# CORRESPONDING RESIDUE SYSTEMS IN ALGEBRAIC NUMBER FIELDS

H. S. BUTTS AND H. B. MANN

In this paper we shall consider integral ideals in finite algebraic extensions of the field $R$ of rational numbers. Algebraic number fields will be denoted by $\mathfrak{F}$ with subscripts or superscripts, ideals by German letters, algebraic numbers by lower case Greek letters, and numbers of the rational field $R$ by lower case Latin letters.

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

If $\mathfrak{a}_1$ is an ideal in a field $\mathfrak{F}_1$ and $\mathfrak{a}_2$ is an ideal in a field $\mathfrak{F}_2$, then we shall write $\mathfrak{a}_1=\mathfrak{a}_2$ provided $\mathfrak{a}_1$ and $\mathfrak{a}_2$ generate the same ideal in some field containing all the numbers of $\mathfrak{F}_1$ and of $\mathfrak{F}_2$ (see [1, § 37]). 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 $\mathfrak{F}$ if it may be generated by numbers in $\mathfrak{F}$, that is to say, if it has a basis in $\mathfrak{F}$.

Let $\mathfrak{a}$ be an ideal contained in the fields $\mathfrak{F}_1$ and $\mathfrak{F}_2$. We say that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have *corresponding residue systems modulo* $\mathfrak{a}$ if for every integer $\alpha_1$ of $\mathfrak{F}_1$ there exists an integer $\alpha_2$ of $\mathfrak{F}_2$ such that $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{a}}$, and for every integer $\alpha_2$ of $\mathfrak{F}_2$ there exists an integer $\alpha_1$ of $\mathfrak{F}_1$ such that $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{a}}$.

The problem considered in this paper is the following one: if $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are two fields containing an ideal $\mathfrak{a}$, under what conditions will $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{a}$. We shall 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 $\mathfrak{F}_1$ and $\mathfrak{F}_2$ to have corresponding residue systems mod $\mathfrak{a}$ is derived in case that $\mathfrak{a}$ is a prime ideal. A necessary (but not sufficient) condition is derived in case $\mathfrak{a}$ is a power of a prime ideal and $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are normal over $\mathfrak{F}_1 \cap \mathfrak{F}_2$. A special case in which the fields are of the type $\mathfrak{F}(\sqrt[q]{\mu})$ is considered. These fields are of interest in themselves and in view of Corollary 7.1 seem to have a direct connection with the general problem.

THEOREM 1. *Let $\mathfrak{a}$ be an ideal in the number fields $\mathfrak{F}_1$ and $\mathfrak{F}_2$ and suppose $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{a}$. Then $\mathfrak{a}$ has the same prime ideal decomposition in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$.*

Received May 28, 1954.

*Proof.* Let

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

$$\mathfrak{a}=\mathfrak{q}_1^{f_1}\cdot\ldots\cdot\mathfrak{q}_s^{f_s} \text{ in } \mathfrak{F}_2$$

where the $\mathfrak{p}_i$ are prime ideals in $\mathfrak{F}_1$ and the $\mathfrak{q}_i$ are prime ideals in $\mathfrak{F}_2$. Let $\alpha$ be an integer in $\mathfrak{F}_1$ such that $\alpha$ is exactly divisible by $\mathfrak{p}_1$ and $(\alpha, \mathfrak{p}_i)=(1)$ for i=2, $\cdots$, $r$. There exists an integer $\beta$ in $\mathfrak{F}_2$ such that $\alpha\equiv\beta$ (mod $\mathfrak{a}$) and thus in $\mathfrak{F}_1\cup\mathfrak{F}_2$ we have $(\beta, \mathfrak{a})=\mathfrak{p}_1$. Since $\beta$ is in $\mathfrak{F}_2$ and $\mathfrak{a}\subset\mathfrak{F}_2$, it follows that $\mathfrak{p}_1\subset\mathfrak{F}_2$. In the same manner it follows that $\mathfrak{p}_i\subset\mathfrak{F}_2$ for $i=1, \cdots, r$ and $\mathfrak{q}_i\subset\mathfrak{F}_1$ for $i=1, \cdots, s$. Therefore in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$ 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 $\mathfrak{F}_2$ the $\mathfrak{q}_i$ are prime ideals and hence $\mathfrak{q}_1|\mathfrak{p}_j$ in $\mathfrak{F}_2$ for some $j$. In $\mathfrak{F}_1$ the $\mathfrak{p}_i$ are prime ideals and therefore $\mathfrak{p}_k|\mathfrak{q}_1$ in $\mathfrak{F}_1$ for some $k$. Thus in $\mathfrak{F}_1\cup\mathfrak{F}_2$ we have $\mathfrak{p}_k|\mathfrak{p}_j$ which implies that $\mathfrak{p}_k=\mathfrak{p}_j=\mathfrak{q}_1$ in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$. By renumbering and repeated application of the above argument we obtain $r=s$ and $\mathfrak{p}_i=\mathfrak{q}_i$ for $i=1, \cdots, r=s$ in $\mathfrak{F}_1$ and $\mathfrak{F}_2$.

THEOREM 2. *Let $\mathfrak{a}$ be an ideal in the number fields $\mathfrak{F}_1$ and $\mathfrak{F}_2$. In order that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{a}$ it is necessary and sufficient that $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdot\ldots\cdot\mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i$ is a prime ideal in $\mathfrak{F}_1$ and $\mathfrak{F}_2$, and $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}_i^{e_i}$ for $i=1, \cdots, r$.*

*Proof.* The necessity follows from Theorem 1. Suppose $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdot\ldots\cdot\mathfrak{p}_r^{e_r}$ in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$, where $\mathfrak{p}_i$ is a prime ideal in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$, and that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}_i^{e_i}$ for $i=1, \cdots, r$. Let $\alpha$ be any integer of $\mathfrak{F}_1$. There exist integers $\beta_i$ in $\mathfrak{F}_2$ such that $\alpha\equiv\beta_i$ (mod $\mathfrak{p}_i^{e_i}$) for $i=1, \cdots, r$. By the Chinese remainder theorem there exists an integer $\beta$ in $\mathfrak{F}_2$ such that $\beta\equiv\beta_i$ (mod $\mathfrak{p}_i^{e_i}$) for $i=1, \cdots, r$ and hence $\alpha\equiv\beta$ (mod $\mathfrak{a}$). It follows that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{a}$.

