 1.17. Hence if $\mathfrak{l}_1$ is a prime divisor of $\mathfrak{L}$ in $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$, then $\mathfrak{l}_1$ is not of order ℓ^2 with respect to F.

Suppose both μ_1, μ_2 are exactly divisible by $\mathfrak{L}$. Let

$$(\mu_1) = \mathfrak{a}_1 \mathfrak{L} \qquad (\mathfrak{a}_1, \mathfrak{L}) = (1)$$

$$(\mu_2) = \mathfrak{a}_2 \mathfrak{L} \qquad (\mathfrak{a}_2, \mathfrak{L}) = (1)$$

where $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of F. Then

$$\frac{(\mu_2)}{(\mu_1)} = \frac{\mathfrak{a}_2 \mathfrak{L}}{\mathfrak{a}_1 \mathfrak{L}} = \frac{\mathfrak{a}_2}{\mathfrak{a}_1} \quad .$$

There exists an ideal $\mathfrak{c}$ of F such that $\mathfrak{a}_1 \mathfrak{c} = (\omega)$ is principal and $(\mathfrak{c}, \mathfrak{L}) = (1)$. Thus

$$\frac{(\mu_2)}{(\mu_1)} = \frac{\mathfrak{a}_2}{\mathfrak{a}_1} = \frac{\mathfrak{a}_2 \mathfrak{c}}{\mathfrak{a}_1 \mathfrak{c}} = \frac{\mathfrak{a}_2 \mathfrak{c}}{(\omega)}$$

$$\frac{(\omega)(\mu_2)}{(\mu_1)} = \mathfrak{a}_2 \mathfrak{c}$$

Since $\mathfrak{a}_2 \mathfrak{c}$ is an integral ideal of F, it follows that $\dfrac{\omega \mu_2}{\mu_1}$ is an integer of F prime to $\mathfrak{L}$. Hence

$$\rho = \frac{\omega^{\ell} \mu_2}{\mu_1}$$

is an integer of F prime to $\mathfrak{L}$. Since

$$\rho \mu_2^{\ell-1} = \frac{\omega^\ell \mu_2}{\mu_1} \cdot \mu_2^{\ell-1} = \frac{\omega^\ell \mu_2^\ell}{(\sqrt[\ell]{\mu_1})^\ell}$$

is the ℓ^{th} power of a number in $F(\sqrt[\ell]{\mu_1})$, it follows (see Hecke, Theorie der algebraischen Zahlen, page 149) that $F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\rho})$ $= F(\sqrt[\ell]{\mu_1}, \sqrt[\ell]{\mu_2})$. Therefore the case in which both μ_1, μ_2 are exactly divisible by $\mathfrak{L}$ reduces to the case in which one of μ_1, μ_2 is prime to $\mathfrak{L}$.

<u>Corollary</u> 4.2.1: Let $F' = F(\sqrt[\ell]{\mu_1}, \ldots, \sqrt[\ell]{\mu_r})$ where $\mu_1, \ldots, \mu_r$ are integers of F, and let F" be any number field such that $F' \cap F'' = F$. If $F(\sqrt[\ell]{\mu_i})$ and $F(\sqrt[\ell]{\mu_j})$ have corresponding residue systems mod. $\mathfrak{L}^a$ for any pair μ_i, μ_j of the integers $\mu_1, \ldots, \mu_r$ such that $F(\sqrt[\ell]{\mu_i}) \neq F(\sqrt[\ell]{\mu_j})$, then F' and F" do not have corresponding residue systems mod. any divisor of $\mathfrak{L}$.

<u>Proof</u>: The corollary follows from Theorems 2.5 and 4.2.

