J.C. Parnami, M.K. Agrawal, A.R. Rajwade

ON THE FOURTH POWER STUFE OF \( p \)-ADIC COMPLETIONS
OF ALGEBRAIC NUMBER FIELDS

§ 1. Introduction and notation.

The problem of representation of numbers of a field (ring) by \( m \)-th powers of elements of the field (ring) has been extensively discussed by various authors such as Siegel [9], Birch [1] and [2], Ramanujam [8], Tornheim [10], Niven [5] and others. Of special interest is the minimal such representation of \(-1\) (when possible) and leads, in the case \( m = 2 \), to the notion of the stufe (length) of the field (ring) in question. This has been investigated by many and recently Pfister [7] has proved some very striking results about it.

Following Pfister, we define the fourth power stufe \( s_4(K) \) of a field \( K \) to be the least value of the positive integer \( s \) for which the equation

\[
-1 = a_1^4 + ... + a_s^4
\]

is solvable with \( a_j \in K \). If (*) is not solvable in \( K \), we put \( s_4(K) = \infty \).

In contrast to \( s_4(K) \), the Pfister stufe of \( K \) will be denoted by \( s_2(K) \). When \( K \) is a totally complex algebraic number field, it is easy to prove, using the Hasse principle, that \( s_2(K) \leq 4 \) and in a recent paper of ours [6], we have shown that \( s_4(K) \leq 16 \). For a given algebraic number field \( K \) the exact determination of \( s_4(K) \) is difficult; indeed even \( s_2(K) \) is known only when \( K \) is an imaginary quadratic field or a cyclotomic field, apart from perhaps some stray isolated examples. In [6], we showed that \( s_4(Q(\sqrt{-m})) = 15 \) if \( m = 7 \mod 8 \) and worked out some inequalities for \( s_4(K) \) for other imaginary quadratic fields \( K \). With the idea of determining \( s_4(K) \) exactly for at
least some class of fields, we discuss, in this paper, the determination of 
$s_4(K_p)$, where $K_p$ is the $p$-adic completion of $K$ at $p$. This leads to 
certain non-trivial lower bounds for $s_4(K)$ and in some cases determines 
$s_4(K)$ exactly (see §6).

We use the following notation:

$k$ as algebraic number field.

$\mathcal{O}$ the ring of integers of $k$.

$p$ a finite prime ideal of $k$.

$k_p$ the $p$-adic completion of $k$ at $p$.

$\mathcal{O}_p$ the ring of integers of $k_p$.

$e = e_p$ the ramification index of $p$.

$f = f_p$ the residue class degree of $p$.

$s = s_4(k_p)$ the fourth power stufe of $k_p$.

We note to begin with that

(i) $s_4(k_p) \leq s_4(k)$,

(ii) for $p \nmid 2$, by Hensel’s lemma, $s = s_4(\mathcal{O}/p) = s_4(\mathbb{F}_p^f)$, where $p$ is 
the unique rational prime lying below $p$, and this has been determined 
exactly in [6], viz

$$s_4(\mathbb{F}_p^f) = \begin{cases} 
1 & \text{if } p^\alpha \equiv 1 \pmod{8} \text{ or if } p = 2, \\
3 & \text{if } p^\alpha = 29, \\
4 & \text{if } p^\alpha = 5, \\
2 & \text{otherwise.} 
\end{cases}$$

So in what follows, we shall assume that $p \mid 2$. In this paper we shall 
prove that $s \leq 15$ and equality holds if and only if $e = f = 1$. We also prove 
that $s \leq 11$ if $k$ is a cyclotomic field and we determine $s$ exactly when $k$ 
is either a quadratic field or a cubic field (see theorems 2 and 3). All the 
results have been compiled in a table at the end of § 5.

In § 3 and 4 we shall frequently use the following elementary result: if 
$p$ is a prime ideal with norm 2 in an algebraic number field $k$ and $\alpha, \beta \in \mathcal{O}$ 
are such that $p^n$ exactly divides both $\alpha$ and $\beta$ then $p^{n+1}$ divides $\alpha + \beta$.

This result follows immediately by observing that $p^n/p^{n+1} \cong \mathcal{O}/p \cong \mathbb{F}_2$ 
(the field of 2 elements).
§ 2. An analogue of Hensel's lemma.

By Hensel's lemma it follows immediately that $s$ is the least positive integer such that

$$x_1^4 + ... + x_{s+1}^4 \equiv 0 \pmod{p^{4e+1}}$$

has a solution in $\mathfrak{a}$ in which at least one $x_j$ is not divisible by $p$. We shall show that the exponent $4e + 1$ of $p$ can be replaced by $3e + 1$.

Suppose $x_1^4 + ... + x_{s+1}^4 \equiv 0 \pmod{p^\beta}$ has a solution in $\mathfrak{a}$ with $p | x_1$ and $\beta \geq 3e + 1$. Let $x_1^4 + ... + x_{s+1}^4 = u$, $p^\beta | u$. Let $\pi \in p^{-2e} - p^{-2e+1}$ and $z \in \mathfrak{a}$. Then

$$(x_1 + \pi z)^4 + x_2^4 + ... + x_{s+1}^4 = u + 4\pi x_1^3 + 6\pi^2 x_2^2 + 4\pi^3 x_3^3 + \pi^4 x_4^4$$

$$\equiv u + 4\pi x_1^3 \pmod{p^{\beta+1}}$$

(since $2\beta - 4e + e \geq 3e + 1$, $2e + 3\beta - 6e \geq 3e + 1$, $4\beta - 3e \geq 3e + 1$).

