ILLINOIS JOURNAL OF MATHEMATICS
Volume 40, Number 1, Spring 1996

A NEW LOWER BOUND FOR CORRESPONDING RESIDUE SYSTEMS IN NORMAL, TOTALLY RAMIFIED EXTENSIONS OF NUMBER FIELDS

STEVEN R. BENSON

Introduction

Let F be the quotient field of a Dedekind domain $\mathfrak{O}_F$ having finite residue fields $\mathfrak{O}_F/\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of $\mathfrak{O}_F$ (e.g., a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$). Let K, K' and L be finite extensions of F such that L/F is normal, $KK' \subseteq L$ and $K \cap K' = F$. If $\mathfrak{A}$ is an ideal of $\mathfrak{O}_L$ such that $\mathfrak{O}_K + \mathfrak{A} = \mathfrak{O}_{K'} + \mathfrak{A}$, then $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ are said to have *corresponding residue systems* mod $\mathfrak{A}$. We are interested in finding $\mathfrak{M}(K, K')$, the unique minimal ambiguous (over F) ideal of $\mathfrak{O}_L$ so that $\mathfrak{O}_K + \mathfrak{M}(K, K') = \mathfrak{O}_{K'} + \mathfrak{M}(K, K')$. In this paper, we will usually focus on the (local) case where F is a finite extension of $\mathbb{Q}_p$, L/F is totally ramified, and K/F and K'/F are normal extensions. In this case, $\mathfrak{M}(K, K')$ is a power of $\mathfrak{P}$, the unique maximal ideal of $\mathfrak{O}_L$, so our task is to find $M_L(K, K')$, the largest integer m so that $\mathfrak{O}_K + \mathfrak{P}^m = \mathfrak{O}_{K'} + \mathfrak{P}^m$. The method developed by the author utilizes canonical invariants of the field towers $L/K/F$ and $L/K'/F$, which are determined by the ith elementary symmetric functions on the sets $\{(\sigma\pi - \pi)/\pi\colon \sigma \in G\}$ and $\{(\sigma'\pi' - \pi')/\pi'\colon \sigma' \in G'\}$, where π (resp. π') is an arbitrary prime element of $\mathfrak{O}_K$ (resp. $\mathfrak{O}_{K'}$). We see that these invariants can be computed in terms of $\operatorname{irr}_F(\pi)$, but are actually independent of the choice of π. By comparing the invariants associated to $L/K/F$ and $L/K'/F$, we show that

$$M_L(K, K') \geq p^n(t+1) - tp^{n-1},$$

where $t = \min\{t_1(K/F), t_1(K'/F)\}$, and $t_1(K/F)$ (resp. $t_1(K'/F)$) denotes the first breakpoint in the Hilbert ramification sequence for $\operatorname{Gal}(K/F)$ (resp. $\operatorname{Gal}(K'/F)$). In addition, we prove that if $1 = t_1(K/F) < t_1(K'/F)$, then $M_L(K, K')$ can be computed completely in terms of the coefficients of $\operatorname{irr}_F(\pi)$, where again π is *any* prime element of $\mathfrak{O}_K$. This, together with a previous result of the author, provides a method for determining $M_L(K, K')$ whenever $\min\{t_1(K/F), t_1(K'/F)\} = 1$. As a final consequence, we "globalize" our results in order to sharpen previous lower bounds for the highest power of $\mathfrak{P}$ dividing $\mathfrak{M}(K, K')$ when F is an algebraic number field.

In this article, we intend to expand on the results of [1], where the author's methods were introduced. As in [1] then, unless otherwise specified, we will assume that F

Received September 27, 1993
1991 Mathematics Subject Classification. Primary 11S15; Secondary 11R, 12F.

is a finite extension of $\mathbb{Q}_p$ and that L/F is a normal, totally ramified extension with normal subextensions K/F and K'/F satisfying $KK' = L$, $K \cap K' = F$ and $[K : F] = [K' : F] = p^n$. Denote by $\mathfrak{P}_K$ and $\mathfrak{P}_{K'}$ the maximal ideals of $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$, respectively.

Stout showed in 3.1 and 4.1 of [6] that, under these hypotheses,

$$p^n(t_1(L/F)+1)-p^{n-1}t_1(L/F) \le M_L(K, K') \le \min\begin{Bmatrix} p^n(t_1(K/F)+1)-t_1(L/K'), \\ p^n(t_1(K'/F)+1)-t_1(L/K). \end{Bmatrix} \quad (0.1)$$

If, in addition, K/F and K'/F are *cyclic* extensions, then McCulloh and Stout proved (in Theorem 3.1 of [3] and Theorem A of [4])

$$M_L(K, K') = p^n(t+1) - p^{n-1}t_1(L/F),$$

where, as above, $t = \min\{t_1(K/F), t_1(K'/F)\}$.

In Chapter V of [7], Vogt constructed a finite extension F of $\mathbb{Q}_2$ and an elementary abelian, totally ramified extension L/F of degree 16 such that the Hilbert sequence for L/F had a unique breakpoint at 1. Therefore, the sequences for all subextensions also had unique breakpoints at 1. However, he then exhibited subfields K, K' and K'' of L such that $K \cap K' = K' \cap K'' = F$ and $KK' = K'K'' = L$, but $M_L(K, K') \neq M_L(K', K'')$, showing that the knowledge of the ramification numbers alone does not suffice, in general, if one is interested in computing $M_L(K, K')$.