In the remainder of this chapter we consider fields of the type $F(\sqrt[\ell^m]{\mu})$ where m is a positive integer and μ is an integer of F and not the ℓ^{th} power of an integer in F. Let $\mathfrak{q}$ be a prime ideal in $F(\sqrt[\ell^m]{\mu_1}) = F_1$ and in $F(\sqrt[\ell^m]{\mu_2}) = F_2$. In order that F_1 and F_2 have corresponding residue systems mod. $\mathfrak{q}$ it is necessary and sufficient that $\mathfrak{q}$ be of order ℓ^m in F_1 and F_2 over F. Therefore it is necessary that $\mathfrak{q}$ divide the relative differentes $\underset{F_1\ F}{\mathfrak{D}}$ and $\underset{F_2\ F}{\mathfrak{D}}$. The relative number differente of $\sqrt[\ell^m]{\mu_i}$ over F is equal to $(\sqrt[\ell^m]{\mu_i})^{\ell^m-1}\ell^m$ and therefore

$$(\sqrt[\ell^m]{\mu_i})^{\ell^m-1}\ell^m = \mathfrak{C}_i \underset{F_i\ F}{\mathfrak{D}} \qquad (i = 1, 2)$$

where $\mathfrak{C}_i$ is the relative conductor of $\sqrt[\ell^m]{\mu_i}$ over F. Hence it is necessary that $\mathfrak{q}$ divide $(\sqrt[\ell^m]{\mu_i})^{\ell^{m-1}}\ell^m$ for i = 1, 2.

We consider first the case in which $\mathfrak{q}$ is prime to ℓ. Let $\mathfrak{q}$ correspond to the prime ideal $\mathfrak{p}$ in F. The ideal $\mathfrak{p}$ becomes an ℓ^{th} power in $F(\sqrt[\ell]{\mu})$ if and only if $(\mu) = \mathfrak{p}^a\mathfrak{a}$ with $(\mathfrak{p}, \mathfrak{a}) = (1)$ and $(a, \ell) = 1$ by Theorem 2.1. Suppose

$$(\mu) = \mathfrak{p}^a\mathfrak{a} \text{ with } (\mathfrak{p}, \mathfrak{a}) = (1), \quad (a, \ell) = 1 .$$

Then $\mathfrak{p} = \mathfrak{p}_1^{\ell}$ in $F(\sqrt[\ell]{\mu})$ where $\mathfrak{p}_1$ is a prime ideal and

$$(\sqrt[\ell]{\mu})^{\ell} = (\mathfrak{p}_1^a)^{\ell}\mathfrak{a} \quad \text{in } F(\sqrt[\ell]{\mu}) .$$

It follows that $\mathfrak{a} = \mathfrak{a}_1^{\ell}$ in $F(\sqrt[\ell]{\mu})$ and hence

$$(\sqrt[\ell]{\mu}) = \mathfrak{p}_1^{a}\mathfrak{a}_1 \quad \text{with} \quad (\mathfrak{p}_1, \mathfrak{a}_1) = (1) .$$

Therefore (by Theorem 2.1) $\mathfrak{p}_1$ becomes an ℓ^{th} power of a prime ideal in $F(\sqrt[\ell^2]{\mu})$, say $\mathfrak{p}_1 = \mathfrak{p}_2^{\ell}$. Hence $\mathfrak{p} = \mathfrak{p}_2^{\ell^2}$ in $F(\sqrt[\ell^2]{\mu})$. Applying the above argument and induction, it is clear that $\mathfrak{p} = \mathfrak{q}^{\ell^m}$ in $F(\sqrt[\ell^m]{\mu})$ and thus $\mathfrak{q}$ is of order ℓ^m over F.

Now, suppose $\mathfrak{q}$ is of order ℓ^m over F, that is, $\mathfrak{p} = \mathfrak{q}^{\ell^m}$, and let $\mathfrak{p}_1$ in $F(\sqrt[\ell]{\mu})$ correspond to $\mathfrak{q}$. Clearly $\mathfrak{p}_1$ is of order ℓ with respect to F, that is, $\mathfrak{p} = \mathfrak{p}_1^{\ell}$ in $F(\sqrt[\ell]{\mu})$. Hence $(\mu) = \mathfrak{p}^a\mathfrak{a}$ with $(\mathfrak{p}, \mathfrak{a}) = (1)$ and $(a, \ell) = 1$.