We have $(4\pi x_1^3, p^{\beta+1}) = p^\beta | u$. Hence there exists a $z$ such that $4\pi x_1^3 z \equiv -u \pmod{p^{\beta+1}}$ and for this choice of $z$, $(x_1 + \pi z)^4 + x_2^4 + ... + x_{s+1}^4 \equiv 0 \pmod{p^{\beta+1}}$ and $p | (x_1 + \pi z)$. Now proceeding as in the proof of Hensel's lemma, we obtain a solution of $x_1^4 + ... + x_{s+1}^4 = 0$, with $x_1 \in \mathfrak{a}$ and the remaining $x_j \in \mathfrak{a}$.

§ 3. We prove the following

**THEOREM 1.** $s \leq 15$ and equality holds if and only if $e = f = 1$.

**Proof.** $\sum_{j=1}^{16} x_j^4 \equiv 0 \pmod{p^{3e+1}}$, on taking each $x_j = 1$ and so by § 2, $s \leq 15$.

When $e = f = 1$, $0, 1, 2, ..., 15$ is a complete residue system modulo $p^4$. Hence for any $p$-adic integer $\alpha$, $\alpha^4 \equiv 0$ or $1 \pmod{p^4}$. It follows that $s \geq 15$ (for a rational integer $n \equiv 0 \pmod{p^4}$ if and only if $n \equiv 0 \pmod{16}$).

Let now $ef > 1$ and we have to show that $s < 15$.

**Case 1:** $f > 1$. Take an $\alpha \in \mathfrak{a}$, $\alpha \not\equiv 0, 1 \pmod{p}$ (such an $\alpha$ exists since $N(p) = 2^f > 2$). Then $\alpha^2 + \alpha \not\equiv 0 \pmod{p}$. Find $y \in \mathfrak{a}$ such that $y^4 (\alpha^2 + \alpha) \equiv 1(p)$ (such a $y$ exists since $\mathfrak{a}/p$ is a field with $2^f$ elements and so every element of $\mathfrak{a}/p$ is a fourth power). Put $t = y(1 + 2\alpha)$, then $t^4 \equiv y^4 (1 + 8(\alpha^2 + \alpha)) \pmod{16} \equiv y^4 + 8 \pmod{8p}$, and so $3 + 3y^4 + t^4 + 4(1 + p)^4 (1 + 2y)^4 \equiv 8 + t^4 + 16y + 32y^2 + 16y^3 + 31y^4 + 32y^6 + 16y^8 \equiv 0 \pmod{8p}$ and $(mod p^{3e+1})$. It follows that $s \leq 11$.
Case 2: \( e > 1, \ e \) even. Let \( (2) = p_1^{e_1} \cdots p_r^{e_r} \) be the decomposition of 2 into prime ideals in \( \mathfrak{o} \). Take \( \alpha \equiv 0 \pmod{p_1^{e_1} \cdots p_r^{e_r}} \).

Then \( \alpha^4 = 4\beta \) where \( p \mid \beta \ (\beta \in \mathfrak{o}) \). Find \( \gamma \) such that \( \gamma^4 \beta \equiv 1 \pmod{p} \). Then \( (\alpha \gamma)^4 \equiv 4 \pmod{4p} \) and so \( 2 + (2\alpha \gamma)^4 \equiv 0 \pmod{8p} \equiv 0 \pmod{p^{3e+1}} \).

It follows that \( s \leq 9 \).

Case 3: \( e > 1, \ e \) odd. We need only look at the case when \( f = 1 \) since the case \( f > 1 \) has already been dealt with.

Choose \( \pi \in \mathfrak{p} - \mathfrak{p}^2 \) and let \( d = (e-1)/2 \). Then \( 4d = 2e - 2 \geq e + 1 \), and \( 8 + 3\pi^{4d} + \pi^{4(d+1)} + (\pi^d(1 + \pi))^4 = 8 + 4\pi^{4d} + 4\pi^{4d+1} + 6\pi^{4d+2} + 4\pi^{4d+3} + 2\pi^{4(d+1)} \equiv 8 + 2\pi^{4d+2} \pmod{p^{3e+1}} \equiv 8 \pmod{p^{3e+1}} \) since \( p^{3e} \parallel 8 \) and \( 2\pi^{4d} \) and \( p^{3e}/p^{3e+1} \equiv \mathfrak{o}/p \) (a field of 2 elements, since \( f = 1 \)). It follows that \( s \leq 12 \).

Remark. When \( k = Q(e^{2\pi i/m}) \ (m \geq 2) \) is a cyclotomic field, we have \( s \leq 11 \).

Proof. If \( 8 \mid m \) then \( s = 1 \) (since \( (e^{2\pi i/8})^4 = -1 \) in \( k \) and so in \( k\mathfrak{p} \)). If \( 4 \mid m \) then \( Q(i) \subset k \) and since \( -1 = 4 \left( \frac{1+i}{2} \right)^4 \) so \( s \leq 4 \). If \( m \) is odd then \( e = 1 \) and \( f > 1 \), hence \( s \leq 11 \).