The invariants introduced in [1] (and mentioned briefly above) are computed as follows: Recall that if π is any prime element of $\mathfrak{P}_K$, then an element $\sigma \in G$ $(= \mathrm{Gal}(K/F))$ is in the ith ramification subgroup G_i of G if and only if $\sigma\pi - \pi \in \mathfrak{P}_K^{i+1}$. Let $t = t_1(K/F) = \min\{i\colon G_i \neq G_{i+1}\}$ (the first breakpoint in the ramification sequence, which will be greater than or equal to 1 in this case). Note that since L/F is totally ramified and $[L : K] = p^n$, we have $\mathfrak{P}_K^i\mathfrak{O}_L = \mathfrak{P}^{ip^n}$. For $i = 1, \ldots, p^n - 1$, we define $\varepsilon_i \in \mathfrak{P}^{itp^n}/\mathfrak{P}^{itp^n+1}$ to be the ith elementary symmetric function on the set $\{(\sigma\pi - \pi)/\pi + \mathfrak{P}^{tp^n+1}\colon \sigma \in G\}$ (Alternatively, one can think of ε_i as the canonical image (in $\mathfrak{P}^{itp^n}/\mathfrak{P}^{itp^n+1}$) of the ith elementary symmetric function of $\{(\sigma\pi - \pi)/\pi\}$). The author showed in [1] that each ε_i is independent of the choice of π and is thus an invariant of the extension $L/K/F$. We similarly define the invariant $\varepsilon_i' \in \mathfrak{P}^{it'p^n}/\mathfrak{P}^{it'p^n+1}$ to be the ith elementary symmetric function on the set $\{(\sigma'\pi' - \pi')/\pi' + \mathfrak{P}^{t'p^n+1}\colon \sigma' \in G'\}$, where π' is a prime element of $\mathfrak{O}_{K'}$ and $t' = t_1(K'/F)$. Under the additional hypothesis that $t_1(K/F) = t_1(K'/F) = 1$, the author showed in Theorem 3.1 of [1] that $M_L(K, K') = p^n + i$, where i is the smallest integer satisfying $\varepsilon_i \neq \varepsilon_i'$ (in fact, it was shown that i will always take the form $p^n - p^k$ for some $0 \le k \le n-1$).

In this article, we will eliminate the assumption that $t_1(K/F) = t_1(K'/F) = 1$ and use our invariants to determine (or provide bounds for) $M_L(K, K')$. Toward this end, in the following section, we review some background material concerning our invariants and obtain necessary preliminary results.

1. Preliminary results

In this preliminary section, we will present several results which will be needed in both of the succeeding sections. We shall assume throughout that F is a finite extension of $\mathbb{Q}_p$ and that L, K and K' are normal, totally ramified extensions of F satisfying $K \cap K' = F$, $KK' = L$ and $[K : F] = [K' : F] = [L : K] = p^n$. Recall that, if $\mathfrak{P}$ is the maximal ideal of $\mathfrak{O}_L$, then $M_L(K, K')$ is defined to be the largest rational integer m so that $\mathfrak{O}_K + \mathfrak{P}^m = \mathfrak{O}_{K'} + \mathfrak{P}^m$. As was demonstrated in [1], there is a connection between $M_L(K, K')$ and the coefficients of $\mathrm{irr}_F(\pi)$ and $\mathrm{irr}_F(\pi')$, where π and π' are prime elements of $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$, respectively. By (1.1) and (1.2) of [1], we know that

$$M_L(K, K') = \max\{v_L(\pi - \pi') \colon \pi\mathfrak{O}_K = \mathfrak{P}_K \text{ and } \pi'\mathfrak{O}_{K'} = \mathfrak{P}_{K'}\} \tag{1.1}$$

and

$$v_L(\pi - \pi') = \min\{v_K(a_i - a_i') + i \colon 0 \le i \le p^n - 1\}, \tag{1.2}$$

if we define $\mathrm{irr}_F(\pi) = a_0 + a_1x + \cdots + a_{p^n-1}x^{p^n-1} + x^{p^n}$ and $\mathrm{irr}_F(\pi') = a_0' + a_1'x + \cdots + a_{p^n-1}'x^{p^n-1} + x^{p^n}$.

Next, we illustrate the connection between the invariants $\{\varepsilon_i \colon 1 \le i \le p^n - 1\}$ and the coefficients of $\mathrm{irr}_F(\pi)$ by stating, without proof, Proposition 2.1 of [1].

(1.3) LEMMA. *Let π be a prime element of $\mathfrak{O}_K$ with $\mathrm{irr}_F(\pi) = a_0 + a_1x + \cdots + x^{p^n}$ and define $a_{p^n} = 1$. For $1 \le i \le p^n - 1$ and $t = t_1(K/F)$, let $0 \le j \le p^n - 1$ satisfy $j \equiv it \pmod{p^n}$. Then*

$$\varepsilon_i = (-1)^i a_j \binom{j}{p^n - i} \pi^{j-p^n} + \mathfrak{P}^{itp^n+1} \quad \left(\textit{where } j < p^n - i \textit{ implies } \binom{j}{p^n - i} = 0\right).$$

Furthermore, for all l, $v_K\left(a_l \binom{l}{p^n - i} \pi^{l-p^n}\right) \ge it$ with equality only if $l \equiv it \pmod{p^n}$.

