PACIFIC JOURNAL OF MATHEMATICS
Vol. 75, No. 2, 1978

PRIME IDEAL DECOMPOSITION IN $F(\mu^{1/p})$

WILLIAM YSLAS VÉLEZ

Let F be a finite extension of the field of rational numbers, $\mathscr{P}$ a prime ideal in the ring of algebraic integers in F, and $x^m - \mu$ irreducible over F. If m is a prime and $\zeta_m \in F$, then the ideal decomposition of $\mathscr{P}$ in $F(\mu^{1/m})$ has been described by Hensel. If $m = l^t$, l a prime and $(l, \mathscr{P}) = 1$, then the decomposition of $\mathscr{P}$ in $F(\mu^{1/l^t})$ was obtained by Mann and Vélez, with no restriction on roots of unity. In this paper we describe the decomposition of $\mathscr{P}$ in the fields $F(\zeta_p)$ and $F(\mu^{1/p})$, where $\mathscr{P} \supset (p)$.

I. Notation and introduction. Let $\mathscr{Q}$ denote the rational numbers and F a finite extension of $\mathscr{Q}$ where the degree of an extension is denoted by $[F: \mathscr{Q}]$. By a prime ideal $\mathscr{P}$ in F we shall mean a prime, integral ideal in the ring of algebraic integers in F. For an ideal $\mathscr{P}$, we have $N(\mathscr{P}) = p^f$, p a prime, where N denotes the absolute norm and $(p) = \mathscr{P}^a \mathscr{A}$, $(\mathscr{P}, \mathscr{A}) = 1$, where (a, b) denotes the greatest common divisor of a and b. If $p - 1 \mid a$, then we set $a = sp^{k-1}(p-1)$, $(s, p) = 1$. By $F_{\mathscr{P}}$ we shall mean the $\mathscr{P}$-adic completion of F, $[x]$ denotes the largest integer less than or equal to x, $a/b + c$ shall mean $a/(b + c)$, and ζ_{p^t} denotes a primitive p^t-root of unity.

If A is an abelian group, then we say that $\{\alpha_i\}_{i \in I}$, is a basis for A if $A = \bigoplus_{i \in I} \langle \alpha_i \rangle$, where $\langle \alpha_i \rangle$ denotes the group generated by α_i in A.

We say $p^c \| b$ if $p^c \mid b$, $p^{c+1} \nmid b$.

This paper is devóted to a generalization of what is called in the literature, "Kummer's Theorem." This theorem deals with the ideal decomposition of prime ideals in F when considered as ideals in $F(\mu^{1/p})$.

Hilbert [12, pg. 254–257] proved the following theorem:

THEOREM 1.1. *If $x^p - \mu$ is irreducible over $\mathscr{Q}(\zeta_p)$, $(\mu, \mathscr{P}) = 1$, then in $\mathscr{Q}(\zeta_p, \mu^{1/p})$ we have*

(1) *the ideal $\mathscr{P}$ splits into p factors iff $\mu \equiv \xi^p \pmod{\mathscr{P}^{p+1}}$,*

(2) *the ideal $\mathscr{P}$ remains prime iff $\mu \not\equiv \xi^p \pmod{\mathscr{P}^{p+1}}$, $\mu \equiv \xi^p \pmod{\mathscr{P}^p}$,*

(3) *the ideal $\mathscr{P}$ becomes the pth-power of a prime ideal iff $\mu \not\equiv \xi^p \pmod{\mathscr{P}^p}$.*

Later Hensel [9, 10] generalized these theorems to the situation where $\zeta_p \in F_{\mathscr{P}}$. Hensel calls these theorems "Kummer's Theorem," but he references Hilbert, and Hilbert gives no reference for these theorems.

In §4 we describe the decomposition rules for the extensions $F(\mu^{1/p})$ and $F(\zeta_p)$ over F, for those prime ideals which divide p. Sections 2 and 3 develop some machinery to tackle this problem. This machinery will hopefully be used to describe the decomposition rules for the case $F(\mu^{1/p^c})$, $c > 1$, in a subsequent paper.

We point out that decomposition rules for the ideal $\mathcal{P}$ in the extension $F(\mu^{1/l^c})$, l a prime different from p, have already been worked out. We refer the reader to the paper by Mann and Vélez.

This paper is based on my Ph.D. thesis at the University of Arizona. I wish to express my deep appreciation to Professor Henry B. Mann for his advice and encouragement during that venture.

II. Preliminaries. We say that α is a principal unit if $\alpha \equiv 1 \pmod{\mathcal{P}}$.

Let $\mathcal{G}_m$ be the multiplicative group of units modulo $\mathcal{P}^m$. Then $|\mathcal{G}_m| = \Phi(\mathcal{P}^m) = (p^f - 1)p^{f(m-1)}$, where Φ is the Euler function. Clearly $\mathcal{G}_m$ is abelian. It can be shown that $\zeta_{p^f-1} \in F_{\mathcal{P}}$ and that $\mathcal{G}_m = \langle\zeta_{p^f-1}\rangle \oplus G_m$, where G_m is the multiplicative group of principal units modulo $\mathcal{P}^m$, and $|G_m| = p^{f(m-1)}$.

There have been several papers devoted to the study of G_m, e.g., Wolf [**25**], Tagenouchi [**18**], Hensel [**5, 6, 7, 8, 11**] and Mann [**14**]. We state some results which we shall need later. We first determine the rank of G_m, denoted by $R(G_m)$, as a p-group [see Fuchs **3**, pg. 85].