Therefore, in order that $\mathfrak{q}$ in $F(\sqrt[\ell^m]{\mu})$ be of order ℓ^m with respect to F it is necessary and sufficient that $(\mu) = \mathfrak{p}^a\mathfrak{a}$ with $(\mathfrak{p}, \mathfrak{a}) = (1)$, $(a, \ell) = 1$ in F where $\mathfrak{p}$ is the prime ideal in F corresponding to $\mathfrak{q}$. Combining this result with Theorem 2.5, we obtain the following theorem.

<u>Theorem</u> 4.3: Let μ_1, μ_2 be two integers of F, m a positive integer. Let $\mathfrak{q}$ be a prime ideal in $F(\sqrt[\ell^m]{\mu_i})$ for i = 1, 2 such that $(\mathfrak{q}, \ell) = (1)$, and let $\mathfrak{q}$ correspond to the prime ideal $\mathfrak{p}$ in F. Then $F(\sqrt[\ell^m]{\mu_1})$ and $F(\sqrt[\ell^m]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{q}$ if and only if $(\mu_i) = \mathfrak{p}^{a_i}\mathfrak{n}_i$ in F where $(a_i, \ell) = 1$ and $(\mathfrak{p}, \mathfrak{n}_i) = (1)$.

In case F contains the ℓ^m roots of unity, it follows from corollary 2.7.1 that $F(\sqrt[\ell^m]{\mu_1})$ and $F(\sqrt[\ell^m]{\mu_2})$ do not have corresponding residue systems mod. $\mathfrak{q}^2$ if $(\mathfrak{q}, \ell) = (1)$.

We now consider prime divisors of $\ell = (1 - \zeta)^{\ell - 1}$ in fields $F(\sqrt[\ell^m]{\mu})$. As before let $(1 - \zeta) = \mathfrak{L}^a\mathfrak{n}$ in F where $\mathfrak{L}$ is a prime ideal and $(\mathfrak{L}, \mathfrak{n}) = (1)$. We may assume that either $(\mu, \mathfrak{L}^2) = \mathfrak{L}$ or $(\mu, \mathfrak{L}) = (1)$.

<u>Theorem</u> 4.4: Let μ_1, μ_2 be integers of F each exactly divisible by $\mathfrak{L}$, and let m be a positive integer. Then $\mathfrak{L} = \mathfrak{l}^{\ell^m}$ ($\mathfrak{l}$ a prime ideal) in each of the fields $F(\sqrt[\ell^m]{\mu_1})$, $F(\sqrt[\ell^m]{\mu_2})$ and these two fields have corresponding residue systems mod. $\mathfrak{l}^{a\ell + 1 - a}$.

<u>Proof</u>: We prove the theorem by induction. If m = 1 the theorem is true by Theorems 3.2 and 3.3. Suppose the theorem true for m = k.

We have $\mathfrak{L} = \mathfrak{l}_1^{\ell^k}$ ($\mathfrak{l}_1$ a prime ideal) in each of the fields $F(\sqrt[\ell^k]{\mu_1})$, $F(\sqrt[\ell^k]{\mu_2})$. Since μ_i is exactly divisible by $\mathfrak{L}$ it follows that $\sqrt[\ell^k]{\mu_i}$ is exactly divisible by $\mathfrak{l}_1$ for i = 1, 2. Therefore by Theorem 1.16, $\mathfrak{l}_1 = \mathfrak{l}^{\ell}$ ($\mathfrak{l}$ a prime ideal) in the field $F(\sqrt[\ell^{k+1}]{\mu_i})$ for i = 1, 2. Thus $\mathfrak{L} = \mathfrak{l}^{\ell^{k+1}}$ in each of the fields $F(\sqrt[\ell^{k+1}]{\mu_1})$, $F(\sqrt[\ell^{k+1}]{\mu_2})$ and the first conclusion of the theorem follows by induction.