§ 4. We consider the case \( ef = 2 \) and deduce the following

THEOREM 2. Let \( k = Q(\sqrt{m}) \), \( m \) square-free \( \neq 1 \), be a quadratic extension of \( Q \), real or imaginary; then (cf. theorems 2, 3, 4 of \( [1] \))

\[
s_4(k\mathfrak{p}) = \begin{cases} 
2 & \text{if } m \equiv 5 \pmod{8} \\
4 & \text{if } m \equiv 3 \pmod{4} \\
6 & \text{if } m \equiv 2 \pmod{4} \\
15 & \text{if } m \equiv 1 \pmod{8}
\end{cases}
\]

for every prime ideal \( \mathfrak{p} \) in \( k \), dividing 2.

LEMMA 1. (i) If \( f \) is even then \( s \leq 2 \).

(ii) If \( s = 1 \) then \( 4 \mid e \).

Proof. Find an integer \( \alpha \in \mathfrak{o} \) such that \( \alpha^3 \equiv 1 \pmod{p} \) and \( \alpha \equiv 1 \pmod{p} \) (this is possible since \( 3 \mid 2f - 1 \) and \( \mathfrak{o}/p \) is a field with \( 2f \) elements). Next
find a $\beta$ such that $\beta^3 \equiv 1 \pmod{p^{3e+1}}$, $\beta \equiv \alpha \pmod{p}$ (by Hensel’s lemma). Then $1 + \beta^3 + \beta^8 \equiv 1 + \beta + \beta^2 = \frac{1 - \beta^3}{1 - \beta} \equiv 0 \pmod{p^{3e+1}}$. It follows that $s \leq 2$.

Now suppose $s = 1$. Then $x^4 + y^4 \equiv 0 \pmod{p^{3e+1}}$ is solvable in $\mathfrak{d}$ with $p \mid x$. Find $z \in \mathfrak{d}$ such that $xz \equiv 1 \pmod{p^{3e+1}}$; then $1 + (yz)^4 \equiv 0 \pmod{p^{3e+1}}$. Thus for $t = yz$ we have

$$(t - 1)(t + 1)(t^2 + 1) + 2 \equiv 0 \pmod{p^{3e+1}}.$$  

This gives $p^e \mid t^4 - 1$ and so $p \mid t - 1$. Let $p^e \mid t - 1$, then $p^e \mid t + 1$, $p \mid t^2 + 1$ and therefore $2\alpha + 1 \leq e$ and hence $p^{2\alpha} \mid t^2 - 1 + 2$. Consequently $p^{4\alpha} \mid t^4 - 1$ or $4\alpha = e$.

**COROLLARY.** If $e = 1$, $f = 2$ then $s = 2$.

**LEMMA 2.** Let $e = 2$, $f = 1$. Let $\pi$ be any element of $\mathfrak{d}$ such that $p \mid \pi$ (i.e. $\pi \in p - p^2$). Then $s = \begin{cases} 6 & \text{if } \pi^2 \equiv 2 \pmod{p^4} \\ 4 & \text{otherwise.} \end{cases}$

(Note that if the condition $\pi^2 \equiv 2(p^4)$ holds for any $\pi \in p - p^2$, then it holds for all $\pi \in p - p^2$).

**Proof.** First let $\pi^2 \equiv 2 \pmod{p^4}$ hold for each $\pi \in p - p^2$. Then $\pi^2 = 2 + \gamma$ ($\gamma \in p^4$) and $\pi^4 = 4 + \gamma^2 + 4\gamma \equiv 4 \pmod{p^8}$ and $4 \cdot 1^4 + 3 \cdot \pi^4 \equiv 0 \pmod{p^8} \equiv 0 \pmod{p^{3e+1}}$. It follows that $s \leq 2$.

Now suppose $x_1^4 + \ldots + x_{4+1}^4 \equiv 0 \pmod{p^7}$ ............................................... $(\ast)$ where $p \mid x_1$. We may suppose that $p^2 \mid x_i$ for any $i$ (otherwise $p^6 \mid x_i^4$ and the $s$ in $(\ast)$ can be reduced). Now observe that $x \equiv y (p^2)$ implies $x^4 \equiv y^4 (p^7)$ (for $x^4 - y^4 = (x-y)(x+y)(x^2+y^2) \equiv 0 (mod p^6)$, since each term $\equiv 0 (mod p^2)$. If $p^7 \mid x^4 - y^4$ then $p^2 \mid x - y$, $x + y$, $x^2 + y^2$, which gives $p \mid y$ and then $p^4 \mid x^2 + y^2$ which is a contradiction). So without loss of generality we may suppose that $x_i = 1$, $1 + \pi$ (since $0, 1, \pi, 1 + \pi$ is a complete residue system modulo $p^2$). We have $(1 + \pi)^4 = 1 + 4\pi + 6\pi^2 + 4\pi^3 + \pi^4 \equiv 5 + 4\pi + 6\pi^2$ (mod $p^3$) (since $\pi^4 \equiv 4 (mod p^8) \equiv 1 (mod p^4)$, and $\pi^4 \equiv 0$ (mod $p^4$)). So the number of $i$ in $(\ast)$ with $p \mid x_i$ must be a multiple of 4 and hence equals 4. Without loss of generality suppose $p \not\mid x_1$. We may suppose $x_1^4 = \pi^4 \equiv 4 \pmod{p^7}$ if $i > 4$. Then $x_i^4 = 1$ or $5 + 4\pi + 6\pi^2$ (mod $p^7$) ($1 \leq i \leq 4$) and so $x_1^4 + \ldots + x_4^4 \equiv 4$ or $8 + 4\pi + 6\pi^2$ (mod $p^7$) ($\equiv 0$ (mod $p^7$)) since $2(5 + 4\pi + 6\pi^2) \equiv 10 + 12\pi^2$ (mod $p^7$) $\equiv 10 + 24$ (mod $p^7$) (because $\pi^2 \equiv 2 (mod p^3) \equiv 2 (mod p^7)$, and hence $x_1^4 + \ldots + x_4^4 \equiv 8$ or $12 + 4\pi +$
+ 6\pi^2 \pmod{p^7} \neq 0 \pmod{p^7} and so finally \( x_1^4 + \ldots + x_k^4 \equiv 12 \pmod{p^7} \). It follows that \( s > 5 \) and so \( s = 6 \).