THEOREM 2.1.
If $m \leqq ap/p-1$, *then* $R(G_m) = (m-1-[(m-1)/p])f$.
If $m \geqq ap/p-1$, $\zeta_p \notin F_{\mathcal{P}}$, *then* $R(G_m) = af$.
If $m = ap/p-1$, $\zeta_p \in F_{\mathcal{P}}$, *then* $R(G_m) = af$.
If $m > ap/p-1$, $\zeta_p \in F_{\mathcal{P}}$, *then* $R(G_m) = af + 1$.

Proof. See Mann [**14**, pg. 3, pg. 9], Tagenouchi [**18**, pg. 22], Hensel [**6**, §§3 and 4], Vélez [**19**, pg. 10].

We now construct a basis for G_m, for m not too large. The residue system modulo $\mathcal{P}$ forms a finite, commutative field of degree f over its prime field. Hence, there exist algebraic integers $\{g_1, \cdots, g_f\}$ such that every element modulo $\mathcal{P}$ can be written uniquely as

$$\sum_{i=1}^{f} a_i g_i, \qquad a_i \in \{0, 1, \cdots, p-1\}.$$

The set $\{g_1, \cdots, g_f\}$ will be called an additive basis.

From the collection of positive integers choose the smallest a of them which are relatively prime to p and call them $k_1 < k_2 < \cdots < k_a$. Let π be an algebraic integer such that $\mathcal{P} \| \pi$.

Set

$$\eta_{ij} = 1 + g_i \pi^{k_j}. \tag{2.1}$$

THEOREM 2.2. (1) *If $m \leqq ap/p - 1$ and $q = m - 1 - [(m-1)/p]$, then $\{\eta_{ij} \mid i = 1, \cdots, f; j = 1, \cdots, q\}$ is a basis for G_m.*

(2) *If $\zeta_p \notin F_{\mathcal{P}}$ and $m \geqq ap/p - 1$, then $\{\eta_{ij} \mid i = 1, \cdots, f; j = 1, \cdots, a\}$ is a basis for G_m.*

Proof. See Mann [**14**, pg. 8], Hensel [**6**, pgs. 204, 205], Vélez [**19**, pg. 26].

Now, let $\zeta_p \in F_{\mathcal{P}}$. Then clearly $p - 1 \mid a$, so $ap/p - 1$ is an integer. Since $R(G_m) = af + 1$, when $m > ap/p - 1$, we need an extra element.

LEMMA 2.1. *Let $-p \equiv \pi^a g^{p-1} \pmod{\mathcal{P}^{a+1}}$, then there is a g' such that $x^p - g^{p-1}x - g'$ has no solution modulo $\mathcal{P}$.*

Proof. See Mann [**14**, pg. 10], Hensel [**6**, Section 3], Vélez [**19**, pg. 29].

With g' defined as in Lemma 2.1, set

$$\eta' = 1 + g' \pi^{sp^k}.$$

Note that $sp^k = a + (a/p - 1)$.

LEMMA 2.2. *Let $\zeta_p \in F_{\mathcal{P}}$ and $m \geqq ap/p - 1$, then η' is not a pth-power in G_m.*

Proof. See Mann [**14**, pg. 10, 11], Hensel [**6**, §4], Vélez [**19**, pg. 29].

THEOREM 2.3. *If $\zeta_p \in F_{\mathcal{P}}$ and $m = (ap/p - 1) + 1 = sp^k + 1$, then $\{\eta', \eta_{ij} \mid i = 1, \cdots, f; j = 1, \cdots, a\}$ forms a basis for G_m. If $m > sp^k + 1$, then $\{\eta', \eta_{ij} \mid i = 1, \cdots, f; j = 1, \cdots, a\}$ is a generating set for G_m, though it is not necessarily a basis.*

Proof. See Mann [**14**, pgs. 12–14], Hensel [**6**, §4], Vélez [**19**, pg. 29].

III. Analysis in $F_{\mathcal{P}}$.

Let $A = \{\alpha_i\}$ be a complete residue system modulo $\mathcal{P}$. That is, if β is an integer in F, then there exists a unique i such that $\beta \equiv \alpha_i \pmod{\mathcal{P}}$. Let $\mathcal{P} \,\|\, \pi$, then every element $\gamma \in F_{\mathcal{P}}$ can be written uniquely as

$$\gamma = \sum_{n=l}^{\infty} a_n \pi^n, \qquad l \in Z, \quad a_n \in A.$$

We say that γ is an integer if $l \geqq 0$.

If

$$x = \sum_{n=l}^{\infty} \gamma_n \pi^n,$$

γ_n is an integer for all n and $\gamma_l \not\equiv 0 \pmod{\mathcal{P}}$, then we set $\nu_{\mathcal{P}}(x) = l$. Let $\nu(x) = \nu_{\mathcal{P}}(x)$ if there is no danger of ambiguity.

It is clear that $\nu(x)$ is well-defined. Moreover, $\nu(x) = l$ iff $\mathcal{P}^l \,\|\, x$. It can also be shown that the series $\Sigma_{n=0}^{\infty} \beta_n$, $\beta_n \in F_{\mathcal{P}}$, converges in $F_{\mathcal{P}}$ iff $\lim_{n\to\infty} \nu(\beta_n) = \infty$ in $\mathcal{Q}$.

Fact 1. The domain of convergence of the exponential series $E(x) = \Sigma_{n=0}^{\infty} x^n/n!$, is the set of all x for which $\nu(x) > N$, where $N = [a/p - 1]$. The domain of convergence of the logarithmic series $\log(1 + x) = \Sigma_{n=1}^{\infty} (-1)^{n-1} x^n/n$, is the set of all x for which $\nu(x) \geqq 1$.

Let $f(y) = \Sigma_{n=0}^{\infty} a_n y^n$ and $g(x) = \Sigma_{m=1}^{\infty} b_m x^m$. If we substitute $g(x)$ for y in $f(y)$ and carry out the formal multiplications, we obtain a power series in x, which we call $G(x)$.

