GALOIS EXTENSIONS AND THE RAMIFICATION
SEQUENCE OF SOME WILDLY RAMIFIED
\(\pi\)-ADIC FIELDS

R. D. DAVIS AND E. F. WISHART

Abstract. In this paper the authors have found necessary and sufficient conditions for a \(p\)th degree Eisenstein extension of an arbitrary \(\pi\)-adic field to be normal. In addition we have found where the Galois automorphisms must appear in the ramification sequence of the extended ring.

In the study of the factors of the ramification sequence of a valuation ring it is of interest to know when extensions of the quotient field are normal and where in the ramification sequence the Galois automorphisms appear. This work answers these questions for a \(p\)th degree Eisenstein extension of an arbitrary \(\pi\)-adic field \(K_q\), and is an extension of results that appear in the authors’ dissertations [1], [5]. A special case has been used by Heerema in [3, Lemma 8] to analyze the ramification sequence when the ramification index is \(p\).

Let \(K\) be an unramified \(p\)-adic field [4, p. 226, Definition 2] and consider \(K_{pq}/K_q\) and \(K_q/K\) totally ramified extensions of degrees \(p\) and \(q\) respectively, where \(p\) is an odd prime and \(q\) is arbitrary. Let \(\pi\) and \(\tau\) denote prime elements of \(K_{pq}\) and \(K_q\) respectively, and by \(V(a)\) we denote the normalized exponential valuation of an element \(a \in K_{pq}\) so that \(V(\pi) = 1\), \(V(\tau) = p\), and \(V(p) = pq\). Recall that \(\pi\) is a root of an Eisenstein polynomial

\[
f(x) = x^p + \tau \sum_{i=0}^{p-1} b_ix^i
\]

over \(K_q\). We use \(M(r)\) to denote the \(r\)th power of the maximal ideal \(M\) of the valuation ring \(R_{pq}\) of \(K_{pq}\) and \(h = R_{pq}/M\) denotes the common residue field of \(K\), \(K_q\), and \(K_{pq}\). Also \(t^*\) denotes the residue of \(t\) modulo \(p-1\), \(0 \leq t^* < p-1\), and \([\ ]\) denotes the greatest integer function. Finally, let

\[
G_1 \supseteq H_1 \supseteq G_2 \supseteq H_2 \supseteq \cdots
\]

be the ramification sequence of \(R_{pq}\), where

Received by the editors September 28, 1970.


Key words and phrases. Eisenstein extension, ramification sequence, wildly ramified extension, normal extension, Galois automorphism.
G_i = \{ \alpha \in G \mid \alpha(a) - a \in M(i) \text{ for all } a \in R_{pq} \},

H_i = \{ \alpha \in G_i \mid \alpha(a) - a \in M(i + 1) \text{ for all } a \in M \},

and G is the group of automorphisms of \( R_{pq} \).

**Theorem.** Suppose \( K_{pq}, K_q \) and \( K \) are as above; let

\[ t_p = \min\{ V(b_i) \mid i = 1, 2, \ldots, p-1 \} \]

and \( j \) be the least positive integer \( i \) such that \( V(b_i) = t_p \). If \( b_1 = \cdots = b_{p-1} = 0 \), set \( t = +\infty \) and \( j = 1 \). Then necessary and sufficient conditions for \( K_{pq}/K_q \) to be normal are:

- **Case 1.** \( t < q \).
  - (a) \( j = p - 1 - t_p^* \)
  - (b) the residue in \( h \) of \( -j b_i/(\tau(t-b_0)^{t+1}) \) has a \((p-1)\)th root.
- **Case 2.** \( t \geq q \).
  - (c) \( q = s(p - 1), s \) an arbitrary, positive integer and
  - (d) the residue in \( h \) of \(-\tau^q/p\) has a \((p-1)\)th root.

Moreover, the nontrivial Galois automorphisms of \( K_{pq}/K_q \) are in \( G_n \setminus H_n \), where \( n = \{ t + 2 + \lfloor t/(p-1) \rfloor \text{ in Case 1, } sp+1 \text{ in Case 2} \} \).

For \( f(x) = x^p + rb_0 \) clearly \( K_{pq}/K_q \) is normal if and only if \( K_q \) contains the \( p \)th roots of 1. Let \( M' \) be the maximal ideal of the valuation ring of \( K_q \). Then Case 2 yields:

**Corollary [2, V, p. 215].** \( K_q \) contains the \( p \)th roots of 1 if and only if \((p-1)|q \) and \( x^p-1 = -\tau^q/p \text{ mod } M' \) has a solution in \( K_q \).