Now suppose that \( \pi^2 \neq 2 \pmod{p^4} \) for any \( \pi \in p^2 \). Then \( p^3 | \pi^2 - 2 \) (since \( f = 1 \)) and so we have \( 4 + \pi^4 = (\pi^2 + 2)^2 - 4\pi^2 \equiv 0 \pmod{p^7} \). It follows that \( s \leq 4 \). Finally let \( x_1^4 + \ldots + x_{s+1}^4 \equiv 0 \pmod{p^7} \) with \( p | x_i \). As above we may suppose that \( x_i = 1, \pi, 1+\pi \) for all \( i \). Now \( (1+\pi)^4 = 1 + 4\pi + 6\pi^2 + 4\pi^3 + \pi^4 \equiv 1 \pmod{p^5} \). It follows that the number of \( i \) with \( p | x_i \) is a multiple of 4 and hence equals 4. Again without loss of generality \( p | x_1 x_2 x_3 x_4 \). Then \( x_1^4 + \ldots + x_4^4 \equiv 4 \pmod{p^5} \).

\( \neq 0 \pmod{p^7} \). It follows that \( s > 3 \) and hence equals 4.

**Proof of theorem 2.** First let \( m \equiv 1 \pmod{8} \), then \( (2) = pp' \) and so \( e = f = 1 \) and by theorem 1, \( s = 15 \).

Next let \( m \equiv 5 \pmod{8} \), then \( (2) = p \) and so \( e = 1, f = 2 \) and by the corollary to lemma 1, \( s = 6 \) (note that \( \pi \in p^2 \)).

Again let \( m \equiv 2 \pmod{4} \), then \( (2) = p^2 \) and so \( e = 2, f = 1 \). We take \( \pi = \sqrt{m} \) so that \( \pi^2 = m \equiv 2 \pmod{p^4} \) and so by lemma 2, \( s = 6 \) (note that \( \pi \in p^2 \)).

Finally let \( m \equiv 3 \pmod{4} \), then \( (2) = p^2 \) again and so \( e = 2, f = 1 \). We take \( \pi = 1 + \sqrt{m} \), so that \( \pi^2 = m + 1 + 2\sqrt{m} \equiv 2\sqrt{m} \pmod{p^4} \), (since \( 2 | 1 - \sqrt{m} \)) (note that this \( \pi \in p^2 \)) and so by lemma 2, \( s = 4 \).

§ 5. We consider the case \( ef = 3 \) and deduce the following

**Theorem 3.** Let \( k = \mathbb{Q}(\theta) \) be a cubic extension of \( \mathbb{Q} \) where \( \theta \) is a zero of the integral polynomial

\[ X^3 + CX + D \]

where without loss of generality for any prime \( p \), either \( p^3 | C \) or \( p^3 | D \). Write \( \Delta = 2^6 | C_1, D = 2^6 | D_1 \) and \( \Delta = -27D^2 - 4C^3 \) (the discriminant of the cubic) = \( 2^6 \Delta' \), where \( C_1, D_1, \Delta' \) are odd integers. Then

(i) If \( D \) is odd and \( C \) is even, then \( (2) \sim p_1 p_2 \), \( \deg p_1 = 1, \deg p_2 = 2 \) and \( s_4(k_{p_1}) = 15 \) and \( s_4(k_{p_2}) = 2 \).

(ii) If \( C, D \) are both odd, then \( (2) \sim p \) and \( s = s_4(k_p) = 5 \).

(iii) If \( C \) is odd, \( D \) is even, \( \nu \) is even and \( \Delta' \equiv 1 \pmod{8} \), then \( (2) \sim p_1 p_2 p_3 \) and \( s = s_4(k_{p_i}) = 15 \) \((i = 1, 2, 3)\).
(iv) If \( C \) is odd, \( D \) is even, \( v \) is even and \( \Delta' \equiv 5 \pmod{8} \), then \((2) \sim p_1p_2, \deg p_1 = 1, \deg p_2 = 2 \) and \( s_4(kp_1) = 15, s_4(kp_2) = 2 \).

(v) If \( C \) is odd, \( D \) is even, \( v \) is even and \( \Delta' \equiv 3 \pmod{4} \), then \((2) \sim p_1p_2^2 \) and \( s_4(kp_1) = 15, s_4(kp_2) = 4 \).