Fact 2. (On Substitution of Series in Series). Let the series $f(y) = \Sigma_{n=0}^{\infty} a_n y^n$ converge for all y which satisfy $\nu(y) \geqq l$, $l \in Z$. If the series $g(x) = \Sigma_{m=1}^{\infty} b_m x^m$ converges for some $x \in F_{\mathcal{P}}$ and $\nu(b_m x^m) \geqq l$, for all $m \geqq 1$, then the series $G(x)$ also converges (for this value of x) and

$$G(x) = f(g(x)).$$

We note two properties of these power series: $E(x)^n = E(nx)$, for $n \in Z$, and $E(\log(1 + x)) = 1 + x$, for $\nu(x^n/n) > N$. We refer the reader to Borevich and Shafarevich [Chapter 4] for proofs of the above statements.

THEOREM 3.1. *The series* $f(x) = 1 + \Sigma_{n=1}^{\infty} \binom{1/p^t}{n} x^n$ *converges in* $F_{\mathcal{P}}$ *if* $\nu(x) > ta + N$. *Furthermore* $1 + x = (f(x))^{p^t}$ *for* $\nu(x) > ta + N$.

Proof. The series

$$1 + \sum_{n=1}^{\infty} \binom{1/p^t}{n} x^n = 1 + \sum_{n=1}^{\infty} (z_n/n!)(x/p^t)^n,$$

where $z_n = (1-p^t)(1-2p^t)\cdots(1-(n-1)p^t)$. Note that $(z_n, p)=1$, so $\nu(z_n)=0$. But $\nu(x/p^t)=\nu(x)-\nu(p^t)> ta+N-ta=N$. But, from Fact 1, $\Sigma_{n=1}^{\infty}(1/n!)(x/p^t)^n$ converges, which implies that

$$\nu((1/n!)(x/p^t)^n)=\nu((z_n/n!)(x/p^t)^n)\to\infty \quad \text{in} \quad \mathcal{Q}.$$

Hence $1+\Sigma_{n=1}^{\infty}\binom{1/p^t}{n}x^n$ converges if $\nu(x)>ta+N$.

Consider the series $(1/p^t)\log(1+x)=\Sigma_{n=1}^{\infty}(-1)^{n-1}x^n/np^t$, for $\nu(x)>ta+N$. Then we can show that $\nu(x^n/np^t)>N$ for all n. Hence we can substitute this series in the series $E(x)$, and formally carry out the multiplications. But since this is formal multiplication, we can perform these computations in $\mathcal{C}[x]$, where $\mathcal{C}$ is the field of complex numbers. So we have

$$E((1/p^t)\log(1+x))=f(x),$$

and by Fact 2, these two series converge in $F_{\mathcal{P}}$ to the same value. But then,

$$(f(x))^{p^t}=E((1/p^t)\log(1+x))^{p^t}=E(\log(1+x))=1+x.$$

THEOREM 3.2. *If $\alpha\equiv\eta^{p^t} \pmod{\mathcal{P}^{ta+N+1}}$, then there exists $\beta\in F_{\mathcal{P}}$ such that $\alpha=\beta^{p^t}$ in $F_{\mathcal{P}}$.*

Proof. If $\alpha\equiv\eta^{p^t} \pmod{\mathcal{P}^{ta+N+1}}$, then $\alpha/\eta^{p^t}=1+x$, where $\nu(x)>ta+N$. Hence, $(1+x)^{1/p^t}\in F_{\mathcal{P}}$. Let $\beta=(1+x)^{1/p^t}\eta$, then $\alpha=\beta^{p^t}$.

IV. The Decomposition of $\mathcal{P}$ in $F(\zeta_p)$ and $F(\mu^{1/p})$. Let K be a finite extension of F of degree n. We are interested in the prime ideal decomposition of $\mathcal{P}$ in K. Assume that $\mathcal{P}$ factors into g_i ideals of relative degree f_i and relative multiplicity e_i, that is, $n=\Sigma_i g_if_ie_i$. Then we define the counting function

$${}_F\Psi_K(\mathcal{P})=\sum_i g_i[f_i]^{e_i}.$$

For example, if K is a normal extension, then ${}_F\Psi_K(\mathcal{P})=g[d]^e$, which means $\mathcal{P}$ factors into g ideals, each of relative degree d and relative multiplicity e. In certain cases, these counting functions have some interesting properties. We refer the reader to the paper by Mann and Vélez.

LEMMA 4.1. *If $(a,b)=d$, where $a,b\in Z$, then there exists an $x\in Z$ such that $(a,x)=1$ and $bx+ay=d$.*

Proof. Mann and Vélez, pg. 2.

Let $\mathcal{Q}_p$ denote the p-adic completion of $\mathcal{Q}$; $\mathcal{F}$, $\mathcal{K}$, and $\mathcal{L}$ are finite extensions of $\mathcal{Q}_p$, and $e(\mathcal{F}\,|\,\mathcal{Q}_p) = e'$ denotes the ramification degree of $\mathcal{F}$ over $\mathcal{Q}_p$.

LEMMA 4.2. *If $\mathcal{K}$ is an unramified extension of $\mathcal{F}$, then $\mathcal{K}$ is a normal extension. Furthermore, if $\mathcal{F}' \supset \mathcal{F}$, then $\mathcal{K}\cdot\mathcal{F}'$ is unramified over $\mathcal{F}'$, where $\mathcal{K}\cdot\mathcal{F}'$ denotes the smallest field containing both $\mathcal{K}$ and $\mathcal{F}'$.*

Proof. We refer the reader to Weiss [**22**, pgs. 83–85].