THEOREM 3. *Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be two number fields, $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$, and let $\mathfrak{p}$ be a prime ideal in both $\mathfrak{F}_1$ and $\mathfrak{F}_2$. Suppose $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}^j$ and let $\mathfrak{F}_n$ be the smallest normal extension over $\mathfrak{F}$ containing $\mathfrak{F}_1$ and $\mathfrak{F}_2$. Then for every automorphism $A$ in the Galois group $\mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$ of $\mathfrak{F}_n$ over $\mathfrak{F}$ we have $\alpha_1^A\equiv\alpha_1$ (mod $\mathfrak{p}^j$) and $\alpha_2^A\equiv\alpha_2$ (mod $\mathfrak{p}^j$) for every integer $\alpha_1$ in $\mathfrak{F}_1$ and $\alpha_2$ in $\mathfrak{F}_2$.*

*Proof.* Let $\mathfrak{G}_1$ and $\mathfrak{G}_2$ be the subgroups of $\mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$ which leave $\mathfrak{F}_1$ and $\mathfrak{F}_2$ fixed respectively. Since $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$ we have by Galois theory that $\mathfrak{G}_1\cup\mathfrak{G}_2$ corresponds to $\mathfrak{F}$ under the Galois correspondence between subgroups and subfields. Hence $\mathfrak{G}_1\cup\mathfrak{G}_2=\mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$.

Denote by $\mathfrak{S}_i$ $(i=1, 2)$ the set of automorphisms $A$ in $\mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$ such that $\alpha_i^A \equiv \alpha_i \pmod{\mathfrak{p}^j}$ for all integers $\alpha_i$ in $\mathfrak{F}_i$ for $i=1, 2$. The sets $\mathfrak{S}_i$ are subgroups of $\mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$. Furthermore the sets $\mathfrak{S}_i$ contain $\mathfrak{G}_i$ for $i=1, 2$.

Let $A$ be an automorphism of $\mathfrak{S}_2$. For every integer $\alpha_1$ in $\mathfrak{F}_1$ there exists an integer $\alpha_2$ in $\mathfrak{F}_2$ such that $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{p}^j}$. Therefore $(\alpha_1 - \alpha_2)^A \equiv 0 \pmod{\mathfrak{p}^j}$, $\alpha_1^A \equiv \alpha_2^A \pmod{\mathfrak{p}^j}$, $\alpha_1^A \equiv \alpha_2 \pmod{\mathfrak{p}^j}$, and thus $\alpha_1^A \equiv \alpha_1 \pmod{\mathfrak{p}^j}$. Hence the automorphism $A$ is also in $\mathfrak{S}_1$ and it follows that $\mathfrak{S}_2 \subset \mathfrak{S}_1$. Similarly $\mathfrak{S}_1 \subset \mathfrak{S}_2$ and therefore $\mathfrak{S}_1 = \mathfrak{S}_2$. Hence $\mathfrak{S}_1 = \mathfrak{S}_2 = \mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$ since $\mathfrak{S}_i \supset \mathfrak{G}_i$ for $i=1, 2$ and $\mathfrak{G}_1 \cup \mathfrak{G}_2 = \mathfrak{G}(\mathfrak{F}_n|\mathfrak{F})$.

COROLLARY 3.1. *Under the conditions of Theorem 3 it follows that* $\mathfrak{d}_1 \equiv 0 \pmod{\mathfrak{p}^{n_1 j}}$ *and* $\mathfrak{d}_2 \equiv 0 \pmod{\mathfrak{p}^{n_2 j}}$, *where* $n_1 + 1 = (\mathfrak{F}_1|\mathfrak{F})$, $n_2 + 1 = (\mathfrak{F}_2|\mathfrak{F})$, *and* $\mathfrak{d}_i$ *denotes the relative differente of* $\mathfrak{F}_i$ *over* $\mathfrak{F}$ *for* $i=1, 2$.

THEOREM 4. *Let* $\mathfrak{F}_1 \supset \mathfrak{F}$ *be two number fields and let* $\mathfrak{P}$ *be a prime ideal in* $\mathfrak{F}_1$. *Suppose that for every integer* $\alpha$ *in* $\mathfrak{F}_1$ *we have* $\alpha \equiv \alpha^{(i)}$ $\pmod{\mathfrak{P}}$ *for* $i=1, \cdots, k=(\mathfrak{F}_1|\mathfrak{F})$, *where* $\alpha^{(i)}$ *is the* $i^{th}$ *conjugate of* $\alpha$ *in* $\mathfrak{F}_1$ *over* $\mathfrak{F}$. *Then* $\mathfrak{P}$ *is of order* $k=(\mathfrak{F}_1|\mathfrak{F})$ *with respect to* $\mathfrak{F}$.

*Proof*. It is clear that $\mathfrak{P}$ coincides with its conjugates. Moreover if $\alpha$ is any integer in $\mathfrak{F}_1$ and $\alpha_2, \cdots, \alpha_k$ its conjugates over $\mathfrak{F}$ then

$$f(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_k) \equiv (x-\alpha)^k \pmod{\mathfrak{P}}.$$

The polynomial $f(x)$ has its coefficients in $\mathfrak{F}$ and since the field of residue classes mod $\mathfrak{P}$ is separable over the field or residue classes mod $\mathfrak{p}$, it must be of degree one.

THEOREM 5. *Let* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *be two number fields and* $\mathfrak{p}$ *a prime ideal in both fields. Then* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *have corresponding residue systems mod* $\mathfrak{p}$ *if and only if* $\mathfrak{p}$ *is of order* $(\mathfrak{F}_1|\mathfrak{F}_1 \cap \mathfrak{F}_2)$ *in* $\mathfrak{F}_1$ *over* $\mathfrak{F}_1 \cap \mathfrak{F}_2$ *and of order* $(\mathfrak{F}_2|\mathfrak{F}_1 \cap \mathfrak{F}_2)$ *in* $\mathfrak{F}_2$ *over* $\mathfrak{F}_1 \cap \mathfrak{F}_2$.

*Proof*. If $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}$, it follows immediately from Theorems 3 and 4 that the order of $\mathfrak{p}$ satisfies the conditions of the theorem.

The converse is clear since $\mathfrak{p}$ is of degree one over $\mathfrak{F}_1 \cap \mathfrak{F}_2$ and therefore every residue class mod $\mathfrak{p}$ contains an integer of $\mathfrak{F}_1 \cap \mathfrak{F}_2$.

COROLLARY 5.1. *Let* $\mathfrak{a}$ *be an ideal in the number fields* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$. *If* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *have corresponding residue systems mod* $\mathfrak{a}$, *then* $(\mathfrak{F}_1|\mathfrak{F}_1 \cap \mathfrak{F}_2) = (\mathfrak{F}_2|\mathfrak{F}_1 \cap \mathfrak{F}_2)$.

THEOREM 6. *Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be two number fields each normal over $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$ and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$. In order that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}$ it is necessary and sufficient that the inertial group of $\mathfrak{p}$ in $\mathfrak{F}_j$ over $\mathfrak{F}$ be equal to the Galois group of $\mathfrak{F}_j$ over $\mathfrak{F}$ for $j=1, 2$.*

*Proof.* The condition is sufficient since $\mathfrak{p}$ is of degree one in $\mathfrak{F}_j$ over $\mathfrak{F}$ if the inertial group of $\mathfrak{p}$ in $\mathfrak{F}_j$ over $\mathfrak{F}$ is equal to the Galois group of $\mathfrak{F}_j$ over $\mathfrak{F}$ for $j=1, 2$.