(vi) If \( C \) is odd, \( D \) is even and \( v \) is odd, then \((2) \sim p_1p_2 \) and \( s_4(kp_1) = 15, s_4(kp_2) = 6 \).

(vii) If \( C, D \) are both even and \( \lambda \geq \mu > 0 \), then \((2) \sim p_3 \) and \( s_4(kp) = 9 \).

(viii) If \( C, D \) are both even and \( 0 < \lambda < \mu \) (i.e. \( \lambda = 1, \mu > 1 \)), then \((2) \sim p_1p_2 \) and \( s_4(kp_1) = 15, s_4(kp_2) = \begin{cases} 4 & \text{if } \mu = 2, \\ 6 & \text{if } \mu > 2. \end{cases} \)

**Lemma 3.** Let \( e = 3, f = 1 \), then \( s = 9 \).

**Proof.** Let \( \pi \) be any element of \( \mathfrak{p} - \mathfrak{p}^2 \). Then \( \pi^3 \equiv 2 \pmod{p^4} \). We have \( 2(1 + \pi)^4 + 6 + \pi^4 + (\pi(1 + \pi))^4 \equiv 8 + 4\pi^2 + 2\pi^6 + \pi^8 \pmod{p^{10}} \equiv 4\pi^2 + + \pi^8 \pmod{p^{10}} \equiv -4\pi^2 + \pi^8 \pmod{p^{10}} \equiv \pi^2(\pi^3 - 2)(\pi^3 + 2) \pmod{p^{10}} \equiv 0 \pmod{p^{10}} \). It follows that \( s \leq 9 \). Now suppose

\[
x_1^4 + ... + x_{s+1}^4 \equiv 0 \pmod{p^{10}} \tag{*}
\]

We may suppose that \( \mathfrak{p} \nmid x_i, \mathfrak{p} \mid x_1 ... x_r, r \geq 1 \) and \( \mathfrak{p} \mid x_i \) if \( i > r \). Notice that if \( x \equiv y \pmod{p^3} \) then \( x^4 \equiv y^4 \pmod{p^4} \). So without loss of generality we may suppose that

\[
x_i = \begin{cases} 1, 1 + \pi, 1 + \pi^2, 1 + \pi + \pi^2 & \text{for } 1 \leq i \leq r, \\ \pi, \pi + \pi^2, \pi^2 & \text{for } i > r. \end{cases}
\]

Now for \( i \leq r, x_i \equiv 1 \pmod{p} \) and therefore \( x_i^4 \equiv 1 \pmod{p^4} \), and for \( i > r, x_i^4 \equiv \pi^4, \pi^4 + \pi^8 + 8, \pi^8 \pmod{p^{10}} \equiv 0 \pmod{p^4} \). Hence \( 4 \mid r \) giving \( r = 4 \) or \( 8 \). Now suppose \( r = 4 \). Then direct calculations show (using the fact that \( 4\pi^3 \equiv 8 \pmod{p^{10}} \)) that

\[
x_1^4 + ... + x_4^4 \equiv \{ 4, 4 + 4\pi^2 + 2\pi^4, 12 + 2\pi^2 + 4\pi^4, 4 + 4\pi^2 + 2\pi^4 + \pi^8, \\
12 + 4\pi + 2\pi^2 + 3\pi^4 + \pi^8, 12 + 4\pi + 2\pi^2 + 3\pi^4, 4 + \pi^8, \\
12 + 4\pi + 6\pi^2 + \pi^4 + \pi^8 \pmod{p^{10}} \tag{†} \]
\]

and \( x_{r+1}^4 + ... + x_{s+1}^4 \equiv i\pi^4 + j\pi^8 + k \cdot 8 \) (0 \( \leq i \leq 3, 0 \leq j, k \leq 1 \)) \pmod{p^{10}}. For \( i \) odd, the exact power of \( \mathfrak{p} \) in \( x_1^4 + ... + x_r^4 + ... + x_{s+1}^4 \) can be 4 or 5 while for \( i \) even, this exact power can be 4 or 6 and this contradicts (*) above and so \( r \neq 4 \).
Next suppose $r = 8$. Then again a direct calculation shows that $x_1^4 + \ldots + x_8^4 = 4$ added to each element of the set $(\dagger)$ above (mod $p^{10}$) and none of these is $\equiv 0, -\pi^4, -(\pi^4 + \pi^8 + 8), -8$ (mod $p^{10}$) as a simple calculation shows. Hence $s > 8$. This completes the proof.