THEOREM 4.1. *Let $\mathcal{L}\cap\mathcal{F} = \mathcal{L}'$, and $e(\mathcal{L}'\,|\,\mathcal{Q}_p) = l_1$, $[\mathcal{L}:\mathcal{L}'] = e(\mathcal{L}\,|\,\mathcal{L}') = l$, $(l, p) = 1$, and $(e'/l_1, l) = d$. Then $\mathcal{L} = \mathcal{L}'(\pi^{1/l})$, where π is some prime element in $\mathcal{L}'$ and $e(\mathcal{F}(\pi^{1/l})\,|\,\mathcal{F}) = l/d$. Furthermore, if $\mathcal{K}$ is an unramified extension of $\mathcal{F}$, that is, $e(\mathcal{K}\,|\,\mathcal{F}) = 1$, then $e(\mathcal{K}(\pi^{1/l})\,|\,\mathcal{K}) = l/d$.*

Proof. We refer the reader to the paper by Vélez entitled "A Characterization of Completely Regular Fields."

The following corollary, though not new (see the paper by Ishida), is an interesting application of Theorem 4.1.

COROLLARY 1. *Let α be an integer in $\mathcal{Q}$ with $(\alpha, p) = 1$, and p an odd prime, then $\mathcal{Q}((\alpha p)^{1/p-1}, \zeta_p)$ is an abelain extension of $\mathcal{Q}((\alpha p)^{1/p-1})$ with relative discriminant* 1.

Proof. It is clear that $\mathcal{Q}((\alpha p)^{1/p-1}, \zeta_p)$ is an abelian extension of $\mathcal{Q}((\alpha p)^{1/p-1})$, and $(p) = \mathfrak{P}^{p-1}$, where $\mathfrak{P} = ((\alpha p)^{1/p-1}, p)$.

Let $\mathcal{F} = \mathcal{Q}_p((\alpha p)^{1/p-1})$, $\mathcal{L} = \mathcal{Q}_p(\zeta_p)$, and $\mathcal{L}' = \mathcal{F}\cap\mathcal{L}$. Then

$$e(\mathcal{F}\,|\,\mathcal{Q}_p) = [\mathcal{F}:\mathcal{Q}_p] = e(\mathcal{L}\,|\,\mathcal{Q}_p) = [\mathcal{L}:\mathcal{Q}_p] = p-1.$$

Let $l' = [\mathcal{L}':\mathcal{Q}_p] = e(\mathcal{L}'\,|\,\mathcal{Q}_p)$, then $[\mathcal{L}:\mathcal{L}'] = e(\mathcal{L}\,|\,\mathcal{L}') = (p-1)/l'$ and $(p-1)/l' = ((p-1)/l', (p-1)/l')$, so $e(\mathcal{Q}_p((\alpha p)^{1/p-1}, \zeta_p)\,|\,\mathcal{Q}_p((\alpha p)^{1/p-1}) = 1$. Hence $\mathcal{Q}((\alpha p)^{1/p-1}, \zeta_p)$ over $\mathcal{Q}((\alpha p)^{1/p-1})$ is unramified.

As before, let $\mathcal{P}$ be a prime ideal in F with $N(\mathcal{P}) = p^f$ and $(p) = \mathcal{P}^a\mathcal{A}$, where $(\mathcal{P}, \mathcal{A}) = 1$. Let $F\cap\mathcal{Q}(\zeta_p) = \mathcal{Q}^{(e_1)}$, where $e_1 = [F\cap\mathcal{Q}(\zeta_p):\mathcal{Q}]$ and $\mathcal{Q}^{(e_1)}$ is the unique subfield of $\mathcal{Q}(\zeta_p)$ of degree e_1 over $\mathcal{Q}$. Hence $[F(\zeta_p):F] = (p-1)/e_1$. Let $\mathcal{P}_1 \subset \mathcal{Q}^{(e_1)}$, $\mathcal{P}_1 \supset (p)$, and $(p) =$

$\mathcal{P}_1^{e_1}$. Also since $\mathcal{P}^a \| (p)$, we have that $a = a_1 e_1$ and $\mathcal{P}^{a_1} \| \mathcal{P}_1$. Let $f(x)$ denote the irreducible polynomial for ζ_p over F.

THEOREM 4.2. *Let $f(x) \equiv \Pi_{i=1}^{g} f_i(x) (\bmod \mathcal{P}^{a_1(p-1)/e_1})$, and*

$$d = (a/e_1 g, (p-1)/e_1 g),$$

then if $K = F(\zeta_p)$, we have that

$${}_F\Psi_K(\mathcal{P}) = g[d]^e, \quad \textit{where} \quad e = (p-1)/g e_1 d.$$

Proof. The discriminant of $f(x)$ over $\mathcal{Q}^{(e_1)}$ is $\mathcal{P}_1^{((p-1)/e_1)-1}$. Since $\mathcal{P}^{a_1} \| \mathcal{P}_1$, $a_1 = a/e_1$, we have that the discriminant of $f(x)$ over F is exactly divisible by $\mathcal{P}^{(a_1(p-1)/e_1)-a_1}$. If

$$f(x) \equiv \prod_{i=1}^{g} f_i(x) (\bmod \mathcal{P}^{a_1(p-1)/e_1}),$$

where the $f_i(x)$ are irreducible modulo $\mathcal{P}^{(a_1(p-1)/e_1)+1}$, then

$$f(x) = \prod_{i=1}^{g} \bar{f}_i(x) \tag{4.1}$$

in $F_{\mathcal{P}}$, [24, pg. 90], where $\bar{f}_i(x)$ is irreducible in $F_{\mathcal{P}}$ and $\deg \bar{f}_i(x) = (p-1)/e_1 g$, for all i. Set $\mathcal{L}' = F_{\mathcal{P}} \cap \mathcal{Q}_p(\zeta_p)$. Since $\deg \bar{f}_i(x) = (p-1)/e_1 g$, we have that $[\mathcal{L}' \colon \mathcal{Q}_p] = e_1 g$. Furthermore, $e(\mathcal{Q}_p(\zeta_p) | \mathcal{Q}_p) = p-1$, hence $e(\mathcal{L}' | \mathcal{Q}_p) = e_1 g$ and $e(\mathcal{Q}_p(\zeta_p) | \mathcal{L}') = (p-1)/e_1 g$. Since $((p-1)/e_1 g, p) = 1$, we can apply Theorem 4.1 and we obtain that