By the inductive hypothesis $F(\sqrt[\ell^k]{\mu_1})$ and $F(\sqrt[\ell^k]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}_1^{a\ell+1-a}$ where $\mathfrak{l}_1$ is a prime ideal in each of these fields and $\mathfrak{L} = \mathfrak{l}_1^{\ell^k}$. Furthermore we know that $\mathfrak{l}_1 = \mathfrak{l}^\ell$ ($\mathfrak{l}$ a prime ideal) in $F(\sqrt[\ell^{k+1}]{\mu_1})$ and $F(\sqrt[\ell^{k+1}]{\mu_2})$. It is clear that $\sqrt[\ell^{k+1}]{\mu_i}$ is exactly divisible by $\mathfrak{l}$ for i = 1, 2.

Let α be any integer of $F(\sqrt[\ell^{k+1}]{\mu_1})$ and let $n = a(\ell-1)\ell^k$. Then

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[\ell^{k+1}]{\mu_1} + \dots + \alpha_{n-1} \sqrt[\ell^{k+1}]{\mu_1}^{\,n-1} (\text{mod. } \mathfrak{l}^n)$$

where the α_i are residues mod. $\mathfrak{l}$ and may be chosen in F since $\mathfrak{l}$ is of order ℓ^{k+1} with respect to F. Hence

$$\alpha^\ell \equiv \alpha_0^\ell + \alpha_1^\ell \sqrt[\ell^k]{\mu_1} + \dots + \alpha_{n-1}^\ell \sqrt[\ell^k]{\mu_1}^{\,n-1} (\text{mod. } \mathfrak{l}^{\ell n} = \mathfrak{l}_1^n)$$

$$\alpha^\ell \equiv \tau \quad (\text{mod. } \mathfrak{l}_1^n)$$

where τ is an integer of $F(\sqrt[\ell^k]{\mu_1})$. If α and α' are two integers of $F(\sqrt[\ell^{k+1}]{\mu_1})$ such that $\alpha^\ell \equiv \alpha'^\ell \equiv \tau$ (mod. $\mathfrak{l}_1^n$) where τ is an integer of $F(\sqrt[\ell^k]{\mu_1})$, then $\alpha \equiv \alpha'$ (mod. $\mathfrak{l}^n$). If $\alpha^\ell \equiv \tau_1$ (mod. $\mathfrak{l}_1^n$) and $\alpha^\ell \equiv \tau_2$ (mod. $\mathfrak{l}_1^n$) where τ_1 and τ_2 are integers of $F(\sqrt[\ell^k]{\mu_1})$, then $\tau_1 \equiv \tau_2$ (mod. $\mathfrak{l}_1^n$). The number of residue classes mod. $\mathfrak{l}^n$ in $F(\sqrt[\ell^{k+1}]{\mu_1})$ is equal to the number of residue classes mod. $\mathfrak{l}_1^n$ in in $F(\sqrt[\ell^k]{\mu_1})$. Therefore if τ is any integer of $F(\sqrt[\ell^k]{\mu_1})$, there exists an integer α in $F(\sqrt[\ell^{k+1}]{\mu_1})$ such that $\alpha^\ell \equiv \tau$ (mod. $\mathfrak{l}_1^n$).

The statements in the above paragraph are valid if μ_1 is replaced by μ_2.

Let α be any integer of $F(\sqrt[\ell^{k+1}]{\mu_1})$. There exists an integer τ of $F(\sqrt[\ell^k]{\mu_1})$ such that

$$\alpha^\ell \equiv \tau \quad (\text{mod. } \mathfrak{l}_1^n).$$

Since $F(\sqrt[\ell^k]{\mu_1})$ and $F(\sqrt[\ell^k]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}_1^{a\ell+1-a}$, there exists an integer σ of $F(\sqrt[\ell^k]{\mu_2})$ such that

$$\tau \equiv \sigma \pmod{\mathfrak{l}_1^{a\ell+1-a}} .$$

There exists an integer β in $F(\sqrt[\ell^{k+1}]{\mu_2})$ such that

$$\beta^\ell \equiv \sigma \pmod{\mathfrak{l}_1^n} .$$

Since $n = a(\ell - 1)\ell^k$, and $k \geq 1$, it follows that

$$\alpha^\ell \equiv \beta^\ell \pmod{\mathfrak{l}_1^{a\ell+1-a}} .$$

Therefore

$$\alpha \equiv \beta \pmod{\mathfrak{l}^{a\ell+1-a}}$$

and $F(\sqrt[\ell^{k+1}]{\mu_1})$, $F(\sqrt[\ell^{k+1}]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1-a}$. The theorem follows by induction.