**Lemma 4.** Let $3 | f$, then $s \leq 5$.

**Proof.** $\mathbb{F}_8$, the field of 8 elements. Hence there exists an $\alpha \in \mathbb{F}$ such that $\alpha^7 \equiv 1$ (mod $p$), $\alpha \not\equiv 1$ (mod $p$). Find $\beta$ such that $\beta \equiv \equiv \alpha$ (mod $p$), $\beta^7 \equiv 1$ (mod $p^{3e+1}$) (in fact $x^7 = 1$ has a solution in $k_p$ with $x \equiv \alpha$ (mod $p$)). Then $(1 + \beta + \ldots + \beta^6)(1 - \beta) \equiv 0$ (mod $p^{3e+1}$) giving $1 + \beta + \ldots + \beta^6 \equiv 0$ (mod $p^{3e+1}$) (since $1 - \beta \not\in \mathbb{F}$). We now have

$$3 \cdot 1^4 + (\beta + \beta^6)^4 + (\beta^2 + \beta^5)^4 + (\beta^3 + \beta^4)^4 \equiv 3 + \beta^4 + 4\beta^2 + 6 + 4\beta^5 + \beta^3 + \beta + 4\beta^4 + 6 + 4\beta^3 + \beta^6 + \beta^2 + 4\beta + 6 + 4\beta^6 + \beta^5 \equiv 21 + 5(\beta + \beta^2 + \ldots + \beta^6) \equiv 0$$

It follows that $s \leq 5$.

**Lemma 5.** Let $e = 1$ and let $f$ be odd, then $s \geq 4$.

**Proof.** Suppose to the contrary that $s < 4$. Then there exists $x_1, x_2, x_3, x_4 \in \mathbb{F}$ such that

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod{p^4} \quad (p | x_1). \quad (*)$$

We can then find $t \in \mathbb{F}$ such that $x_1 t \equiv 1$ (mod $p^4$) and multiplying $(*)$ by $t$; we get $x, y, z \in \mathbb{F}$ such that

$$1 + x^4 + y^4 + z^4 \equiv 0 \pmod{p^4} \quad (1)$$

Hence $(1 + x + y + z)^4 \equiv 0$ (mod $p$) and therefore $z \equiv 1 + x + y$ (mod $p$), giving $z^2 \equiv 1 + x^2 + y^2 + 2(x + y + xy)$ (mod $p^2$) and $z^4 \equiv 1 + x^4 + y^4 + 2x^2 + 2y^2 + 2x^2y^2 + 4[(x + y + xy)^2 + (x + y + xy)(1 + x^2 + y^2)]$ (mod $p$) and by (1) this implies $2(1 + x^4 + y^4 + x^2 + y^2 + 2xyy) \equiv 0$ (mod $p^2$), giving $1 + x^4 + y^4 + x^2 + y^2 + 2x^2y^2 \equiv 0$ (mod $p$). This implies

$$(x^2 + 1)^2 + (y^2 + 1)^2 + (x^2 + 1)(y^2 + 1) \equiv 0 \pmod{p} \quad (2)$$

Now since $f$ is odd so $3 \not| 2^f - 1$ and so $\gamma^3 \equiv 1$ (mod $p$) implies $\gamma \equiv 1$ (mod $p$). Thus for any $\delta \in \mathbb{F}$, $\delta^2 + \delta + 1 \not\equiv 0$ (mod $p$). This gives $\alpha^2 + \beta^2 + \alpha \beta \equiv 0$ (mod $p$) (or $\alpha, \beta \in \mathbb{F}$) implies $p | \alpha$ and $p | \beta$. (2) now gives $p | x^2 + 1$.
and \( p \mid y^2 + 1 = (y - 1)^2 + 2y \). Hence \( x \equiv 1 \pmod{p} \), \( y \equiv 1 \pmod{p} \) and then \( z \equiv 1 \pmod{p} \). It follows that \( 1 + x^4 + y^4 + z^4 \equiv 4 \pmod{p^3} \) and this contradicts (1). That completes the proof.

**Lemma 6.** Let \( e = 1 \), \( f = 3 \), then the congruence
\[
2 + x^4 + y^4 + z^4 \equiv 0 \pmod{p^3}
\]
has no solution in \( \mathbb{Z} \).

**Proof.** If a solution exists then \( z \equiv x + y \pmod{p} \) and so \( z^4 \equiv (x + y)^4 \equiv (x^2 + y^2 + 2xy)^2 \equiv x^4 + y^4 + 4x^2y^2 + 4xy(x^2 + y^2) + 2x^2y^2 \pmod{p^3} \).

Eliminating \( z \), using (1) gives
\[
2(x^4 + y^4 + x^2y^2 + 1) + 4xy(x^2 + y^2 + xy) \equiv 0 \pmod{p^3}
\]
This implies \( x^4 + y^4 + x^2y^2 + 1 \equiv 0 \pmod{p} \), i.e.
\[
x^2 + y^2 + xy + 1 \equiv 0 \pmod{p}
\]
(2) and (3) give
\[
2(x^4 + y^4 + x^2y^2 + 1) + 4xy \equiv 0 \pmod{p^3}
\]
or
\[
x^4 + y^4 + x^2y^2 + 1 + 2xy \equiv 0 \pmod{p^2}
\]
(4) But by (3),
\[
x^4 + y^4 + x^2y^2 + 2xy(x^2 + y^2) \equiv 1 \pmod{p^3}
\]
(4) and (5) imply \( 2xy(x^2 + y^2 - 1) \equiv 2 \pmod{p^2} \) i.e. \( xy(x^2 + y^2 - 1) \equiv 1 \pmod{p} \), i.e. \( xy(x^2 + y^2 + 1) \equiv 1 \pmod{p} \). But by (3) now this gives \( (x^2 + y^2 + 1)^2 \equiv 1 \pmod{p} \) i.e. \( (x^2 + y^2) \equiv 1 \pmod{p} \), i.e. \( x^2 + y^2 \equiv 0 \pmod{p} \), i.e. \( x \equiv y \pmod{p} \). Hence \( z \equiv x + y \equiv 2x \equiv 0 \pmod{p} \). By symmetry \( x \equiv y \equiv 0 \pmod{p} \) too, hence (1) gives \( 2 \equiv 0 \pmod{p^3} \) which is a contradiction. This proves the lemma.