Suppose $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}$ and let $\mathfrak{F}_i$ denote the inertial field of $\mathfrak{p}$ in $\mathfrak{F}_1$ over $\mathfrak{F}$. The order of $\mathfrak{p}$ in $\mathfrak{F}_1$ over $\mathfrak{F}$ is equal to $(\mathfrak{F}_1|\mathfrak{F}_i)$ and hence by Theorem 5 we have $(\mathfrak{F}_1|\mathfrak{F}_i)=(\mathfrak{F}_1|\mathfrak{F})$. It follows that $\mathfrak{F}_i=\mathfrak{F}$ and hence the Galois group of $\mathfrak{F}_1$ over $\mathfrak{F}$ is equal to the inertial group of $\mathfrak{p}$ in $\mathfrak{F}_1$ over $\mathfrak{F}$.

THEOREM 7. *Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be two number fields each normal over $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$. If $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}^j$, then the $j^{th}$ ramification group of $\mathfrak{p}$ in $\mathfrak{F}_k$ over $\mathfrak{F}$ is equal to the Galois group of $\mathfrak{F}_k$ over $\mathfrak{F}$ for $k=1, 2$.*

*Proof.* Let $A$ be any automorphism of $\mathfrak{G}(\mathfrak{F}_1\cup\mathfrak{F}_2|\mathfrak{F})$. It follows from Theorem 3 that $\alpha_i^A\equiv\alpha_i \pmod{\mathfrak{p}^j}$ for every integer $\alpha_i$ in $\mathfrak{F}_i$ for $i=1, 2$. Hence if $A_i$ is an automorphism of $\mathfrak{G}(\mathfrak{F}_i|\mathfrak{F})$, $(i=1, 2)$, it follows that $\alpha_i^{A_i}\equiv\alpha_i \pmod{\mathfrak{p}^j}$ since every automorphism $A_i$ of $\mathfrak{G}(\mathfrak{F}_i|\mathfrak{F})$ can be continued to an automorphism of $\mathfrak{G}(\mathfrak{F}_1\cup\mathfrak{F}_2|\mathfrak{F})$. Thus the $j^{th}$ ramification group of $\mathfrak{p}$ in $\mathfrak{F}_i$ over $\mathfrak{F}$ is equal to the Galois group of $\mathfrak{F}_i$ over $\mathfrak{F}$ for $i=1, 2$.

COROLLARY 7.1. *Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be two number fields normal over $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$ and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$. If $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}^j$ for $j>1$, then $(\mathfrak{F}_1|\mathfrak{F})=(\mathfrak{F}_2|\mathfrak{F})=p^r$ where $p$ is the rational prime belonging to $p$.*

*Proof.* By Theorem 7 we have $\mathfrak{G}(\mathfrak{F}_1|\mathfrak{F})=\mathfrak{G}_1=\cdots=\mathfrak{G}_j$ where $\mathfrak{G}_j$ is the $j^{th}$ ramification group of $\mathfrak{p}$ in $\mathfrak{F}_1$ over $\mathfrak{F}$. By Theorem 5 the order $e$ of $\mathfrak{p}$ in $\mathfrak{F}_1$ over $\mathfrak{F}$ is equal to $(\mathfrak{F}_1|\mathfrak{F})$. But $\mathfrak{G}_1/\mathfrak{G}_2$ is cyclic of order $e_0$ where $e=p^re_0$, $(e_0, p)=1$, $p$ the rational prime belonging to the ideal $\mathfrak{p}$. Therefore $(\mathfrak{F}_1|\mathfrak{F})=e_0p^r$. Since $\mathfrak{G}_1=\mathfrak{G}_2$ we have $e_0=1$ and $(\mathfrak{F}_1|\mathfrak{F})=p^r$. Therefore $(\mathfrak{F}_1|\mathfrak{F})=(\mathfrak{F}_2|\mathfrak{F})=p^r$.

COROLLARY 7.2. *Let $\mathfrak{F}_1$ and $\mathfrak{F}_2$ be two number fields normal over $\mathfrak{F}=\mathfrak{F}_1\cap\mathfrak{F}_2$ and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{F}_1$ and in $\mathfrak{F}_2$. Let $v_i$ denote* *the order of ramification of* $\mathfrak{p}$ *in* $\mathfrak{F}_i$ *over* $\mathfrak{F}$ *for* $i=1, 2$ *and suppose* $v_1 \geqq v_2 \geqq 2$. *If* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *have corresponding residue systems mod* $p^{v_2}$, *then* $\mathfrak{G}(\mathfrak{F}_2|\mathfrak{F})$ *is Abelian of type* $(p, \cdots, p)$ *where* $p$ *is the rational prime belonging to* $\mathfrak{p}$.

*Proof.* If $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have corresponding residue systems mod $\mathfrak{p}^{v_2}$, it follows from Theorem 7 that $\mathfrak{G}(\mathfrak{F}_2/\mathfrak{F})=\mathfrak{G}_1=\cdots=\mathfrak{G}_{v_2}$ where $\mathfrak{G}_j$ is the $j^{th}$ ramification group of $\mathfrak{p}$ in $\mathfrak{F}_2$ over $\mathfrak{F}$. By the definition of $v_2$, $\mathfrak{G}_{v_2+1}$ is the group identity. But $\mathfrak{G}_{v_2}/\mathfrak{G}_{v_2+1}$ is Abelian of type $(p, \cdots, p)$ where $p$ is the rational prime belonging to $\mathfrak{p}$. It follows that $\mathfrak{G}(\mathfrak{F}_2|\mathfrak{F})$ is Abelian of type $(p, \cdots, p)$.

The condition of Theorem 7 is not sufficient as the following example shows. Denote by $R$ the field of rational numbers and let $\mathfrak{F}_1=R(\sqrt{2})$, $\mathfrak{F}_2=R(\sqrt{3})$, $\mathfrak{p}=(\sqrt{2})$. It is clear that the second ramification group of the ideal $(\sqrt{2})$ in $\mathfrak{F}_1$ over $R$ is equal to the Galois group of $\mathfrak{F}_1$ over $R$, and likewise for $\mathfrak{F}_2$. However $\mathfrak{F}_1$ and $\mathfrak{F}_2$ do not have corresponding residue systems mod $(\sqrt{2})^2$.

In the remainder of this paper we consider fields of the type $\mathfrak{F}(\sqrt[q]{\mu})$ where $\mathfrak{F}$ is a number field containing a $q^{th}$ root of unity $\zeta \neq 1$, $q$ is a rational prime, and $\mu$ is an integer of $\mathfrak{F}$ and not the $q^{th}$ power of an integer in $\mathfrak{F}$.