The key to (1.3), as was proved in [1], is that ε_i is independent of the choice of prime element π. As K/F is totally ramified and π is a prime element of $\mathfrak{O}_K$, we know that $\mathrm{irr}_F(\pi)$ is an Eisenstein polynomial, and therefore, the constant term a_0 satisfies $v_K(a_0) = [K : F] = p^n$. The next two propositions use (1.3) to provide lower bounds for the degree of divisibility of the other coefficients of $\mathrm{irr}_F(\pi)$ by $\mathfrak{P}_K$. The next proposition is a restatment of (2.6) from [1].

(1.4) PROPOSITION. *Let K/F be a normal, totally ramified extension of degree p^n with $t = t_1(K/F) < p$. Suppose π is a prime element of $\mathfrak{O}_K$ with* $\operatorname{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$. *If $0 < l < p^n$ and $v_p(l) = k$, then*

$$v_K(a_l) \geq (t+1)p^n \qquad \text{if } l < p^n - tp^k,$$
$$v_K(a_l) \geq tp^n \qquad \text{if } l \geq p^n - tp^k.$$

In particular, when $t = 1$, (1.4) gives us

$$\text{(1)} \qquad v_K(a_l) \geq 2p^n \qquad \text{if } l < p^n - p^k,$$
$$v_K(a_l) \geq p^n \qquad \text{if } l = p^n - p^k.$$

In this article, we will not necessarily assume that $t_1(K/F) < p$, so we need to prove the following generalization of (1.4).

(1.6) PROPOSITION. *Suppose K/F is a normal, totally ramified extension with $[K : F] = p^n$ and $t = t_1(K/F)$. Let π be a prime element of $\mathfrak{O}_K$ with* $\operatorname{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$. *If $0 < l < p^n$ and $v_p(l) = k$, then*

$$v_K(a_l) \geq tp^n - (t-1)p^k.$$

Proof. Let l be given and suppose $v_p(l) = k$. By (2.5) of [1], we know that $v_p\left(\binom{l}{p^k}\right) = 0$, so $v_K\left(\binom{l}{p^k}\right) = 0$, as well. Letting $i = p^n - p^k$ in (1.3), we have

$$(p^n - p^k)t \leq v_K\left(a_l \binom{l}{p^k} \pi^{l-p^n}\right) = v_K(a_l) + l - p^n.$$

Observing that $l \leq p^n - p^k$, the proposition follows immediately. □

A fact which will prove to be useful in the section which follows is that if $t > 1$, then $tp^n - (t-1)p^k - (2p^n - p^k) = (t-2)(p^n - p^k) \geq 0$, so $tp^n - (t-1)p^k \geq (2p^n - p^k)$. Therefore, by (1.6), if $v_p(l) = k$, then $v_K(a_l) \geq 2p^n - p^k$. Finally, since $a_l \in F$ for each l, we know that $v_K(a_l)$ is an integral multiple of p^n, so we may conclude:

$$\text{If } t > 1, \text{ then } v_K(a_l) \geq 2p^n, \text{ for all } 0 < l < p^n. \tag{1.7}$$

2. The case $\min\{t_1(K/F), t_1(K'/F)\} = 1$

In this section, L/F is a normal, totally ramified extension of degree p^{2n} with normal subextensions K/F and K'/F satisfying $K \cap K' = F$, $KK' = L$ and $[K : F] = [K' : F] = p^n$. We will also assume that $\min\{t_1(K/F), t_1(K'/F)\} = 1$. For ease of notation, we shall denote $t = t_1(K/F)$ and $t' = t_1(K'/F)$. Recall that the case $t = t' = 1$ was addressed in [1], so we shall assume that $t = 1$ and $t' > 1$.

The following theorem provides a method of computing $M_L(K, K')$ in terms of the canonical invariants ε_i of K/F.

(2.1) THEOREM. *If* $1 = t < t'$, *then* $M_L(K, K') = 2p^n - p^k$, *where* $p^n - p^k = \min\{i \colon \varepsilon_i \neq 0 + \mathfrak{P}^{ip^n+1}\}$.

Proof. As ε_i is independent of the choice of prime element π of $\mathfrak{O}_K$, let us assume that we have chosen π and π' so that $v_L(\pi - \pi') = M_L(K, K')$, and let $\mathrm{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$ and $\mathrm{irr}_F(\pi') = \sum_{i=0}^{p^n} a_i' x^i$. Let $0 < l < p^n$ and suppose that $v_p(l) = k$. Since $t = 1$, (1.5) gives us

$$\begin{aligned} v_K(a_l) &\geq 2p^n \qquad \text{if } l \neq p^n - p^k, \\ v_K(a_l) &\geq p^n \qquad \text{if } l = p^n - p^k. \end{aligned}$$

In particular, if $l \neq p^n - p^k$, then $a_l \in \mathfrak{P}^{2p^{2n}}$, so $\varepsilon_l = 0 + \mathfrak{P}^{lp^n+1}$ by (1.3).