**Lemma 7.** Let \( e = 1 \), \( f = 3 \), then \( s = 5 \).

**Proof.** Suppose \( s \neq 5 \), then by lemmas 4 and 5, \( s = 4 \). Let
\[
x_1^4 + \ldots + x_5^4 \equiv 0 \pmod{p^4}
\]
have a solution, where \( p \mid x_i \) for any \( i \). We may assume that the \( x_i \) are distinct modulo \( p \), for otherwise, multiplying by a suitable fourth power, \( (*) \) will yield a solution of \( 2 + x^4 + y^4 + z^4 \equiv 0 \pmod{p^3} \), contradicting lemma 6.
Now observe that (*) implies \( x_1 + ... + x_5 \equiv 0 \pmod{p} \), and then it is easy to check that the elements \( 0, x_1, x_2, x_3, x_4, x_5, x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_5 \) (and indeed 6 other similar ones) are distinct modulo \( p \). But \( \mathbb{F}/p \) is a field of 2^f = 8 elements and this gives a contradiction.

**Proof of theorem 3.** The decomposition of (2) in \( k \), as written in the statement of theorem 3 has been given by Wahlin [11]. For any \( p \parallel 2 \), we have the following possibilities:

1. \( e = 1 = f \). Then by theorem 1, \( s = 15 \).
2. \( e = 1, f = 2 \). Then by lemma 1, \( s = 2 \).
3. \( e = 1, f = 3 \). Then by lemma 7, \( s = 5 \).
4. \( e = 3, f = 1 \). Then by lemma 3, \( s = 9 \).
5. \( e = 2, f = 1 \). Then by lemma 2, \( s = 4 \) or 6.

It remains to determine \( s \) in the last case i.e. when \( e = 2, f = 1 \), i.e. to determine \( s_4(k_{p_2}) \) in the cases (v), (vi) and (viii) of the theorem.

**Proof of (viii) for \( p_2 \).** We have \( \theta^3 = -C\theta - D \) and so since \( C, D \) are both even, \( p_1 \mid \theta, \ p_2 \mid \theta \). In case \( p_2^2 \mid \theta \) we have \( 2 \mid \theta \) which is not possible since \( 2^2 \mid C \) and so one can take the \( \pi \) of lemma 2 to be \( = \theta \). Now \( \theta (\theta^2 + 2) = (-\langle C-2 \rangle \theta - D, \ so \ p_2^4 \parallel \theta (\theta^2 + 2) \) if \( \mu = 2 \) (since \( p_2^4 \parallel \langle C-2 \rangle \theta \) and \( \frac{4}{2} \parallel D \)) and \( p_2^4 \parallel \theta (\theta^2 + 2) \) if \( \mu > 2 \) (since \( p_2^4 \parallel \langle C-2 \rangle \theta \) and \( \frac{6}{2} \parallel D \)).

For \( \mu = 2 \), \( p_2^3 \parallel \theta^2 + 2 \) and hence \( s = 4 \) by lemma 2, while for \( \mu > 2 \), \( p_2^4 \parallel \theta^2 + 2 \) and again by lemma 2, \( s = 6 \).

**Proof of the cases (v) and (vi) for \( p_2 \).** Let \( K = k(\sqrt{\Delta}) \), the splitting field of \( X^3 + CX + D \). We have \([K:Q] = 6 \). Let \( \mathfrak{O} \) be the ring of integers of \( K \).

A simple observation reveals that \( p_1 \mathfrak{O} = p_{21}^2, p_2 \mathfrak{O} = p_{21} p_{22} \) is the decomposition of \( p_1 \) and \( p_2 \) in \( \mathfrak{O} \). Thus (2) = \( p_{11}^2 p_{21}^2 p_{22}^2 \). Here clearly \( f \), the residue class degree of \( p_{21} \) is 1 and \( e \), the ramification index of \( p_{21} \) is 2.

We have now the two cases \( \nu \) even and odd.

**Case (v) (\( \nu \) even).** Then \( \Delta' \equiv 3 \pmod{4} \) and \( (1 + \sqrt{\Delta'})^2 = 1 + \Delta' + 2\sqrt{\Delta'} \). Here \( 4 \mid 1 + \Delta' \), so \( p_{21}^6 \mid 1 + \Delta' \) and \( p_{21}^2 \mid 2\sqrt{\Delta'} \). Hence \( p_{21}^2 \parallel (1 + \sqrt{\Delta'})^2 \) and so \( p_{21} \mid (1 + \sqrt{\Delta'}) \). Now in \( K \), for \( \mathfrak{p} = p_{21} \), we take \( \pi = 1 + \sqrt{\Delta'} \) (the \( \pi \) of lemma 2). Then \( \pi^2 + 2 = 1 + \Delta' + 2(1 + \sqrt{\Delta'}) \equiv 0 \pmod{p_{21}} \). It follows that \( s_4(K_{p_{21}}) = 4 \).