$$e(F_{\mathcal{P}}(\zeta_p) | F_{\mathcal{P}}) = (p-1)/e_1 g d. \tag{4.2}$$

On putting (4.1) and (4.2) together, we have that $\mathcal{P}$ factors in $F(\zeta_p)$ into g distinct prime ideals of relative degree d, and relative multiplicity $e = (p-1)/e_1 g d$. That is; we have

$$F^{\Psi}K^{(\mathcal{P})} = g[d]^e.$$

LEMMA 4.3. *Let $x^p - \mu$ be irreducible over F, μ an integer, $\mu = \mathcal{P}^{\nu}\mathcal{C}$, $(\mathcal{P}, \mathcal{C}) = 1$. If $p \nmid \nu$, then $\mathcal{P}$ becomes the pth-power of a prime ideal in $F(\mu^{1/p})$. If $p \mid \nu$, then we can find an integer μ_1 such that $(\mu_1, \mathcal{P}) = 1$ and $F(\mu^{1/p}) = F(\mu_1^{1/p})$.*

Proof. We first find a $\rho \in F$ such that ρ has ideal denominator $\mathcal{P}$. To find ρ we first determine an ideal C_1 so that $\mathcal{P}C_1 = (\alpha)$. Next determine an ideal C_2 so that $C_1C_2 = (\beta)$ and $(C_2, \mathcal{P}) = 1$ [**15**, 1955, *Theorem* 5.11]. Then $\rho = \beta/\alpha$ has the desired property.

If $p \nmid \nu$, then we can write $\nu x - py = 1$. Set $\mu_1 = \mu^x \rho^{yp}$. Then μ_1 is an integer, $F(\mu^{1/p}) = F(\mu_1^{1/p})$, and $\mathcal{P} \| \mu_1$. Hence $(\mathcal{P}, \sqrt[p]{\mu_1})^p = \mathcal{P}$, so $\mathcal{P}$ becomes the pth-power of a prime ideal in $F(\mu^{1/p})$.

If $p \mid \nu$, set $\mu_1 = \mu\rho^{\nu}$. Then μ_1 is an integer prime to $\mathcal{P}$ and $F(\mu^{1/p}) = F(\mu_1^{1/p})$.

Because of Lemma 4.3 we may assume that $(\mu, \mathcal{P}) = 1$.

LEMMA 4.4. *Let $x^p - \mu$ be irreducible over F, $(\mu, \mathcal{P}) = 1$. Then the ideal $\mathcal{P}$ has more than one factor in $F(\mu^{1/p})$ iff $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$, where $\mathcal{P}^a \| (p)$ and $N = [a/p - 1]$.*

Proof. From Theorem 3.2 we have that $\mu = \alpha^p$ in $F_{\mathcal{P}}$ iff $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$. But the number of relatively prime factors of $\mathcal{P}$ in $F(\mu^{1/p})$ is equal to the number of distinct prime factors of $x^p - \mu$ in $F_{\mathcal{P}}$, and $x^p - \mu$ is reducible in $F_{\mathcal{P}}$ iff $\mu = \alpha^p$ in $F_{\mathcal{P}}$. Hence $\mathcal{P}$ has at least two factors iff $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$.

If $\zeta_p \in F_{\mathcal{P}}$ then $a = sp^{k-1}(p-1)$ and $-p \equiv g^{p-1}\pi^a \pmod{\mathcal{P}^{a+1}}$. As before, we set $\eta' = 1 + g'\pi^{sp^k}$, where g' is chosen so that $h(x) = x^p - g^{p-1}x - g'$ has no solution modulo $\mathcal{P}$. Furthermore $x^p - g^{p-1}x - g'$ is irreducible modulo $\mathcal{P}$ and so $h(x)$ is irreducible in F. We also point out that $a + N = a + (a/p - 1) = sp^k$.

LEMMA 4.5. *The ideal $\mathcal{P}$ remains prime in $F((\eta')^{1/p})$.*

Proof. By Lemma 2.2, $\eta' \not\equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$, so $\mathcal{P}$ has only one factor in $F((\eta')^{1/p})$.

Let α be a root of $h(x)$ and consider $F(\alpha)$. The different of α is $(p\alpha^{p-1} - g^{p-1})$, which is prime to $\mathcal{P}$ since g is prime to $\mathcal{P}$. Hence $\mathcal{P}$ is not ramified in $F(\alpha)$. However, we have that

$$\begin{aligned}(1 + \alpha\pi^{sp^{k-1}})^p &\equiv 1 + p\alpha\pi^{sp^{k-1}} + \alpha^p\pi^{sp^k} \equiv 1 + (\alpha^p - g^{p-1}\alpha)\pi^{sp^k} \\ &\equiv 1 + g'\pi^{sp^k} \equiv \eta' \pmod{\mathcal{P}^{sp^k+1}}.\end{aligned}$$

If $\mathfrak{P}$ is any prime divisor of $\mathcal{P}$ in $F(\alpha)$, then $\mathfrak{P}^a \| (p)$ and

$$(1 + \alpha\pi^{sp^{k-1}})^p \equiv \eta' \pmod{\mathfrak{P}^{a+N+1}}.$$

Hence $(\eta')^{1/p} \in F(\alpha)_{\mathfrak{P}} = F_{\mathcal{P}}(\alpha)$, which implies that

$$F_{\mathcal{P}}(\alpha) = F_{\mathcal{P}}((\eta')^{1/p})$$

is an unramified extension, so $\mathcal{P}$ remains prime in $F((\eta')^{1/p})$.