Let $\mathfrak{P}$ be a prime ideal in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$. We may suppose that $\mathfrak{F}(\sqrt[q]{\mu_1}) \neq \mathfrak{F}(\sqrt[q]{\mu_2})$ since the problem of corresponding residue systems is trivial in case equality holds. By Theorem 5, in order that $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{P}$ it is necessary and sufficient that $\mathfrak{P}$ be of order $q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ over $\mathfrak{F}$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$. Therefore it is necessary and sufficient that $\mathfrak{P}$ divide the relative differente $\mathfrak{d}_i$ of $\mathfrak{F}(\sqrt[q]{\mu_i})$ over $\mathfrak{F}$ for $i=1, 2$. If $\mathfrak{c}_i$ denotes the relative conductor of $\sqrt[q]{\mu_i}$ for $i=1, 2$ then

$$(\sqrt[q]{\mu_i})^{q-1}q=\mathfrak{c}_i\mathfrak{d}_i$$

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

Denote by $\mathfrak{p}$ the prime ideal corresponding to $\mathfrak{P}$ in $\mathfrak{F}$. If $\mathfrak{p}$ divides $\mu_i$ but not $q$ then $\mathfrak{p}=\mathfrak{P}^q$ in $F(\sqrt[q]{\mu_i})$ if and only if $(\mu_i)=\mathfrak{p}^{a_i}\mathfrak{a}_i$ for $i=1, 2$ where $(a_i, q)=1$ and $(\mathfrak{a}_i, \mathfrak{p})=(1)$. (See [1, p. 150]). Thus we have the following theorem.

THEOREM 8. *If* $(\mathfrak{P}, q)=(1)$, *then* $\mathfrak{F}(\sqrt[q]{\mu_1})$ *and* $\mathfrak{F}(\sqrt[q]{\mu_2})$ *have corresponding residue systems mod* $\mathfrak{P}$ *if and only if* $(\mu_i)=\mathfrak{p}^{a_i}\mathfrak{a}_i$ *with* $(a_i, q)=1$ *and* $(\mathfrak{a}_i, \mathfrak{p})=(1)$ *for* $i=1, 2$.

From Corollary 7.1 it follows that $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ do not have corresponding residue systems mod $\mathfrak{P}^j$ for $j>1$ in case $(\mathfrak{P}, q)=(1)$.

We now consider prime ideals in fields $\mathfrak{F}(\sqrt[q]{\mu})$ which divide $q$, that is, prime ideals which divide the ideal $(1-\zeta)$ where $\zeta\neq 1$ is a $q^{th}$ root of unity. Let $(1-\zeta)=\mathfrak{Q}^a\mathfrak{a}$ in $\mathfrak{F}$ where $(\mathfrak{Q}, \mathfrak{a})=(1)$ and $\mathfrak{Q}$ is a prime ideal in $\mathfrak{F}$, and let $\mathfrak{q}$ be a prime ideal of $F(\sqrt[q]{\mu})$ which divides $\mathfrak{Q}$. By Theorem 5 we are concerned only with the case in which $\mathfrak{q}$ is of order $q$ in $\mathfrak{F}(\sqrt[q]{\mu})$ over $\mathfrak{F}$, that is $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu})$. We may suppose without loss of generality that either $(\mu, \mathfrak{Q})=(1)$ or $(\mu, \mathfrak{Q}^2)=\mathfrak{Q}$. The ideal $\mathfrak{Q}$ becomes the $q^{th}$ power of a prime ideal in $\mathfrak{F}(\sqrt[q]{\mu})$ in case $(\mu, \mathfrak{Q}^2)=\mathfrak{Q}$. In case $(\mu, \mathfrak{Q})=(1)$, $\mathfrak{Q}$ becomes a $q^{th}$ power of a prime ideal in $\mathfrak{F}(\sqrt[q]{\mu})$ if the congruence $\mu\equiv\xi^q \pmod{\mathfrak{Q}^{aq}}$ is not solvable for $\xi$ in $\mathfrak{F}$.

The main result of this paper for fields of the type $\mathfrak{F}(\sqrt[q]{\mu})$ is the following one: if $\mu_1, \mu_2$ are two integers of $\mathfrak{F}$ such that $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$, and $\mathfrak{q}$ has ramification orders $\geq v>a$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$ then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{v-a}$.

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

THEOREM 9. *If* $(\mu, \mathfrak{Q}^2)=\mathfrak{Q}$ *and* $n$ *is a positive integer, then* $\mathfrak{Q}=\mathfrak{q}^q$ *in* $\mathfrak{F}(\sqrt[q]{\mu})$ *and every integer* $\alpha$ *in* $\mathfrak{F}(\sqrt[q]{\mu})$ *satisfies a congruence*

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

*where the* $\alpha_i$ *are integers in* $\mathfrak{F}$. *Furthermore the order of ramification* $v$ *of* $\mathfrak{q}$ *in* $\mathfrak{F}(\sqrt[q]{\mu})$ *over* $\mathfrak{F}$ *is equal to* $aq+1$.

*Proof.* Since $(\mu, \mathfrak{Q}^2)=\mathfrak{Q}$, we have $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu})$ where $\mathfrak{q}$ is a prime ideal. It follows that $\sqrt[q]{\mu}$ is exactly divisible by $\mathfrak{q}$. Let $n$ be any positive integer. If $\alpha$ is any integer of $\mathfrak{F}$ we have

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

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

The order of ramification of $\mathfrak{q}$ is equal to $v$ if and only if

$$\sqrt[q]{\mu}\equiv\zeta\sqrt[q]{\mu} \pmod{\mathfrak{q}^v} \quad\text{and}\quad \sqrt[q]{\mu}\not\equiv\zeta\sqrt[q]{\mu} \pmod{\mathfrak{q}^{v+1}}.$$

Hence $v=aq+1$ since $(1-\zeta)=\mathfrak{Q}^a\mathfrak{a}$, $\mathfrak{Q}=\mathfrak{q}^q$, and $(\mathfrak{Q}, \mathfrak{a})=(1)$.

THEOREM 10. *If $\mu_1$, $\mu_2$ are two integers of $\mathfrak{F}$ each exactly divisible by $\mathfrak{Q}$, then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod* $\mathfrak{q}^{aq+1-a}$.