Since $t' > 1$, (1.7) gives us $v_{K'}(a_l') \geq 2p^n$. As $a_l' \in F$, and the extensions K/F and K'/F are totally ramified of equal degree, we have $v_K(a_l') = v_{K'}(a_l') \geq 2p^n$. Therefore, if $l \neq p^n - p^k$, then $v_K(a_l - a_l') \geq \min\{v_K(a_l), v_K(a_l')\} \geq 2p^n$, which implies $v_K(a_l - a_l') + l > 2p^n$. However, by (1.2) and (0.1), $2p^n - 1 \geq v_L(\pi - \pi') = \min\{v_K(a_i - a_i') + i \colon 0 \leq i \leq p^n - 1\}$, and we may conclude that $M_L(K, K') \neq v_K(a_l - a_l') + l$ for such l. To summarize, we have proven that, if $v_p(l) = k$ and $l \neq p^n - p^k$, then $\varepsilon_l = 0 + \mathfrak{P}^{lp^n+1}$ and $M_L(K, K') \neq v_K(a_l - a_l') + l$. Note that, by (0.1), $M_L(K, K') \geq 2p^n - p^{n-1}$, so $\min\{v_K(a_i - a_i') + i\} \geq 2p^n - p^{n-1}$, by (1.2). In particular, $v_K(a_0 - a_0') + 0 \geq 2p^n - p^{n-1}$. Therefore, since $a_0 - a_0' \in F$, $v_K(a_0 - a_0') \geq 2p^n$ $(> M_L(K, K'))$. Hence

$$M_L(K, K') = \min\{v_K(a_{p^n-p^k} - a'_{p^n-p^k}) + p^n - p^k \colon 0 \leq k \leq n-1\}.$$

Next, we shall investigate the case $l = p^n - p^k$.

Suppose that $l = p^n - p^k$ for some $0 \leq k \leq n-1$. Then, by (1.3),

$$\begin{aligned} \varepsilon_{p^n-p^k} \neq 0 + \mathfrak{P}^{p^{2n}-p^{k+n}+1} &\iff v_L(a_{p^n-p^k}) < p^{2n} + 1 \\ &\qquad\qquad \left(\text{since } v_L\left(\binom{p^n - p^k}{p^k}\right) = 0\right) \\ &\iff v_K(a_{p^n-p^k}) < p^n + 1 \\ &\qquad\qquad (\text{since } v_L(a_{p^n-p^k}) = p^n \cdot v_K(a_{p^n-p^k})) \\ &\iff v_K(a_{p^n-p^k}) = p^n \qquad (\text{since } a_{p^n-p^k} \in \mathfrak{O}_F) \\ &\iff v_K\left(a_{p^n-p^k} - a'_{p^n-p^k}\right) = p^n \\ &\qquad\qquad (\text{since } v_K(a'_{p^n-p^k}) \geq 2p^n) \\ &\iff v_K\left(a_{p^n-p^k} - a'_{p^n-p^k}\right) + p^n - p^k = 2p^n - p^k. \end{aligned}$$

We have shown, then, that

$$\varepsilon_{p^n-p^k} \neq 0 + \mathfrak{P}^{p^{2n}-p^{k+n}+1} \iff v_K(a_{p^n-p^k} - a'_{p^n-p^k}) + p^n - p^k = 2p^n - p^k.$$

As $2p^n - 1 \geq M_L(K, K') = \min\{v_K(a_{p^n-p^k} - a'_{p^n-p^k}) + p^n - p^k\}$, we know that

$$\begin{aligned} M_L(K, K') &= v_K(a_{p^n-p^k} - a'_{p^n-p^k}) + p^n - p^k \\ &\iff p^n - p^k = \min\{i\colon v_K(a_i - a'_i) = p^n\} \\ &\iff p^n - p^k = \min\{i\colon \varepsilon_i \neq 0 + \mathfrak{P}^{ip^n+1}\}, \end{aligned}$$

and the theorem is proved. □

Notice that, in the midst of the above proof, we demonstrated another technique for computing $M_L(K, K')$, for we showed that if π is chosen (along with π') to satisfy $M_L(K, K') = v_L(\pi - \pi')$, then

$$\varepsilon_{p^n-p^k} \neq 0 + \mathfrak{P}^{p^{2n}-p^{k+n}+1} \iff v_K(a_{p^n-p^k}) = p^n.$$

However, since each ε_i is independent of the choice of π, the proof of (2.1) actually shows that if $\overline{\pi}$ is *any* prime element of $\mathfrak{O}_K$ and $\operatorname{irr}_F(\overline{\pi}) = \sum_{i=0}^{p^n} b_i x^i$, then

$$\varepsilon_{p^n-p^k} \neq 0 + \mathfrak{P}^{p^{2n}-p^{k+n}+1} \iff v_K(b_{p^n-p^k}) = p^n.$$

By (2.1), we have $M_L(K, K') = 2p^n - p^k$, where $p^n - p^k = \min\{i\colon \varepsilon_i \neq 0 + \mathfrak{P}^{ip^n+1}\}$, so we know that

$$\begin{aligned} M_L(K, K') = 2p^n - p^k &\iff p^n - p^k = \min\{i > 0\colon v_K(b_i) = p^n\} \\ &\iff p^n - p^k = \min\{i > 0\colon v_F(b_i) = 1\} \\ &\iff p^n - p^k = \min\{i > 0\colon b_i \notin \mathfrak{p}^2\}, \end{aligned}$$

where $\mathfrak{p}$ is the maximal ideal of $\mathfrak{O}_F$. Hence, we have proven the following:

(2.2) COROLLARY. *Suppose $1 = t < t'$ and that π is a prime element of $\mathfrak{O}_K$ with $\operatorname{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$. If $\mathfrak{p}$ is the maximal ideal of $\mathfrak{O}_F$, then $M_L(K, K') = 2p^n - p^k$ where $p^n - p^k = \min\{i > 0\colon a_i \notin \mathfrak{p}^2\}$.*