We consider next the case in which μ_1, μ_2 are two integers of F each prime to λ.

<u>Theorem</u> 4.5: Let μ_1, μ_2 be integers of F each prime to λ, and let k_i be the largest positive integer such that the congruence $\mu_i \equiv \alpha_i^\ell \pmod{\lambda^{k_i}}$ is solvable for α_i in $F (i = 1, 2)$. If $k_1 \leq k_2 < a\ell$ and $a\ell + 1 - k_2 \geq 2a$, then $\lambda = \mathfrak{l}^{\ell^m}$ ($\mathfrak{l}$ a prime ideal) in each of the fields $F(\sqrt[\ell^m]{\mu_1})$, $F(\sqrt[\ell^m]{\mu_2})$ where m is a positive integer and these two fields have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1-k_2-a}$.

We first prove the following lemma.

<u>Lemma</u>: Let μ be an integer of F prime to λ, m a positive integer, and let k be the largest positive integer such that the congruence $\mu \equiv \alpha^\ell \pmod{\lambda^k}$ is solvable for α in F. If $k < a\ell$ and

and $a\ell + 1 - k \geq 2a$, then $\mathfrak{L} = \mathfrak{l}^{\ell^m}$ ($\mathfrak{l}$ a prime ideal) in $F(\sqrt[\ell^m]{\mu})$ and k is the largest positive integer such that the congruence $\sqrt[\ell^m]{\mu} \equiv \beta^{\ell}$ (mod. $\mathfrak{l}^k$) is solvable for β in $F(\sqrt[\ell^m]{\mu})$.

<u>Proof</u>: We prove the lemma by induction. Suppose $m = 1$. Since k is the largest integer such that $\mu \equiv \alpha^{\ell}$ (mod. $\mathfrak{L}^k$) is solvable for α in F, it follows by Theorem 1.17 that $\mathfrak{L} = \mathfrak{l}_1^{\ell}$ in $F(\sqrt[\ell]{\mu})$ where $\mathfrak{l}_1$ is a prime ideal. Suppose

$$\sqrt[\ell]{\mu} \equiv \beta_1^{\ell} \pmod{\mathfrak{l}_1^{k+1}}$$

where β_1 is in $F(\sqrt[\ell]{\mu})$. By the method used in the proof of Theorem 3.6 there exists an integer γ_1 in F such that

$$\beta_1^{\ell} \equiv \gamma_1 \pmod{\mathfrak{L}^{v-a}} \quad , \quad v = a\ell + 1 - k \ .$$

Since $k < a\ell$ and $a\ell + 1 - k \geq 2a$ by hypothesis, it follows that $\sqrt[\ell]{\mu} \equiv \gamma_1$ (mod. $\mathfrak{l}_1^{k+1}$) and therefore $\mu \equiv \gamma_1^{\ell}$ mod. $\mathfrak{L}^{k+1}$) contrary to assumption. Thus the congruence

$$\sqrt[\ell]{\mu} \equiv \xi^{\ell} \pmod{\mathfrak{l}_1^{k+1}}$$

is not solvable for ξ in $F(\sqrt[\ell]{\mu})$.

Since $\mu \equiv \alpha^{\ell}$ (mod. $\mathfrak{L}^k$) where α is an integer of F, it follows that $\sqrt[\ell]{\mu} \equiv \alpha$ (mod. $\mathfrak{l}_1^k$). By the method in the proof of Theorem 3.6 there exists an integer δ_1 in $F(\sqrt[\ell]{\mu})$ such that

$$\delta_1^{\ell} \equiv \alpha \pmod{\mathfrak{L}^{v-a}} \quad , v = a\ell + 1 - k \ .$$

Hence

$$\sqrt[\ell]{\mu} \equiv \delta_1^{\ell} \pmod{\mathfrak{l}_1^{k}}$$

and the congruence $\sqrt[\ell]{\mu} \equiv \xi^{\ell}$ (mod. $\mathfrak{l}_1^k$) is solvable for ξ in $F(\sqrt[\ell]{\mu})$. This establishes the lemma for the case $m = 1$.