*Proof*. Choose a fixed residue system mod $\mathfrak{Q}$ in $\mathfrak{F}$ consisting of $q^{th}$ powers, which is possible since $\mathfrak{Q}$ is a prime ideal in $\mathfrak{F}$. Represent the residue class 0 by 0 and let $n=a(q-1)$. Since $\mu_1$ is exactly divisible by $\mathfrak{Q}$ we have

$$\mu_2\equiv\alpha_1^q\mu_1+\cdots+\alpha_n^q\mu_1^n \pmod{\mathfrak{Q}^{n+1}}$$

where the $\alpha_i^q$ belong to the fixed residue system mod $\mathfrak{Q}$ chosen above. Hence

$$\begin{aligned}(\sqrt[q]{\mu_2}-\alpha_1\sqrt[q]{\mu_1}-\cdots-\alpha_n\sqrt[q]{\mu_1^n})^q\\ \equiv\mu_2-\alpha_1^q\mu_1-\cdots-\alpha_n^q\mu_1^n \pmod{\mathfrak{Q}^{n+1}}\\ \equiv 0 \pmod{\mathfrak{Q}^{n+1}}.\end{aligned}$$

It follows that

$$\sqrt[q]{\mu_2}\equiv\alpha_1\sqrt[q]{\mu_1}+\cdots+\alpha_n\sqrt[q]{\mu_1^n} \pmod{\mathfrak{q}^{n+1}}$$

and by Theorem 9, $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{aq+1-a}$.

By Theorem 7 the fields $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ do not have corresponding residue systems mod $\mathfrak{q}^{v+1}$ where $v$ is the order of ramification of $\mathfrak{q}$. The following theorem gives a sufficient condition for $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ to have corresponding residue systems mod $\mathfrak{q}^v$.

THEOREM 11. *Let $\mu_1$, $\mu_2$ be two integers of $\mathfrak{F}$ each exactly divisible by $\mathfrak{Q}$. If $\mu_1\equiv\mu_2$ (mod $\mathfrak{Q}^{aq+1}$) then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{aq+1}$, that is, mod $\mathfrak{q}^v$ where $v$ is the order of ramification of* $\mathfrak{q}$.

*Proof*. *Since* $\mu_1\equiv\mu_2$ (mod $\mathfrak{Q}^{aq+1}$) and $(\sqrt[q]{\mu_1}-\sqrt[q]{\mu_2})^q\equiv\mu_1-\mu_2$ (mod $q$) it follows that $\sqrt[q]{\mu_1}\equiv\sqrt[q]{\mu_2}$ (mod $\mathfrak{q}^{a(q-1)}$). Suppose

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

For any polynomial $p(x, y)$ with integral coefficients such that $y$ occurs in every term we have $qp(\sqrt[q]{\mu_1}, \sqrt[q]{\mu_2})\equiv qp(\sqrt[q]{\mu_2}, \sqrt[q]{\mu_2})$ (mod $\mathfrak{q}^{m+1}q$).

Thus $(\sqrt[q]{\mu_1}-\sqrt[q]{\mu_2})^q\equiv\mu_1-\mu_2$ (mod $q\mathfrak{q}^m\mathfrak{q}$).

2.) $(\sqrt[q]{\mu_1}-\sqrt[q]{\mu_2})^q\equiv\mu_1-\mu_2$ (mod $\mathfrak{Q}^{a(q-1)}\mathfrak{q}^m\mathfrak{q}$).

If $\mu_1-\mu_2\not\equiv 0$ (mod $\mathfrak{Q}^{a(q-1)}\mathfrak{q}^m\mathfrak{q}$) then

$$q(aq+1)<aq(q-1)+m+1 \quad \text{since} \quad \mu_1\equiv\mu_2 \pmod{\mathfrak{Q}^{aq+1}}.$$

Therefore $q<-aq+m+1$ and $m\geq aq+1$. On the other hand if $\mu_1-\mu_2\equiv 0 \pmod{\mathfrak{Q}^{a(q-1)}\mathfrak{q}^m\mathfrak{q}}$ then

$$(\sqrt[q]{\mu_1}-\sqrt[q]{\mu_2})^q\equiv 0 \pmod{\mathfrak{Q}^{a(q-1)}\mathfrak{q}^m\mathfrak{q}}$$

from 2.). Thus by 1.) we have $mq\geq aq(q-1)+m+1$, $m>aq$, and hence $m\geq aq+1$. Therefore in either case $m\geq aq+1$ and we have by 1.)

$$\sqrt[q]{\mu_1}-\sqrt[q]{\mu_2}\equiv 0 \pmod{\mathfrak{q}^{aq+1}}.$$

Let $\alpha$ be any integer of $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $v$ the order of ramification of $\mathfrak{q}$, that is, $v=aq+1$. By Theorem 9

$$\alpha\equiv\alpha_0+\alpha_1\sqrt[q]{\mu_1}+\cdots+\alpha_{v-1}\sqrt[q]{\mu_1^{v-1}} \pmod{\mathfrak{q}^v}$$

where the $\alpha_i$ are integers in $\mathfrak{F}$. Let

$$\beta=\alpha_0+\alpha_1\sqrt[q]{\mu_2}+\cdots+\alpha_{v-1}\sqrt[q]{\mu_2^{v-1}}.$$

Then $\alpha\equiv\beta \pmod{\mathfrak{q}^v}$ and $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^v$.

The condition $\mu_1\equiv\mu_2 \pmod{\mathfrak{Q}^{aq+1}}$ in Theorem 11 may be replaced by $\mu_1\equiv\mu_2\sigma^q \pmod{\mathfrak{Q}^{aq+1}}$ where $\sigma$ is in $\mathfrak{F}$.

We now consider the case in which $(\mu,\mathfrak{Q})=(1)$ and the congruence $\mu\equiv\xi^q \pmod{\mathfrak{Q}^{aq}}$ is not solvable for $\xi$ in $\mathfrak{F}$, that is, $(\mu.\mathfrak{Q})=(1)$ and $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu})$. Let $k$ be the largest integer such that the congruence $\mu\equiv\xi^q \pmod{\mathfrak{Q}^k}$ is solvable for $\xi$ in $\mathfrak{F}$. Clearly $0<k<aq$ and $k$ is the largest integer such that the congruence $\sqrt[q]{\mu}\equiv\xi \pmod{\mathfrak{q}^k}$ is solvable for $\xi$ in $\mathfrak{F}$.

THEOREM 12. *Let $\mu$ be an integer of $\mathfrak{F}$ such that $(\mu,\mathfrak{Q})=(1)$ and $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu})$. Let $k$ be the largest integer such that $\mu\equiv\xi^q$ (mod $\mathfrak{Q}^k$) is solvable for $\xi$ in $\mathfrak{F}$. Then the order of ramification $v$ of $\mathfrak{q}$ with respect to $\mathfrak{F}$ is equal to $aq+1-k$.*

*Proof.* Let $\alpha$ in $\mathfrak{F}$ be a solution of the congruence $\mu\equiv\xi^q \pmod{\mathfrak{Q}^k}$ with $k$ maximal. Since $\mu-\alpha^q$ is exactly divisible by $\mathfrak{Q}^k$, it follows that $\sqrt[q]{\mu}-\alpha$ is exactly divisible by $\mathfrak{q}^k$. Furthermore we have $(k,q)=1$ (see [1, p. 153]). Thus there exist positive integers $x$ and $y$ such that $kx=1+qy$.