**Proof (Necessity).** The proof is based on the fact that if a sum is zero, then it must have at least two summands with minimal value. For completeness we include the well-known

**Lemma.** Suppose \( K_{pq}/K_q \) is a normal extension. Every nontrivial \( \alpha \in G(K_{pq}/K_q) \) is such that \( \alpha(\pi) = \pi + \pi^n z \) where \( n \geq 2 \) and \( z \) is a unit.

**Proof.** Since \( f(\alpha(\pi)) = 0, V(\alpha(\pi)) = V(\pi) = 1 \), i.e., \( \alpha(\pi) = r \pi \), where \( r \) is a unit. But \( f(r \pi) = 0 \) and \( \pi^p = -rb_0 \text{ mod } M(p+1) \) imply \((r \pi)^p - \pi^p = (r^p - 1) \pi^p \in M(p+1) \). Hence the residue of \( r \) is a \( p \)th root of unity in \( h \) and since 1 is the only such, \( r = 1 + \pi^n z, \) with \( n \geq 2 \) and \( z \) is a unit.

From \( f(\pi) = f(\pi + \pi^n z) = 0 \) we obtain

\[
\sum_{k=1}^{p} \binom{p}{k} \pi^{p+k(n-1)z^k} + \tau \sum_{k=1}^{p-1} b_k \sum_{i=1}^{k} \binom{k}{i} \pi^{k+i(n-1)z^i} = 0.
\]

1 The authors wish to thank the referee for pointing out this corollary.
Since \( n \geq 2 \), the terms in the sum on the left side of (2) increase in value with increasing \( k \) except when \( k = p \). Also, the terms in the double sum on the right side of (2) increase in value with both increasing \( i \) and \( k \) except when \( k = j \). It follows from these two observations that the following three terms have values less than every other term:

\[
\begin{align*}
(3) & \quad p^n \pi^{p+n-1}z, \\
(4) & \quad \pi^n \pi^p, \\
(5) & \quad \tau j^p \pi^{p+n-1}z.
\end{align*}
\]

Their respective values are \( q_p + p + n - 1, np, \) and \( p + tp + j + n - 1 \).

Case 1. \( t < q \). Since \( 0 < j < p \), we have \( p + tp + j + n - 1 < q_p + p + n - 1 \). Hence, \( np = p + tp + j + n - 1 \) which implies

\[
n = 1 + (tp + j)/(p - 1).
\]

But \( n \) is a positive integer \( \geq 2 \), so that

\[
tp + j = m(p - 1)
\]

for some positive integer \( m \). Since \( t = (p - 1) \lfloor t/(p - 1) \rfloor + t^* \), (7) implies

\[
(8) \quad j = (p - 1) \left( m - t - \left\lfloor \frac{t}{p - 1} \right\rfloor \right) - t^*.
\]

Since \( 0 < j < p \), it follows from (8) that \( m - t - \left\lfloor t/(p - 1) \right\rfloor = 1 \) and hence \( j = p - 1 - t^* \), i.e., condition (a). Substitution of (8) into (6) yields the conclusion \( n = t + 2 + \left\lfloor t/(p - 1) \right\rfloor \). From (1) we have \( \pi^p \equiv -b_0 \mod M(p + 1) \) which implies that

\[
\pi^n \pi^p \equiv \pi^{p+n-p-1}(b_0)^{t+1} \equiv \pi^{p+n-1}(b_0)^{t+1} \mod M(np + 1).
\]

Since the sum of (4) and (5) must have value greater than \( np \), (4) added to (5) becomes

\[
\pi^{p+n-1}(b_0)^{t+1} + \tau j^p \pi^{p+n-1}z \equiv 0 \mod M(np + 1)
\]

or

\[
(9) \quad \pi^{p-1} + \frac{j^*}{\tau(-b_0)^{t+1}} \equiv 0 \mod M.
\]

The residue of (9) in \( h \) yields condition (b) of the theorem.

Case 2. \( t \geq q \). In this case \( q_p + p + n - 1 < p + tp + j + n - 1 \). Thus equating the values of (3) and (4) yields

\[
(10) \quad q = (p - 1)(n - 1)/p.
\]
It follows that $p \mid (n-1)$, implying that $n-1 = sp$ for some positive integer $s$. This is condition (c) of the theorem.