Suppose the lemma is true for $m = n$. We have $\mathfrak{L} = \mathfrak{l}_n^{\ell^n}$ ($\mathfrak{l}_n$ a prime ideal) in $F(\sqrt[\ell^n]{\mu})$ and k is the largest integer such that $\sqrt[\ell^n]{\mu} \equiv \beta_n^{\ell} \pmod{\mathfrak{l}_n^k}$ is solvable for β_n in $F(\sqrt[\ell^n]{\mu})$. It follows from Theorem 1.17 that $\mathfrak{l}_n = \mathfrak{l}_{n+1}^{\ell}$ ($\mathfrak{l}_{n+1}$ a prime ideal) in $F(\sqrt[\ell^{n+1}]{\mu})$. Suppose

$$\sqrt[\ell^{n+1}]{\mu} \equiv \beta_{n+1}^{\ell} \pmod{\mathfrak{l}_{n+1}^{k+1}}$$

where β_{n+1} is an integer of $F(\sqrt[\ell^{n+1}]{\mu})$. There exists an integer γ_n in $F(\sqrt[\ell^n]{\mu})$ such that

$$\beta_{n+1}^{\ell} \equiv \gamma_n \pmod{\mathfrak{l}_n^{v_n - a\ell^{n-1}}}, \quad v_n = a\ell^n + 1 - k.$$

(This follows by taking $F(\sqrt[\ell^n]{\mu})$ to be the ground field in Theorem 3.6 and applying the method used in the proof there.) Since $k < a\ell$ and $a\ell + 1 - k \geq 2a$, it follows that

$$\sqrt[\ell^{n+1}]{\mu} \equiv \gamma_n \pmod{\mathfrak{l}_{n+1}^{k+1}}$$

and therefore

$$\sqrt[\ell^n]{\mu} \equiv \gamma_n^{\ell} \pmod{\mathfrak{l}_n^{k+1}}$$

contrary to assumption. Hence the congruence $\sqrt[\ell^{n+1}]{\mu} \equiv \xi^{\ell} \pmod{\mathfrak{l}_{n+1}^{k+1}}$ is not solvable for ξ in $F(\sqrt[\ell^{n+1}]{\mu})$. However the congruence $\sqrt[\ell^{n+1}]{\mu} \equiv \xi^{\ell} \pmod{\mathfrak{l}_{n+1}^{k}}$ is solvable for ξ in $F(\sqrt[\ell^{n+1}]{\mu})$ by the method used in the case $m = 1$. Thus the lemma is true for $m = n + 1$.

Proof of Theorem 4.5: By the lemma we have $\mathfrak{L} = \mathfrak{l}^{\ell^m}$ in $F(\sqrt[\ell^m]{\mu_1})$ and in $F(\sqrt[\ell^m]{\mu_2})$ where $\mathfrak{l}$ is a prime ideal. We use induction to prove that $F(\sqrt[\ell^m]{\mu_1})$ and $F(\sqrt[\ell^m]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}^{a\ell+1-k-a}$. If $m = 1$ this follows from Theorem 3.6.

Suppose $F(\sqrt[\ell^n]{\mu_1})$ and $F(\sqrt[\ell^n]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}_n^{a\ell+1-k-a}$ where $\mathfrak{l}_n$ is a prime ideal in $F(\sqrt[\ell^n]{\mu_1})$, $F(\sqrt[\ell^n]{\mu_2})$ and $\mathfrak{L} = \mathfrak{l}_n^{\ell^n}$. By the lemma k is the largest integer such that the congruence