Now take any \( \pi' \in \mathfrak{p} \) such that \( \mathfrak{p} \nmid \pi' \). Then \( p_{21} \nmid \pi' \) in \( \mathfrak{O} \). Therefore
\[ \pi^2 + 2 \not\equiv 0 \pmod{p_2^4} \] (since \( s_4(K_{p_2}) = 4 \)) and hence \( \pi^2 + 2 \not\equiv 0 \pmod{p_2^4} \).

It follows that \( s_4(k_{p_2}) = 4 \) (again by lemma 2).

**Case (vi) (\( \nu \) odd).** Here \( \sqrt{2\Delta'} \in \bar{k} \) and \( p_2^2 \parallel 2\Delta' \), i.e. \( p_{21} \parallel \sqrt{2\Delta'} \). Further \( 2\Delta' + 2 \equiv 0 \pmod{4} \) and so \( \equiv 0 \pmod{p_{21}^2} \). By lemma 2 it follows that \( s_4(K_{p_{21}}) = 6 \). But now \( k_{p_2} \subset K_{p_{21}} \) and so \( s_4(k_{p_2}) \geq 6 \). But by lemma 2 again \( s_4(k_{p_2}) = 4 \) or 6. It follows that \( s_4(k_{p_2}) = 6 \). This completes the proof of theorem 3.

### Table of results

Let \( p \mid 2 \) and \( e, f \) be the ramification index, residue class degree of \( p \). We use ‘arb’ for arbitrary and ‘mult’ for multiple.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>1</th>
<th>3</th>
<th>arb</th>
<th>&gt;1</th>
<th>arb</th>
<th>even</th>
<th>arb</th>
<th>arb</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>e</strong></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>arb</td>
<td>&gt;1</td>
<td>arb</td>
<td>even</td>
<td>arb</td>
<td>arb</td>
<td>1</td>
</tr>
<tr>
<td><strong>f</strong></td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>arb</td>
<td>arb</td>
<td>&gt;1</td>
<td>arb</td>
<td>mult of 3</td>
<td>even</td>
<td>odd</td>
</tr>
<tr>
<td><strong>s</strong></td>
<td>15</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>( \leq 15 )</td>
<td>( \leq 12 )</td>
<td>( \leq 11 )</td>
<td>( \leq 9 )</td>
<td>( \leq 5 )</td>
<td>( \leq 2 )</td>
<td>( \geq 4 )</td>
</tr>
</tbody>
</table>

§ 6. \( s_4(k) \) in some special cases.

1. If \( k \) is an algebraic number field such that

   (i) some \( \sqrt{-m} \in k \) where \( m \) is a natural number of the form \( 8n + 7 \),

   (ii) there exists a prime divisor \( p \) of 2 in \( k \) with \( e_p = f_p = 1 \),

   then \( s_4(k) = 15 \).

**Proof.** By theorem 1, \( s_4(k) = 15 \); hence \( s_4(k) \geq 15 \). But \( s_4(k) \leq s_4(Q(\sqrt{-m})) = 15 \), by theorem 2 of [6].

   As an explicit example of the above situation, we may take

   \[ k = Q(\sqrt{m_1}, \ldots, \sqrt{m_r}) \]

   where the \( m_j \) are integers of the form \( 8n + 1 \) and at least one of them is negative. To see this we note using Hasse [3] or proposition 17 of Lang [4] (chapter 3, page 68) that for \( p \mid 2 \), \( e_p = 1 \). Further for

   \( \mathcal{A} = (2, (1 + \sqrt{m_1})/2, \ldots, (1 + \sqrt{m_r})/2) \).
routine direct calculations show that \( N(\mathfrak{A}) = 2 \), and so \( \mathfrak{A} = \mathfrak{p} \) (a prime ideal dividing 2) with \( f_\mathfrak{p} = 1 \).

It may similarly be shown, using theorem 2 and theorems 3-6 of [6] that

II. \( s_4(k) = 6 \) if \( \sqrt{-2} \in k \) and there is a prime divisor \( \mathfrak{p} \) of 2 in \( k \) with \( e_\mathfrak{p} = 2 \), \( f_\mathfrak{p} = 1 \).

As an explicit example of this situation we may take

\[ k = \mathbb{Q}(\sqrt{-2}, \sqrt{m_1}, ..., \sqrt{m_r}) \, , \, m_j \equiv 1 \pmod{8} \]

III. \( s_4(k) = 4 \) if \( \sqrt{-5} \) or \( \sqrt{-1} \in k \) and there is a prime divisor \( \mathfrak{p} \) of 2 in \( k \) with \( e_\mathfrak{p} = 2 \), \( f_\mathfrak{p} = 1 \).

As an example we may take \( k = \mathbb{Q}(\sqrt{-5}, \sqrt{m_1}, ..., \sqrt{m_r}) \) or \( \mathbb{Q}(\sqrt{-1}, \sqrt{m_1}, ..., \sqrt{m_r}) \), with \( m_j \equiv 1 \pmod{8} \).

REFERENCES


[8] Ramanujam, C.P.: "Sums of \( m^{th} \) powers in \( p \)-adic rings", Mathematika, 10 (1963), 137-146.


J.C. PARANI, M.K. AGRAWAL, A.R. RAJWADE - Department of Mathematics, Panjab University, Chandigarh, India.

Lavoro pervenuto in redazione in 26/IX/1984