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

Now, let

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

Then

$$(\rho)=\frac{(\sqrt[q]{\mu}-\alpha)^x}{\mathfrak{a}^y\mathfrak{Q}^y}=\frac{(\sqrt[q]{\mu}-\alpha)^x\mathfrak{c}^y}{\mathfrak{a}^y\mathfrak{c}^y\mathfrak{Q}^y}=\frac{(\sqrt[q]{\mu}-\alpha)^x\mathfrak{c}^y}{(\omega^y)\mathfrak{Q}^y}$$

and

$$(\omega^y\rho)=\frac{(\sqrt[q]{\mu}-\alpha)^x\mathfrak{c}^y}{\mathfrak{Q}^y}.$$

The ideal fraction on the right in the last equation is an integral ideal exactly divisible by $\mathfrak{q}$, and therefore $\omega^y\rho$ is an integer of $\mathfrak{F}$ exactly divisible by $\mathfrak{q}$. It follows that the order of ramification of $\mathfrak{q}$ is equal to $v$ if and only if $\omega^y\rho-(\omega^y\rho)^A$ is exactly divisible by $\mathfrak{q}^v$ where $A$ is the automorphism $\sqrt[q]{\mu}\to\zeta\sqrt[q]{\mu}$, that is, if and only if

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

is exactly divisible by $\mathfrak{q}^v$. Since $(\omega, \mathfrak{Q})=(1)$ this is true if and only if $(\sqrt[q]{\mu}-\alpha)^x-(\zeta\sqrt[q]{\mu}-\alpha)^x$ is exactly divisible by $\mathfrak{Q}^y\mathfrak{q}^v=\mathfrak{q}^{kx-1}\mathfrak{q}^v$. Now

$$\begin{aligned}(\zeta\sqrt[q]{\mu}-\alpha)^x&=[(\zeta\sqrt[q]{\mu}-\sqrt[q]{\mu})+(\sqrt[q]{\mu}-\alpha)]^x\\&=(\sqrt[q]{\mu}-\alpha)^x+x(\sqrt[q]{\mu}-\alpha)^{x-1}(\zeta\sqrt[q]{\mu}-\sqrt[q]{\mu})+\cdots\end{aligned}$$

Therefore

$$\begin{aligned}(\zeta\sqrt[q]{\mu}-\alpha)^x&\equiv(\sqrt[q]{\mu}-\alpha)^x \pmod{\mathfrak{q}^{k(x-1)}(1-\zeta)}\\&\equiv(\sqrt[q]{\mu}-\alpha)^x \pmod{\mathfrak{q}^{k(x-1)}\mathfrak{q}^{aq}}\end{aligned}$$

since $0<k<aq$ and $(1-\zeta)=\mathfrak{Q}^a\mathfrak{a}$ with $(\mathfrak{Q}, \mathfrak{a})=(1)$. Furthermore this congruence holds exactly mod $\mathfrak{q}^{k(x-1)}\mathfrak{q}^{aq}$. It follows that $kx-1+v=k(x-1)+aq$ and $v=aq+1-k$.

THEOREM 13. *Let $\mu_1$, $\mu_2$ be two integers of $\mathfrak{F}$ each prime to $\mathfrak{Q}$ and such that $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ (and $\mathfrak{F}(\sqrt[q]{\mu_2})$. Let $k_i$ be the largest integer such that the congruence $\mu_i\equiv\alpha_i^q$ (mod $\mathfrak{Q}^{k_i}$) is solvable for $\alpha_i$, an integer of $\mathfrak{F}$ $(i=1, 2)$. Let $v_i=aq+1-k_i$ for $i=1, 2$, and suppose $v_1\geqq v_2>a$. Then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{v_2-a}$.*

*Proof.* Since $\mu_i - \alpha_i^q$ is exactly divisible by $\mathfrak{Q}^{k_i}$ it follows that $\sqrt[q]{\mu_i} - \alpha_i$ is exactly divisible by $\mathfrak{q}^{k_i}$ for $i=1, 2$. Since $(k_i, q)=1$ we have positive integers $x_i$ and $y_i$ such that $k_i x_i = 1 + q y_i$ for $i=1, 2$. Let $\pi$ be an integer of $\mathfrak{F}$ exactly divisible by $\mathfrak{Q}$. Using the method of Theorem 12 we obtain an integer

$$\theta_i = \frac{\omega^{y_i}(\sqrt[q]{\mu_i} - \alpha_i)^{x_i}}{\pi^{y_i}}$$

of $\mathfrak{F}(\sqrt[q]{\mu_i})$ which is exactly divisible by $\mathfrak{q}$ for $i=1, 2$.

We now show that $\theta_i^q$ is congruent to an integer of $\mathfrak{F}$ mod $\mathfrak{Q}^{v_i - a}$ for $i=1, 2$. We have

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

where $\lambda_i$ is an integer of $\mathfrak{F}$ and $\lambda_i \equiv 0 \pmod{\mathfrak{Q}^{k_i}}$. Hence since $\rho_i$ is divisible by $\mathfrak{q}^{k_i}$

$$\begin{aligned}\theta_i^q &= \frac{\omega^{y_i q}(\lambda_i^{x_i} - x_i \lambda_i^{x_i - 1}\rho_i q + \cdots)}{\pi^{y_i q}} \\ &= \frac{\omega^{y_i q}\lambda_i^{x_i}}{\pi^{y_i q}} - \frac{(\omega^{y_i q} x_i \lambda_i^{x_i - 1}\rho_i q + \cdots)}{\pi^{y_i q}} \\ &\equiv \frac{\omega^{y_i q}\lambda_i^{x_i}}{\pi^{y_i q}} \quad (\text{mod } \mathfrak{Q}^{aq+1-k_i-a}) \\ &\equiv \frac{\omega^{y_i q}\lambda_i^{x_i}}{\pi^{y_i q}} \quad (\text{mod } \mathfrak{Q}^{v_i - a})\end{aligned}$$

But the expression on the right of the last congruence is an integer of $\mathfrak{F}$, so that $\theta_i^q$ is congruent to an integer of $\mathfrak{F}$ mod $\mathfrak{Q}^{v_i - a}$.