We conclude this section by noting that we can consolidate (2.1) above and (3.1) of [1] by making a slight change in the definition of ε'_i when $t' > 1$. Let $\overline{\varepsilon}'_i$ be defined as follows:

$$\overline{\varepsilon}'_i = \begin{cases} \varepsilon'_i & \text{if } t' = 1 \\ 0 + \mathfrak{P}^{ip^n+1} & \text{if } t' > 1 \end{cases}$$

In Theorem (3.1) of [1], we showed that, if $t = t' = 1$, then $M_L(K, K') = 2p^n - p^k$, where $p^n - p^k$ is the smallest integer i such that $\varepsilon_i \neq \varepsilon'_i$. This result, along with (2.2), gives us a method of determining $M_L(K, K')$ whenever $\min\{t_1(K/F), t_1(K'/F)\} = 1$.

(2.3) THEOREM. *If L/F is a normal, totally ramified extension of degree p^{2n} with normal subextensions K/F and K'/F satisfying $K \cap K' = F$, $KK' = L$, $[K : F] = [K' : F] = p^n$ and $t_1(K/F) = 1$, then*

$$M_L(K, K') = 2p^n - p^k, \qquad \text{where } p^n - p^k = \min\{i\colon \varepsilon_i \neq \overline{\varepsilon_i'}\}.$$

3. The general case

In this section, we will continue to assume that F is a finite extension of $\mathbb{Q}_p$ and that L/F is a normal, totally ramified extension of degree p^{2n} with normal subextensions K/F and K'/F satisfying $K \cap K' = F, KK' = L$ and $[K : F] = [K' : F] = p^n$. We will also continue to use the notation $t = \min\{t_1(K/F), t_1(K'/F)\}$ with the additional observation that, without loss of generality, we may assume that $t = t_1(K/F)$. We will also use the abbreviation $t' = t_1(K'/F)$ and let $\mathfrak{P}$ denote the maximal ideal of $\mathfrak{O}_L$. In (3.3), we will sharpen the previously computed (see (0.1)) lower bounds for $M_L(K, K')$. First we show that, under our hypotheses, p^n cannot divide $M_L(K, K')$, generalizing a result found in the proof of Theorem (3.1) of [3].

(3.1) PROPOSITION. *Let L/F be a normal, totally ramified extension of degree p^{2n} with normal subextensions K/F and K'/F satisfying $KK' = L$, $K \cap K' = F$ and $[K : F] = [K' : F] = p^n$. Then p^n does not divide $M_L(K, K')$.*

Proof. Define $M = M_L(K, K')$ and let π and π' be prime elements of $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ so that $v_L(\pi - \pi') = M$. Since L/K is totally ramified, we have $v_L(\pi) = p^n$. Assume, by way of contradiction, that $p^n | M$. Then $\pi^{M/p^n} \in \mathfrak{O}_K$ and $v_L(\pi^{M/p^n}) = M$. Since L/F is totally ramified, the residue fields $\mathfrak{O}_L/\mathfrak{P}$ and $\mathfrak{O}_F/\mathfrak{p}$ are equal, so there is a $\gamma \in \mathfrak{O}_F$ satisfying $\pi - \pi' \equiv \gamma\pi^{M/p^n} \pmod{\mathfrak{P}^{M+1}}$. Therefore, $\pi' = \pi + \pi' - \pi \equiv \pi - \gamma\pi^{M/p^n} \pmod{\mathfrak{P}^{M+1}}$. Defining $\rho = \pi - \gamma\pi^{M/p^n}$, we see that ρ is an element of $\mathfrak{O}_K$ satisfying $v_L(\rho - \pi') \geq M + 1 > p^n = v_L(\pi')$, so we must have $v_L(\rho) = p^n$. Thus, ρ is a prime element of $\mathfrak{O}_K$ satisfying $v_L(\rho - \pi') > M$, contradicting (1.1). Hence, p^n cannot divide M. □

With (3.1) in mind, if π and π' have been chosen so that $v_L(\pi - \pi') = M_L(K, K')$, then $v_L(\pi - \pi')$ cannot be a multiple of p^n. However, (1.2) gives us $v_L(\pi - \pi') = \min\{v_K(a_i - a_i') + i\colon 0 \leq i \leq p^n - 1\}$, where a_i (resp. a_i') is the coefficient of x^i in $\operatorname{irr}_F(\pi)$ (resp. $\operatorname{irr}_F(\pi')$). As $v_K(a_i - a_i') + i \equiv i \pmod{p^n}$, (3.1) shows that the minimum cannot occur when $i = 0$, and we have the following corollary:

(3.2) COROLLARY. *Along with the hypotheses of* (3.1), *suppose that π and π' are chosen so that $M_L(K, K') = v_L(\pi - \pi')$. If $\operatorname{irr}_F(\pi) = a_0 + a_1x + \cdots + x^{p^n}$ and $\operatorname{irr}_F(\pi') = a_0' + a_1'x + \cdots + x^{p^n}$, then $v_L(\pi - \pi') < v_K(a_0 - a_0')$.*

As a final note on (3.1) and (3.2), we insert a note of caution. Notice that if π and π' are chosen to be arbitrary prime elements of $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$, then we cannot guarantee that $v_L(\pi - \pi')$ is not a multiple of p^n. However, as was shown in (3.1) of [1], if $t_1(K/F) = t_1(K'/F) = 1$ and π and π' are chosen so that $v_L(\pi - \pi')$ is not a multiple of p^n, then $v_L(\pi - \pi') = M_L(K, K')$. Whether this result generalizes to other cases is not known to the author.