Since the value of the sum of (3) and (4) must be greater than $np$, we have

$$p \pi^{p+n-1}z + \pi^{np}r = 0 \quad \text{mod } M(np + 1)$$

which, through the use of (10) and the fact that $\pi^{p} = -rb_0 \mod M(p+1)$, reduces to

$$(-b_0)^{s-1} + (\pi/r^s) = 0 \quad \text{mod } M.$$

Since $g$ is a multiple of $p-1$, this implies condition (d).

**Sufficiency.** We prove that $f(x)$, the minimal polynomial of $\pi$, splits in $K_{pq}$. Since $K_{pq}/K_q$ is of degree $p$, this is equivalent to showing the existence of a root of $f(x)$ in $K_{pq}$ that is different from $\pi$. From the lemma we know that if such a root exists it is of the form $\pi + \pi^n z$, $n \geq 2$, $z$ a unit. Thus it suffices to show the existence of a unit $z$ for which $\pi + \pi^n z$ is a root of (1). We do this by successive approximation.

**Case 1.** $t < q$. Let $z_0$ be a representative in $K_{pq}$ of a $(p-1)$th root of the residue of $-jb_i/(\tau t(-b_0)^{t+1})$ and $n = t + 2 + \lfloor t/(p-1) \rfloor$. Substitute $\pi + \pi^n z_0$ into (1). As in the proof of the necessity, there are two terms with minimal value $pn$, i.e., $\pi^{p}z_0^p$ and $\tau b_i j \pi^{t+n-1}z_0$. Their sum (mod $M(np + m)$) after some simplification reduces to

$$z_0 \pi^{t+n-1} (-b_0)^{t+1} + \tau b_i j,$$

which from the choice of $z_0$, reduces to zero mod $M(np + m)$. With this as the first step, we proceed by induction. Suppose $z_0, z_1, \ldots, z_{m-1}$ have been chosen so that

$$f(\pi + \pi^n z_0 + \pi^{n+1} z_1 + \cdots + \pi^{n+m-1} z_{m-1}) \in M(np + m).$$

Let $\lambda = w + \pi^{n+m} z_m$, where $w = \pi + \pi^n z_0 + \cdots + \pi^{n+m-1} z_{m-1}$. Then

$$f(\lambda) = f(w) + \sum_{k=1}^{p} \binom{p}{k} \pi^{p-k} \frac{k(n+m) k}{z_m} + \tau \sum_{k=1}^{p-1} b_k \sum_{i=1}^{k} \binom{k}{i} \pi^{i(n+m)-i} z_m.$$

Since $m > 1$, every term in the above is in $M(np + m + 1)$ except for $f(w)$ and the term $\tau b_i j \pi^{t+n+m} z_m$, whose value is less than or equal to that of $f(w)$. Hence we can choose $z_m$ so that $f(w) + \tau b_i j \pi^{t+n+m} z_m \in M(np + m + 1)$. Thus by induction, for each integer $m$ we can choose $z_m$ so that

$$f(\pi + \pi^n z_0 + \pi^{n+1} z_1 + \cdots + \pi^{n+m} z_m) \in M(np + m + 1).$$

Let $z = \sum_{i=0}^{m} \pi^{i} z_i$, $f(\pi + \pi^n z) = 0$ so that we obtain our root for Case 1.
Case 2. \( t \geq q \). In this case we let \( z_0 \) be a representative of a \((p - 1)\)th root of \(-\left(\frac{p}{r^*}\right)\) and \( n = sp + 1 \), where \( q = s(p - 1) \). The rest of the details of this case are similar to those of Case 1 and will be omitted here, except to mention that terms (3) and (4) are considered rather than (4) and (5).

A natural question to ask is: Given an extension \( K_{pq}/K_q \) can Cases 1 and 2 both occur for the same extension for different choices of prime elements \( \pi \) and \( \tau \)? That this cannot occur can be easily seen from the following argument.

Suppose for different choices of \( \pi \) and \( \tau \) both Cases 1 and 2 could occur. Then, since the position of the nontrivial Galois automorphisms in the ramification sequence is independent of the choice of \( \pi \) and \( \tau \), we would have

\[(12) \quad t + 2 + \left\lceil \frac{t}{(p - 1)} \right\rceil = sp + 1.\]

Substituting \( t = (p - 1)\left\lceil \frac{t}{(p - 1)} \right\rceil + t^* \) into (12) yields \( t^* = p(s - \left\lceil \frac{t}{(p - 1)} \right\rceil) - 1 \) which is contrary to \( 0 \leq t^* < p - 1 \).

References


University of Nevada, Reno, Nevada 89507