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

Let $\beta$ be any integer of $\mathfrak{F}(\sqrt[q]{\mu_1})$ and let $n = v_1 - a$. Since $\theta_1$ is exactly divisible by $\mathfrak{q}$ we have $\beta \equiv \beta_0 + \beta_1\theta_1 + \cdots + \beta_{n-1}\theta_1^{n-1} \pmod{\mathfrak{q}^n}$, where the $\beta_i$ are residues mod $\mathfrak{q}$ and may be chosen in $\mathfrak{F}$ since $\mathfrak{q}$ is of degree 1 over $\mathfrak{F}$. Hence

$$\begin{aligned}&[\beta - (\beta_0 + \cdots + \beta_{n-1}\theta_1^{n-1})]^q \\ &\equiv \beta^q - (\beta_0 + \cdots + \beta_{n-1}\theta_1^{n-1})^q \pmod{q} \\ &\equiv \beta^q - (\beta_0^q + \cdots + \beta_{n-1}^q \theta_1^{q(n-1)}) \pmod{q} \\ &\equiv \beta^q - \sigma \mod (\mathfrak{Q}^{v_1 - a}),\end{aligned}$$

where $\sigma$ is an integer of $\mathfrak{F}$. It follows that $\beta^q \equiv \sigma \pmod{\mathfrak{Q}^{v_1 - a}}$.

If $\beta$ and $\beta'$ are two integers of $\mathfrak{F}(\sqrt[q]{\mu_1})$ such that $\beta^q \equiv \sigma$ (mod $\mathfrak{Q}^{v_1-a}$) and $\beta'^q \equiv \sigma$ (mod $\mathfrak{Q}^{v_1-a}$), then $\beta \equiv \beta'$ (mod $\mathfrak{q}^{v_1-a}$). Also if $\beta^q \equiv \sigma$ (mod $\mathfrak{Q}^{v_1-a}$) and $\beta^q \equiv \sigma'$ (mod $\mathfrak{Q}^{v_1-a}$) where $\sigma$, $\sigma'$ are integers of $\mathfrak{F}$, then $\sigma \equiv \sigma'$ (mod $\mathfrak{Q}^{v_1-a}$). The number of residue classes mod $\mathfrak{q}^{v_1-a}$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ is equal to the number of residue classes mod $\mathfrak{Q}^{v_1-a}$ in $\mathfrak{F}$. It follows that if $\sigma$ is any integer of $\mathfrak{F}$ there exists an integer $\beta$ of $\mathfrak{F}(\sqrt[q]{\mu_1})$ such that ${}^q\beta \equiv \sigma$ (mod $\mathfrak{Q}^{v_1-a}$).

Similarly, if $\gamma$ is any integer of $\mathfrak{F}(\sqrt[q]{\mu_2})$ there exists an integer $\tau$ of $\mathfrak{F}$ such that $\gamma^q \equiv \tau$ (mod $\mathfrak{Q}^{v_2-a}$). There exists an integer $\beta$ of $\mathfrak{F}(\sqrt[q]{\mu_1})$ such that $\beta^q \equiv \tau$ (mod $\mathfrak{q}^{v_1-a}$). Since $v_1 \geqq v_2$ we have $\beta^q \equiv \gamma^q$ (mod $\mathfrak{Q}^{v_2-a}$) and therefore $\beta \equiv \gamma$ (mod $\mathfrak{q}^{v_2-a}$).

THEOREM 14. *If $\mu_1$, $\mu_2$ are two integers of $\mathfrak{F}$ such that $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$, and $\mathfrak{q}$ has ramification orders $\geqq v > a$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$, $\mathfrak{F}(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$, then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{v-a}$.*

*Proof.* We need only to consider the case in which $\mu_1$ is exactly divisible by $\mathfrak{Q}$ and $\mu_2$ is prime to $\mathfrak{Q}$, the other two cases following from Theorems 10 and 13.

Let $v_1 = aq+1$ be the order of ramification of $\mathfrak{q}$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ over $\mathfrak{F}$, and let $v_2$ be the order of ramification of $\mathfrak{q}$ in $F(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$. From Theorem 12 it follows that $v_1 - 1 = aq \geqq v_2$.

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

$$\alpha \equiv \alpha_0 + \alpha_1 \sqrt[q]{\mu_1} + \cdots + \alpha_{n-1} \sqrt[q]{\mu_1^{n-1}} \pmod{\mathfrak{q}^n},$$

where the $\alpha_i$ are integers in $\mathfrak{F}$. Hence

$$\alpha^q \equiv \alpha_0^q + \alpha_1^q \mu_1 + \cdots + \alpha_{n-1}^q \mu_1^{n-1} \pmod{\mathfrak{Q}^n}$$
$$\equiv \sigma \pmod{\mathfrak{Q}^{aq-a}}$$

where $\sigma$ is an integer of $\mathfrak{F}$. Using the method of Theorem 13, there exists an integer $\beta$ of $\mathfrak{F}(\sqrt[q]{\mu_2})$ such that $\beta^q \equiv \sigma$ (mod $\mathfrak{Q}^{v_2-a}$). Therefore $\alpha^q \equiv \beta^q$ (mod $\mathfrak{Q}^{v_2-a}$) and $\alpha \equiv \beta$ (mod $\mathfrak{q}^{v_2-a}$). Thus $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{v-a}$ where $v_2 \geqq v > a$.

THEOREM 15. *Let $\mu_1$, $\mu_2$ be two integers of $\mathfrak{F}$, each prime to $\mathfrak{Q}$, such that $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$. Suppose $\mu_1 \equiv \mu_2$* (mod $\mathfrak{Q}^{aq}$) and let $k$ be the largest integer such that the congruences $\mu_1 \equiv \alpha^q$ (mod $\mathfrak{Q}^k$) and $\mu_2 \equiv \alpha^q$ (mod $\mathfrak{Q}^k$) are solvable for $\alpha$ an integer of $\mathfrak{F}$.

Then $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^v$ where $v=aq+1-k$.

*Proof.* Since $\mu_1 \equiv \mu_2 \pmod{\mathfrak{Q}^{aq}}$ it follows that $\sqrt[q]{\mu_1} \equiv \sqrt[q]{\mu_2}$ (mod $\mathfrak{Q}^a$) using the method of Theorem 11. We have $kx = 1 + qy$ and following Theorem 12 it is sufficient to show that

$$(\sqrt[q]{\mu_1}-\alpha)^x \equiv (\sqrt[q]{\mu_2}-\alpha)^x \pmod{\mathfrak{q}^{v+qy}} .$$

We have

$$\begin{aligned}(\sqrt[q]{\mu_2}-\alpha)^x &= [(\sqrt[q]{\mu_1}-\alpha)+(\sqrt[q]{\mu_2}-\sqrt[q]{\mu_1})]^x \\ &= (\sqrt[q]{\mu_1}-\alpha)^x + x(\sqrt[q]{\mu_1}-\alpha)^{x-1}(\sqrt[q]{\mu_2}-\sqrt[q]{\mu_1}) + \cdots \\ &= (\sqrt[q]{\mu_1}-\alpha)^x \pmod{\mathfrak{q}^{k(x-1)}\mathfrak{q}^{aq}} \\ &\equiv (\sqrt[q]{\mu_1}-\alpha)^x \pmod{\mathfrak{q}^{v+qy}} .\end{aligned}$$

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

We remark that if $\mathfrak{F}(\sqrt[q]{\mu_1}) \neq \mathfrak{F}(\sqrt[q]{\mu_2})$ then $\sqrt[q]{\mu_1} \not\equiv \sqrt[q]{\mu_2} \pmod{\mathfrak{q}^{aq+1}}$ for otherwise we would have corresponding residue systems mod $\mathfrak{q}^{v+1}$ contrary to Theorem 7.