We now come to the main result of this section. We show that if L, K, K' and F are as above and $t = \min\{t_1(K/F), t_1(K'/F)\}$, then $M_L(K, K') \geq p^n(t+1) - p^{n-1}t$, sharpening the lower bound given in (0.1). To see that this is, indeed, a sharpening of the previous lower bound, recall that $t_1(L/F) \leq \min\{t_1(K/F), t_1(K'/F)\} = t$, so that

$$p^n(t+1) - p^{n-1}t \geq p^n(t_1(L/F)+1) - p^{n-1}t_1(L/F) \quad (= \text{ the lower bound of (0.1)}).$$

(3.3) THEOREM. *Let L/F be a normal, totally ramified extension of degree p^{2n} with normal subextensions K/F and K'/F satisfying $KK' = L$, $K \cap K' = F$ and $[K : F] = [K' : F] = p^n$. If $t = t_1(K/F) \leq t_1(K'/F)$, then $p^n(t+1) - p^{n-1}t \leq M_L(K, K')$, with equality only if t is not divisible by p.*

Proof. Choose π and π' so that $M_L(K, K') = v_L(\pi - \pi')$, and suppose $\mathrm{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$ and $\mathrm{irr}_F(\pi') = \sum_{i=0}^{p^n} a_i' x^i$. By an intermediate step in the proof of (1.6), if $0 < l < p^n$, then

$$v_K(a_l) \geq p^n(t_1(K/F) + 1) - p^{v_p(l)} t_1(K/F) - l$$

and

$$v_{K'}(a_l') \geq p^n(t_1(K'/F) + 1) - p^{v_p(l)} t_1(K'/F) - l.$$

Since $a_l' \in F$, we have $v_K(a_l') = v_{K'}(a_l')$. Hence,

$$v_K(a_l - a_l') + l \geq \min\{v_K(a_l), v_K(a_l')\} + l \geq (t+1)p^n - p^{v_p(l)}t - l + l = tp^n - tp^{v_p(l)}.$$

Moreover, since $0 \leq v_p(l) \leq n - 1$, we have shown that

$$v_K(a_l - a_l') + l \geq (t+1)p^n - tp^{n-1} \quad \text{for all } 0 < l < p^n.$$

Now, recall that, by (1.1) and (1.2), we have $M_L(K, K') = \min\{v_K(a_l - a_l') + l : 0 \leq l \leq p^n - 1\}$. However, (3.2) shows that this minimum cannot occur for $l = 0$. Therefore,

$$M_L(K, K') = v_L(\pi - \pi') = \min\{v_K(a_l - a_l') + l : l \neq 0\} \geq p^n(t+1) - p^{n-1}t.$$

In view of (3.1), we see that this lower bound can only be attained if t is not divisible by p, and the proof is complete. □

4. The case $t = t' < p$

With (3.3) in hand, we now make the additional assumption that $t_1(K/F) = t_1(K'/F) < p$, thus obtaining some partial results concerning the connection between our invariants and $M_L(K, K')$.

(4.1) PROPOSITION. *Let L/F be a normal, totally ramified extension of degree p^{2n} having normal subextensions K/F and K'/F satisfying $[K : F] = [K' : F] = p^n$, $K \cap K' = F$, $KK' = L$ and $t = t_1(K/F) = t_1(K'/F) < p$, and choose π and π' so that $v_L(\pi - \pi') = M_L(K, K')$. If $\operatorname{irr}_F(\pi) = \sum_{i=0}^{p^n} a_i x^i$ and $\operatorname{irr}_F(\pi') = \sum_{i=0}^{p^n} a'_i x^i$, then for $0 \leq k \leq n-1$,*

$$\varepsilon_{p^n - p^k} \neq \varepsilon'_{p^n - p^k} \iff v_K(a_{p^n - tp^k} - a'_{p^n - tp^k}) = tp^n.$$

Proof. Let $0 \leq k \leq n-1$ be given. By hypothesis (and (3.1)), we know $v_L(\pi - \pi') = M_L(K, K') > p^n$, so $(\pi - \pi') \in \mathfrak{P}^{p^n+1}$, which implies $\frac{\pi}{\pi'} \equiv 1 \pmod{\mathfrak{P}}$, and therefore $\left(\frac{\pi}{\pi'}\right)^{tp^k} \equiv 1 \pmod{\mathfrak{P}}$. In light of this, we will define $\alpha = (\pi/\pi')^{tp^k} - 1 \in \mathfrak{P}$. Since $t < p$, we know $v_p(p^n - tp^k) = k$, so $v_p\left(\binom{p^n - tp^k}{p^k}\right) = 0$. Therefore, (1.3) gives us

$$\begin{aligned}
\varepsilon_{p^n - p^k} = \varepsilon'_{p^n - p^k} &\iff \frac{a_{p^n - tp^k}}{\pi^{tp^k}} - \frac{a'_{p^n - tp^k}}{(\pi')^{tp^k}} \in \mathfrak{P}^{tp^{2n} - tp^{n+k} + 1} \\
&\iff a_{p^n - tp^k} - a'_{p^n - tp^k}(1 + \alpha) \in \mathfrak{P}^{tp^{2n}+1}.
\end{aligned}$$