From the proof we also have the following result.

LEMMA 4.6. *The field $F_{\mathcal{P}}(\alpha) = F_{\mathcal{P}}((\eta')^{1/p})$ is an unramified extension of $F_{\mathcal{P}}$, where α is a root of $x^p - g^{p-1}x - g'$.*

LEMMA 4.7. *If $x^p - \mu$ is irreducible over F and $\zeta_p \notin F_{\mathcal{P}}$, then $\mathcal{P}$ never remains a prime ideal in $F(\mu^{1/p})$.*

Proof. If $\mathcal{P}^{\nu} \| \mu$, $(\nu, p) = 1$, then $\mathcal{P} = \mathfrak{P}^p$ in $F(\mu^{1/p})$. If $(\nu, p) = p$ then we may assume that $(\mu, \mathcal{P}) = 1$.

Assume that $\mathcal{P}$ remains prime in $F(\mu^{1/p})$, then $x^p - \mu$ is irreducible over $F_{\mathcal{P}}$ and $F_{\mathcal{P}}(\mu^{1/p})$ is a normal, unramified extension of $F_{\mathcal{P}}$ by Lemma 4.2. Hence $\zeta_p \in F_{\mathcal{P}}(\mu^{1/p})$. But this implies that $[F_{\mathcal{P}}(\zeta_p) : F_{\mathcal{P}}] \mid p$, since $p = [F_{\mathcal{P}}(\mu^{1/p}) : F_{\mathcal{P}}]$. However $([F_{\mathcal{P}}(\zeta_p) : F_{\mathcal{P}}], p) = 1$, so $[F_{\mathcal{P}}(\zeta_p) : F_{\mathcal{P}}] = 1$, which implies that $\zeta_p \in F_{\mathcal{P}}$, and this contradicts the assumption that $\zeta_p \notin F_{\mathcal{P}}$. Hence $\mathcal{P}$ does not remain prime.

LEMMA 4.8. *Let $[F(\mu^{1/p}) : F] = p$, then $F(\mu^{1/p}) = F(\mu_1^{1/p})$ iff $\mu_1 = \beta^p \mu^x$, $(x, p) = 1$, $\beta \in F$.*

Proof. See the paper by Schinzel, pg. 163.

THEOREM 4.3. *Let $\mathcal{P}^a \| (p)$ in F, $F \cap \mathcal{Q}(\zeta_p) = \mathcal{Q}^{(e_1)}$, $x^p - \mu$ irreducible over F, $(\mu, \mathcal{P}) = 1$, and $N = [a/p - 1]$.*

(1) *If $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$, then*

$$_F\Psi_K(\mathcal{P}) = 1[1] + e_1 g[d]^e, \qquad K = F(\mu^{1/p}),$$

where

$$_F\Psi_{K_1}(\mathcal{P}) = g[d]^e, \qquad K_1 = F(\zeta_p).$$

Furthermore, if $\mathfrak{P}$ is a factor of degree d, then $F(\mu^{1/p})_{\mathfrak{P}} = F_{\mathcal{P}}(\zeta_p)$.

(2) *If $a + N > 1$, (1) is not solvable, and $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, then $\zeta_p \in F_{\mathcal{P}}$ and $_F\Psi_K(\mathcal{P}) = 1[p]$.*

(3) *If $a + N > 1$, $\mu \not\equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, then $_F\Psi_K(\mathcal{P}) = 1[1]^p$.*

(4) *If $a + N = 1$, $\mu \not\equiv \xi^p \pmod{\mathcal{P}^2}$, then $_F\Psi_K(\mathcal{P}) = 1[1]^p$.*

Proof. Since $(\mu, \mathcal{P}) = 1$, we have that $\mu^{p^f - 1} \equiv 1 \pmod{\mathcal{P}}$ where $N(\mathcal{P}) = p^f$. Since $(p^f - 1, p) = 1$, we have that $F(\mu^{1/p}) = F((\mu^{p^f-1})^{1/p})$. Hence, we may assume that $\mu \equiv 1 \pmod{\mathcal{P}}$.

(1) If $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N+1}}$, we have that $\mu = \alpha^p$ in $F_{\mathcal{P}}$ by Theorem 3.2. Hence $x^p - \mu = x^p - \alpha^p = (x - \alpha)$. $\Pi_{i=1}^{e_1 g} f_i(x)$ in $F_{\mathcal{P}}$ where $\deg f_i(x) = (p-1)/e_1 g$, each $f_i(x)$ is irreducible in $F_{\mathcal{P}}$, and $\zeta_p^{j(i)}\alpha$, $(j(i), p) = 1$, is a root of $f_i(x)$, for each i. By Theorem 4.2, we have that $e(F_{\mathcal{P}}(\zeta_p^{j(i)}\alpha) \mid F_{\mathcal{P}}) = e$, where $e = (p-1)/ge_1 d$, $d = (a/e_1 g, (p-1)/e_1 g)$.