In Theorem 15 we may replace the condition $\mu_1 \equiv \mu_2 \pmod{\mathfrak{Q}^{aq}}$ by $\mu_1 \equiv \mu_2 \beta^q \pmod{\mathfrak{Q}^{aq}}$ with $\beta$ in $\mathfrak{F}$.

THEOREM 16. *Let $\mu_1$, $\mu_2$ be two integers of $\mathfrak{F}$ such that $\mathfrak{Q}=\mathfrak{q}^q$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and in $\mathfrak{F}(\sqrt[q]{\mu_2})$ and the orders of ramification of $\mathfrak{q}$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$ are $\geq aq$. In order that $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{aq}=\mathfrak{Q}^a$ it is necessary and sufficient that the following congruences be solvable in $\mathfrak{F}$:*

$$\sum_{\substack{e_0+e_1+\cdots+e_{q-1}=q \\ e_1+2e_2+\cdots+(q-1)e_{q-1}=mq+i}} \frac{q!}{e_0!e_1!\cdots e_{q-1}!}\alpha_0^{e_0}\alpha_1^{e_1}\cdots\alpha_{q-1}^{e_{q-1}}\mu_2^m \equiv 0 \quad (mod\ \mathfrak{Q}^{aq})$$

$$\sum_{\substack{e_0+\cdots+e_{q-1}=q \\ e_1+2e_2+\cdots+(q-1)e_{q-1}=mq}} \frac{q!}{e_0!\cdots e_{q-1}!}\alpha_0^{e_0}\cdots\alpha_{q-1}^{e_{q-1}}\mu_2^m \equiv \mu_1 \quad (mod\ \mathfrak{Q}^{aq}) ,$$

*where $\alpha_0, \cdots, \alpha_{q-1}$ are integers of $\mathfrak{F}$ and $e_0, e_1, \cdots, e_{q-1}, m$ are nonnegative* *integers, and* $i=1, \cdots, q-1$; *and the same congruences with* $\mu_1$ *and* $\mu_2$ *interchanged.*

*Proof.* Since the orders of ramification of $\mathfrak{q}$ in $\mathfrak{F}(\sqrt[q]{\mu_j})$ over $\mathfrak{F}$ are $\geqq aq$ for $j=1, 2$, then either $\sqrt[q]{\mu_j}$ is exactly divisible by $\mathfrak{q}$ or $\sqrt[q]{\mu_j}$ is prime to $\mathfrak{q}$ and there exists an integer $\xi_j$ of $\mathfrak{F}$ such that $\sqrt[q]{\mu_j}-\xi_j$ is exactly divisible by $\mathfrak{q}$. In either case $1, \sqrt[q]{\mu_j}, \cdots, \sqrt[q]{\mu_j^{n-1}}$ form a basis for the residue system mod $\mathfrak{q}^n$, $n$ a given positive integer.

If $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $\mathfrak{q}^{aq}$ we have

$$1.)\qquad \sqrt[q]{\mu_1}\equiv\alpha_0+\alpha_1\sqrt[q]{\mu_2}+\cdots+\alpha_{q-1}\sqrt[q]{\mu_2^{q-1}} \pmod{\mathfrak{Q}^a}$$

$$2.)\qquad \mu_1\equiv(\alpha_0+\alpha_1\sqrt[q]{\mu_2}+\cdots+\alpha_{q-1}\sqrt[q]{\mu_2^{q-1}})^q \pmod{\mathfrak{Q}^{aq}}$$

and the congruences of the theorem follow.

Conversely if the congruences of the theorem are valid then 2.) is valid and 1.) follows. Interchanging the roles of $\mu_1$ and $\mu_2$, the converse follows.

THEOREM 17. *If* $\mathfrak{F}=R(\zeta)$, $q=3$, *and* $\mathfrak{F}(\sqrt[q]{\mu_1})$ *and* $\mathfrak{F}(\sqrt[q]{\mu_2})$ *have corresponding residue systems* mod $(1-\zeta)$, *then either* $\mu_1\equiv\alpha^3\mu_2^\varepsilon \pmod{3(1-\zeta)}$ *where* $\alpha$ *is in* $R(\zeta)$ *and* $\varepsilon=1$ *or* 2, *or* $\mu_1\equiv\mu_2\equiv0 \pmod{(1-\zeta)}$.

*Proof.* In $R(\zeta)$ the ideal $(1-\zeta)$ is a prime ideal, that is, $(1-\zeta)=\mathfrak{Q}$. Since $\mathfrak{F}(\sqrt[q]{\mu_1})$ and $\mathfrak{F}(\sqrt[q]{\mu_2})$ have corresponding residue systems mod $(1-\zeta)$ we have $(1-\zeta)=\mathfrak{q}^3$, and the orders of ramification of $\mathfrak{q}$ in $\mathfrak{F}(\sqrt[q]{\mu_1})$, $\mathfrak{F}(\sqrt[q]{\mu_2})$ over $\mathfrak{F}$ are $\geqq3$, and hence either 3 or 4. In either case $1, \sqrt[3]{\mu_j}, \sqrt[3]{\mu_j^2}$ form a basis for the residue system mod $(1-\zeta)$ in $\mathfrak{F}(\sqrt[q]{\mu_j})$ for $j=1, 2$.

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

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

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

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 $(1-\zeta)$, and the coefficients of $\sqrt[3]{\mu_2}$ and $\sqrt[3]{\mu_2^2}$ in $P(\sqrt[3]{\mu_2})$ must vanish mod $(1-\zeta)$. Thus

$$\alpha_0^2\alpha_1+\alpha_0\alpha_2^2\mu_2+\alpha_1^2\alpha_2\mu_2\equiv0 \pmod{(1-\zeta)}$$

$$\alpha_0\alpha_1^2+\alpha_1\alpha_2^2\mu_2+\alpha_0^2\alpha_2\equiv 0 \pmod{(1-\zeta)}\,.$$

By considering two cases, $\mu_2\equiv 0 \pmod{(1-\zeta)}$ and $\mu_2\not\equiv 0 \pmod{(1-\zeta)}$, the conclusion of the theorem follows from the last two congruences.

## REFERENCE

1. E. Hecke, *Theorie der Algebraischen Zahlen*, Leipzig, 1923.

LOUISIANA STATE UNIVERSITY AND OHIO STATE UNIVERSITY