As $a'_{p^n - tp^k} \in \mathfrak{P}^{tp^{2n}}$ and $\alpha \in \mathfrak{P}$, we have $\alpha a'_{p^n - tp^k} \in \mathfrak{P}^{tp^{2n}+1}$, and therefore,

$$\begin{aligned}
\varepsilon_{p^n - p^k} = \varepsilon'_{p^n - p^k} &\iff a_{p^n - tp^k} - a'_{p^n - tp^k} \in \mathfrak{P}^{tp^{2n}+1} \\
&\iff a_{p^n - tp^k} - a'_{p^n - tp^k} \in \mathfrak{P}_K^{tp^n+1} \\
&\iff v_K(a_{p^n - tp^k} - a'_{p^n - tp^k}) > tp^n.
\end{aligned}$$

By (1.4), $v_K(a_{p^n - tp^k}) \geq tp^n$ and $v_K(a'_{p^n - tp^k}) \geq tp^n$, so we have proven that

$$\begin{aligned}
\varepsilon_{p^n - p^k} \neq \varepsilon'_{p^n - p^k} &\iff v_K(a_{p^n - tp^k} - a'_{p^n - tp^k}) \leq tp^n \\
&\iff v_K(a_{p^n - tp^k} - a'_{p^n - tp^k}) = tp^n. \qquad \square
\end{aligned}$$

We conclude this section with two corollaries of (4.1). The first provides a method for computing an *upper* bound for $M_L(K, K')$ whenever $t = t' < p$. The second provides a necessary and sufficient condition for $M_L(K, K')$ to take the value of the lower bound given in (3.3).

(4.2) COROLLARY. *With the hypotheses of* (4.1), *if* $\varepsilon_{p^n-p^k} \neq \varepsilon'_{p^n-p^k}$, *then* $M_L(K, K') \leq p^n(t+1) - tp^k$.

Proof. If π and π' are chosen so that $M_L(K, K') = v_L(\pi - \pi')$, then (4.1) shows that

$$\varepsilon_{p^n-p^k} \neq \varepsilon'_{p^n-p^k} \iff v_K(a_{p^n-tp^k} - a'_{p^n-tp^k}) + p^n - tp^k = 2p^n - tp^k.$$

Therefore, if $\varepsilon_{p^n-p^k} \neq \varepsilon'_{p^n-p^k}$, then

$$p^n(t+1)-tp^k = v_K(a_{p^n-tp^k} - a'_{p^n-tp^k}) + p^n - tp^k \geq \min\{v_K(a_i - a'_i) + i\} = M_L(K, K'),$$

and our inequality is established. $\square$

(4.3) COROLLARY. *With the hypotheses of* (4.1),

$$\varepsilon_{p^n-p^{n-1}} \neq \varepsilon'_{p^n-p^{n-1}} \iff M_L(K, K') = p^n(t+1) - tp^{n-1}.$$

Proof. By (4.2), if $\varepsilon_{p^n-p^{n-1}} \neq \varepsilon'_{p^n-p^{n-1}}$, then $M_L(K, K') \leq p^n(t+1) - tp^{n-1}$. By (3.2), however, $M_L(K, K') \geq p^n(t+1) - tp^{n-1}$, and therefore, we must have $M_L(K, K') = p^n(t+1) - tp^{n-1}$. $\square$

5. Global consequences

The notion of corresponding residue systems was introduced by Butts and Mann in [2] under the hypothesis that F was a number field. We will suppose here that F is the quotient field of a Dedekind domain having characteristic 0 and finite residue fields for every prime ideal in $\mathfrak{O}_F$ (a number field, for example) and that L is a finite extension of F. Recall that if $\mathfrak{A}$ is an ideal of $\mathfrak{O}_L$, then $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ (or K and K') have corresponding residue systems mod $\mathfrak{A}$ if $\mathfrak{O}_K + \mathfrak{A} = \mathfrak{O}_{K'} + \mathfrak{A}$, and $\mathfrak{M}(K, K')$ is defined to be the unique minimal ambiguous ideal of $\mathfrak{O}_L$ so that $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ have corresponding residue systems mod $\mathfrak{M}(K, K')$.

Of course, in order to compute $\mathfrak{M}(K, K')$, we need only find its factorization as a product of prime ideals in $\mathfrak{O}_L$. To this end, for each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$ we compute $\max\{m \in \mathbb{Z}\colon \mathfrak{M}(K, K') \subseteq \mathfrak{P}^m\}$. As $\mathfrak{M}(K, K')$ is ambiguous, if $\mathfrak{P}^m$ divides $\mathfrak{M}(K, K')$, then so does $\overline{\mathfrak{P}}^m$, where $\overline{\mathfrak{P}}$ is any conjugate of $\mathfrak{P}$, so the highest power of $\mathfrak{P}$ dividing $\mathfrak{M}(K, K')$ is the same as the highest power of $\overline{\mathfrak{P}}$ dividing $\mathfrak{M}(K, K')$. Hence, we turn our attention to computing

$$\begin{aligned} M(\mathfrak{P}^\#\colon K, K') &= \max\left\{m \in \mathbb{Z}\colon \mathfrak{M}(K, K') \subseteq (\mathfrak{P}^\#)^m\right\} \\ &= \max\left\{m \in \mathbb{Z}\colon \mathfrak{O}_K + (\mathfrak{P}^\#)^m = \mathfrak{O}_{K'} + (\mathfrak{P}^\#)^m\right\} \end{aligned}$$