Therefore, corresponding to the linear factor $x - \alpha$ we have an ideal factor of $\mathcal{P}$ in $F(\mu^{1/p})$ of relative degree and multiplicity 1. Corresponding to each of the $e_1 g$ polynomials $f_i(x)$, $\mathcal{P}$ has an ideal factor of relative degree d and multiplicity e. Hence

$$_F\Psi_K(\mathcal{P}) = 1[1] + e_1 g[d]^e.$$

Furthermore, if $\mathfrak{P}$ is any prime factor of $\mathcal{P}$ in $F(\mu^{1/p})$ of relative degree d, then $\mathfrak{P}$ corresponds to one of the $f_i(x)$. But a root of $f_i(x)$ is $\zeta_p^{j(i)}\alpha$, $(j(i), p) = 1$. Hence $F_{\mathcal{P}}(\zeta_p^{j(i)}\alpha) = F_{\mathcal{P}}(\zeta_p)$. So $F(\mu^{1/p})_{\mathfrak{P}} = F_{\mathcal{P}}(\zeta_p)$.

(2) We first show that if $\zeta_p \notin F_{\mathcal{P}}$ and $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, $a + N > 1$, then $\mu \equiv \xi_1^p \pmod{\mathcal{P}^{a+N+1}}$. By Theorem 2.2, $\{\eta_{ij} \mid i = 1, \cdots, f; j = 1, \cdots, a\}$ is a basis for G_m, $m \geqq a + N > 1$. But if $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, then $\mu \equiv \Pi \eta_{ij}^{b_{ij}} \pmod{\mathcal{P}^{a+N}}$ and $p \mid b_{ij}$, for all i, j. If $\mu \equiv \Pi \eta_{ij}^{b'_{ij}} \pmod{\mathcal{P}^{a+N+1}}$, then $b'_{ij} = b_{ij} + pc_{ij}$, hence $p \mid b'_{ij}$ and $\mu \equiv \xi_1^p \pmod{\mathcal{P}^{a+N+1}}$.

Assume that $a + N > 1$, (1) is not solvable, and $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N}}$. Then $\zeta_p \in F_{\mathcal{P}}$. Furthermore, by Lemma 4.4, $\mathcal{P}$ has only one factor in $F(\mu^{1/p})$.

By Theorems 2.2 and 2.3, we have that $\{\eta_{ij} \mid i = 1, \cdots, f, j = 1, \cdots, a\}$ is a basis for G_{a+N}, and $\{\eta_{ij} \mid i = 1, \cdots, f, j = 1, \cdots, a, \eta'\}$ is a basis for G_{a+N+1}. Hence,

$$\mu \equiv \prod \eta_{ij}^{b_{ij}} \cdot \eta'^{b} \pmod{\mathcal{P}^{a+N+1}}, \tag{4.3}$$

and

$$\mu \equiv \prod \eta_{ij}^{b_{ij}} \equiv \xi^p \pmod{\mathcal{P}^{a+N}}.$$

So $p \mid b_{ij}$, for all i, j, and $(b, p) = 1$. We can rewrite (4.3) as

$$\mu \cdot \eta'^{-b} \equiv \xi_1^p \pmod{\mathcal{P}^{a+N+1}},$$

so $\mu = \alpha^p \cdot \eta'^{b}$ in $F_{\mathcal{P}}$. Hence $F_{\mathcal{P}}(\mu^{1/p}) = F_{\mathcal{P}}(\eta'^{1/p})$ is an unramified extension of $F_{\mathcal{P}}$ by Lemma 4.5. So $\mathcal{P}$ remains prime in $F(\mu^{1/p})$, that is

$$_F\Psi_K(\mathcal{P}) = 1[p].$$

(3) If $a+N>1$, and $\mu \not\equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, then $\mathcal{P}$ either remains prime or becomes the pth power of a prime ideal.

Assume $\mathcal{P}$ remains prime. Then $\zeta_p \in F_{\mathcal{P}}$ by Lemma 4.7, and $F_{\mathcal{P}}(\mu^{1/p}) = F_{\mathcal{P}}((\eta')^{1/p})$. But this implies that $\mu = \xi^p \eta'^b$, $(b,p)=1$, by Lemma 4.8. Recall that $\eta' = 1 + g'\pi^{sp^k}$ and $sp^k = a+N$, so $\eta' \equiv 1 \pmod{\mathcal{P}^{a+N}}$, hence we have that $\mu \equiv \xi^p \pmod{\mathcal{P}^{a+N}}$, contrary to assumption. Hence, $\mathcal{P}$ becomes the pth power of a prime ideal in $F(\mu^{1/p})$ and ${}_F\Psi_K(\mathcal{P}) = 1[1]^p$.

(4) If $a=1$ and $N=0$, then $a+N+1=2$ and $\zeta_p \notin F_{\mathcal{P}}$. If $\mu \not\equiv \xi^p \pmod{\mathcal{P}^2}$, then $\mathcal{P}$ either remains prime or becomes the pth power of a prime ideal. But since $\zeta_p \notin F_{\mathcal{P}}$, $\mathcal{P}$ cannot remain prime, so ${}_F\Psi_K(\mathcal{P}) = 1[1]^p$.

Remark. Theorem 4.3 could have been proven without the results in §2. In fact, the proof in Hecke [4, pp. 148–154] generalizes to prove this theorem. However, it is our belief that this proof gives more insight into the theorem and shows why $a+N$ is the natural division between splitting and remaining prime.

We now specialize to $F = \mathcal{Q}$. Of course, the prime ideals correspond to the prime numbers and $\zeta_p \notin \mathcal{Q}_p$ iff $p \neq 2$. Furthermore $a = 1$. So $N=0$ if $p>2$ and $N=1$ if $p=2$.

Corollary 1. *Let* $p=2$, $x^2-\mu$ *irreducible over* $\mathcal{Q}$, $(\mu,2)=1$, *and* $K=\mathcal{Q}(\mu^{1/2})$.

(1) *If* $\mu \equiv \xi^2 \pmod{2^3}$, *then* ${}_F\Psi_K(2) = 2[1]$.