$$\sqrt[\ell^n]{\mu_i} \equiv \xi_i^{\ell} \pmod{\mathfrak{l}_n^k}$$

is solvable for ξ_i in $F(\sqrt[\ell^n]{\mu_i})$ $(i = 1, 2)$. Furthermore $\mathfrak{l}_n = \mathfrak{l}_{n+1}^{\ell}$ where $\mathfrak{l}_{n+1}$ is a prime ideal in $F(\sqrt[\ell^{n+1}]{\mu_i})$ for i = 1, 2. Thus $\sqrt[\ell^{n+1}]{\mu_i} - \xi_i$ is exactly divisible by $\mathfrak{l}_{n+1}^k$ for i = 1, 2. It follows by the method used in the proof of Theorem 3.6 that if ν_i is any integer of $F(\sqrt[\ell^{n+1}]{\mu_i})$, there exists an integer τ_i in $F(\sqrt[\ell^n]{\mu_i})$ such that

$$\nu_i^{\ell} \equiv \tau_i \pmod{\mathfrak{l}_n^{v_n - a\ell^{n-1}}}, \quad v_n = a\ell^n + 1 - k$$

for i = 1, 2. Furthermore if τ_i is any integer of $F(\sqrt[\ell^n]{\mu_i})$ there exists an integer ν_i in $F(\sqrt[\ell^{n+1}]{\mu_i})$ such that the above congruence is valid $(i = 1, 2)$.

Let ν_1 be any integer of $F(\sqrt[\ell^{n+1}]{\mu_1})$. There exists an integer τ_1 of $F(\sqrt[\ell^n]{\mu_1})$ such that

$$\nu_1^{\ell} \equiv \tau_1 \pmod{\mathfrak{l}_n^{v_n - a\ell^{n-1}}}, \quad v_n = a\ell^n + 1 - k.$$

Since $F(\sqrt[\ell^n]{\mu_1})$ and $F(\sqrt[\ell^n]{\mu_2})$ have corresponding residue systems mod. $\mathfrak{l}_n^{a\ell+1-k-a}$, there exists an integer τ_2 of $F(\sqrt[\ell^n]{\mu_2})$ such that

$$\tau_1 \equiv \tau_2 \pmod{\mathfrak{l}_n^{a\ell+1-k-a}}.$$

Therefore

$$\nu_1^{\ell} \equiv \tau_2 \pmod{\mathfrak{l}_n^{a\ell+1-k-a}}.$$

There exists an integer ν_2 in $F(\sqrt[\ell^{n+1}]{\mu_2})$ such that $\nu_2^{\ell} \equiv \tau_2 \pmod{\mathfrak{l}_n^{v_n - a\ell^{n-1}}}$

$$\nu_1^{\ell} \equiv \nu_2^{\ell} \pmod{\lambda_n^{a\ell+1-k-a}}$$

and therefore

$$\nu_1 \equiv \nu_2 \pmod{\lambda_{n+1}^{a\ell+1-k-a}}.$$

The theorem follows by induction.

It is clear that if μ_1 is exactly divisible by $\mathfrak{L}$ and μ_2 is prime to $\mathfrak{L}$, a result similar to theorems 4.4 and 4.5 can be obtained. This result together with Theorems 4.4 and 4.5 yields the following theorem.

Theorem 4.6: Let μ_1, μ_2 be two integers of F such that $\mathfrak{L} = \lambda^{\ell}$ in $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$, and let m be a positive integer. If the orders of ramification of λ in $F(\sqrt[\ell]{\mu_1})$ and $F(\sqrt[\ell]{\mu_2})$ are $\geq v \geq 2a$, then $\mathfrak{L} = \lambda_m^{\ell^m}$ in $F(\sqrt[\ell^m]{\mu_1})$ and $F(\sqrt[\ell^m]{\mu_2})$ and these two fields have corresponding residue systems mod. λ_m^{v-a}.

AUTOBIOGRAPHY

I, Hubert Spence Butts, Jr., was born in Burkburnett, Texas, November 7, 1923. I received my secondary school education in the public schools of the city of Burkburnett, Texas. My undergraduate training was received at the North Texas State College from which I received the degree Bachelor of Science in 1947 and Master of Science in 1948. While at North Texas State College, I taught in the Department of Mathematics as an assistant and also as a full-time instructor. In 1948 I received an appointment as assistant in the Department of Mathematics of The Ohio State University. I held this position for four years while completing the requirements for the degree Doctor of Philosophy.