where $\mathfrak{P}^{\#}$ is the product of the distinct conjugates of $\mathfrak{P}$ in $\mathfrak{O}_L$. If we let $e = e(\mathfrak{P} : L/F)$ the (relative) ramification index of $\mathfrak{P}$ over F, then McCulloh and Stout showed in Theorems 1.7 and 1.8 of [3] that $M(\mathfrak{P}^{\#}\colon K, K') > 0$ if and only if $\mathfrak{P}$ is totally ramified in K/F and K'/F. In this case,

$$M(\mathfrak{P}^{\#}\colon K, K') \geq \min\left\{\frac{e}{[K:F]}, \frac{e}{[K':F]}\right\},$$

with equality unless $[K : F] = [K' : F] = p^r$ for some r where p is the characteristic of the residue field $\mathfrak{O}_L/\mathfrak{P}$. Hence, we will assume that $[K : F] = [K' : F] = p^r$ for some positive integer r. Under these hypotheses, Stout further showed, in Theorems 3.1 and 4.1 of [6] that

$$M(\mathfrak{P}^{\#}\colon K, K') \geq p^r(t_1(\mathfrak{P} : L/F) + 1) - p^{r-1}t_1(\mathfrak{P} : L/F),$$

where $t_1(\mathfrak{P} : L/F)$ is the first breakpoint in the Hilbert ramification sequence of the subgroups of $\mathrm{Gal}(L/F)$ with respect to $\mathfrak{P}$. We are now ready to prove the following theorem, a global version of (3.3), sharpening the above lower bound for $M(\mathfrak{P}^{\#}\colon K, K')$:

(5.1) THEOREM. *Let F be the quotient field of a Dedekind domain having characteristic* 0 *and assume that the residue field $\mathfrak{O}_F/\mathfrak{p}$ is finite for for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_F$.*[1] *Let L be an extension of F of degree p^{2n} which is totally ramified at the prime $\mathfrak{P}$ of $\mathfrak{O}_L$ (a divisor of the rational prime p). Suppose K and K' are normal extensions of F satisfying $K \cap K' = F$ and $L = KK'$ and let $t_1(\mathfrak{P}_K\colon K/F)$ (resp. $t_1(\mathfrak{P}_{K'}\colon K'/F)$) denote the first breakpoint in the ramification sequence of subgroups of* $\mathrm{Gal}(K/F)$ *(resp.* $\mathrm{Gal}(K'/F)$*) with respect to $\mathfrak{P}_K$ (resp. $\mathfrak{P}_{K'}$). Then*

$$M(\mathfrak{P}^{\#}\colon K, K') \geq p^n(t+1) - p^{n-1}t,$$

where $t = \min\{t_1(\mathfrak{P}_K\colon K/F), t_1(\mathfrak{P}_{K'}\colon K'/F)\}$.

Proof. As $\mathfrak{P}$ is totally ramified in L/F (and therefore in K/F and K'/F, as well), then $\mathfrak{P}^{\#} = \mathfrak{P}$ and we may assume that L is complete with respect to $\mathfrak{P}$, since $\mathrm{Gal}(L/F)$ and the lattice of intermediate fields (and therefore the sequence of ramification groups) are unchanged if L and F are replaced by their completions $\hat{L}$ and $\hat{F}$ (with respect to $\mathfrak{P}$). Furthermore, since a field is dense in its completion, $M(\mathfrak{P}^{\#}\colon K, K')$ is unchanged if K and K' are replaced by their completions $\hat{K}$ and $\hat{K}'$. That is, $M(\mathfrak{P}^{\#}\colon K, K') = M_{\hat{L}}\left(\hat{K}, \hat{K}'\right)$.

Since the characteristic of F is 0 and $\mathfrak{O}_F/\mathfrak{p}$ is finite (where $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$), $\mathfrak{O}_F$ is a free $\mathbb{Z}_p$ module of finite rank (see [5], p. 36), and therefore, we may regard F as a finite extension of $\mathbb{Q}_p$. But this is the case addressed in the earlier sections, so we may use (3.3), and the theorem is proved.

[1] In fact, we need not assume that *every* residue field of F is finite, only that $\mathfrak{O}_F/\mathfrak{p}$ is finite when $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$.

REFERENCES

1. S. R. Benson, *Canonical invariants for corresponding residue systems in p-adic fields*, J. Number Theory **36** (1990), 339–353.
2. H. S. Butts and H. B. Mann, *Corresponding residue systems in algebraic number fields*, Pacific J. Math. **6** (1956), 211–224.
3. L. R. McCulloh and W. T. Stout, Jr., *Corresponding residue systems in cyclic extensions of prime degree over algebraic number fields*, J. Number Theory **1** (1969), 312–325.
4. L. R. McCulloh, *Cyclic extensions of prime power degree and corresponding residue systems*, J. Number Theory **1** (1969), 459–466.
5. J. -P. Serre, *Local fields*, Springer-Verlag, New York, 1979.
6. W. T. Stout, Jr., *Corresponding residue systems in normal extensions*, J. Number Theory **5** (1973), 116–122.
7. R. L. Vogt, *A new invariant for corresponding residue systems*, doctoral dissertation, University of Illinois, 1974.

SANTA CLARA UNIVERSITY
SANTA CLARA, CALIFORNIA

UNIVERSITY OF NEW HAMPSHIRE
DURHAM, NEW HAMPSHIRE