(2) *If* (1) *is not solvable,* $\mu \equiv \xi^2 \pmod{2^2}$, *then* ${}_F\Psi_K(2) = 1[2]$.

(3) *If* $\mu \not\equiv \xi^2 \pmod{2^2}$, *then* ${}_F\Psi_K(2) = 1[1]^2$.

Corollary 2. *Let* $p \neq 2$ *and* $x^p - \mu$ *irreducible over* $\mathcal{Q}$, $(\mu,p)=1$.

(1) *If* $\mu \equiv \xi^p \pmod{p^2}$, *then* $p = \mathcal{P}_1 \cdot \mathcal{P}_2^{p-1}$, *where the degree of* $\mathcal{P}_i$ *is* 1, *for* $i=1,2$. *Furthermore,* $\mathcal{Q}(\mu^{1/p})_{\mathcal{P}_1} = \mathcal{Q}_p$ *and* $\mathcal{Q}(\mu^{1/p})_{\mathcal{P}_2} = \mathcal{Q}_p(\zeta_p)$.

(2) *If* $\mu \not\equiv \xi^p \pmod{p^2}$, *then* $(p) = \mathcal{P}^p$ *in* $\mathcal{Q}(\mu^{1/p})$.

Corollary 1 is well known [**15**, 1955, Chapter 8]. Corollary 2 is not so well known. Dedekind [**2**, page 156] proved this corollary for $p=3$. More recently we found this result in a paper by Westlund [**23**].

References

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
2. R. Dedekind, *Mathematische Werke*, Volumes II & III, Chelsea, New York, 1969.
3. L. Fuchs, *Infinite Abelian Groups*, Vol. 1, Academic Press, New York, 1970.
4. E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, Chelsea, New York, 1970.

5. K. Hensel, *Untersuchung der Zahlen eines Algebraischen Körpers für den Bereich eines beliebigen Primdivisors*, Journal für der Reine und Angdewendente Mathematik, **145** (1914), 92–113.

6. ———, *Die Multiplikative Darstellung der Algebraischen Zahlen für den Bereich eines beliebigen Primteilers*, Journal für der Reine und Angdewendente Mathematik, **146** (1916a), 189–215.

7. ———, *Untersuchung der Zahlen eines Algebraischen Körpers für eine beliebige Primteilerpotenz als Modul*, Journal für der Reine und Angdewendente Mathematik, **146** (1916b), 216–228.

8. ———, *Allgemeine Theorie der Konogruenz Klassen und ihrer Invarianten ain Algebraischen Körpern*, Journal für der Reine und Angdewendente Mathematik, **147** (1917), 1–15.

9. ———, *Über die Zerlegung der Primteiler in relativ zyklischen Körpern, nebst einer Anwendung auf die Kummerschen Körper*, Journal für der Reine und Angdewendente Mathematik, **151** (1920), 112–120.

10. ———, *Die Zerlegung der Primteiler eines beliebigen Zahlkörpers in einem auflösbaren*, Journal für der Reine und Angdewendente Mathematik, Oberkörper, **151** (1921a), 200–209.

11. ———, *Zur multiplikativen Darstellung der Álgebraischen Zahlen für den Bereich eines Primteilers*, Journal für der Reine und Angdewendente Mathematik, **151** (1921b), 210–212.

12. D. Hilbert, *Gesammelte Abhandlungen*, Vol. 1, Chelsea, New York, 1965.

13. M. Ishida, *Some unramified Abelian extensions of algebraic number fields*, Journal für der Reine und Angewendente Mathematik, **268/269** (1974), 165–173.

14. H. B. Mann, *Darstellung der Gruppe der Relativprimen Restklassen nach Primidealpotenz-moduln Durch eine unabhangige Basis*, Thesis, University of Vienna, 1935.

15. ———, *Introduction to Algebraic Number Theory*, The Ohio University Press, Columbus, 1955.

16. H. B. Mann and W. Y. Vélez, *Prime ideal decomposition in $F(\sqrt[m]{\mu})$*, Monatshefte für Mathematiks und Physiks, **81** (1976), 1–8.

17. A. Schinzel, *On linear dependence of roots*, Acta Arithmetica, **27** (1975), 161–175.

18. T. Tagenouchi, *On the classes of congruent integers in an algebraic Korper*, Journal of the College of Science, Tokyo, Imperial University, **36** (1913), 1–28.

19. W. Y. Vélez, *A Basis for the Group of Units Modulo $\mathcal{P}^m$ and Prime Ideal Decomposition in $F(\mu^{1/m})$*, Thesis. University of Arizona, 1975.

20. ———, *A characterization of completely regular fields*, Pacific J. Math., **63** (1976), 553–554.

21. ———, *Prime Ideal Decomposition in $F(\mu^{1/m})$*, II, to appear in Number Theory and Algebra, edited by H. Zassenhaus, Academic Press.

22. E. Weiss, *Algebraic Number Theory*, McGraw-Hill Book Company, Inc., New York, 1963.

23. J. Westlund, *On the fundamental number of the algebraic number field $\mathcal{K}(\sqrt[p]{m})$*, Trans. Amer. Math. Soc., II, (1910), 388–392.

24. H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press, Princeton, 1940.

25. G. Wolf, *Über Gruppen der Reste eines beliegegen Moduls in Algebraischen Zahlkörper*, Thesis, University of Giessen, 1905.

Received November 22, 1976 and in revised form May 16, 1977. The author was supported in part by a Fellowship from the Ford Foundation and by the U. S. Energy, Research, and Development Administration (ERDA). The author is currently at The University of Arizona.

University of Arizona
Tucson, AZ 85721

and

Sandia Laboratories
Albuquerque, NM 87115