S. Williamson
Nagoya Math. J.
Vol. 46 (1972), 97–109

# RAMIFICATION THEORY FOR EXTENSIONS OF DEGREE p. II

SUSAN WILLIAMSON

**Introduction.** Let $k$ denote the quotient field of a complete discrete rank one valuation ring $R$ of unequal characteristic and let $p$ denote the characteristic of $\bar{R}$; assume that $R$ contains a primitive $p^{th}$ root of unity, so that the absolute ramification index $e$ of $R$ is a multiple of $p-1$, and each Gallois extension $K \supset k$ of degree $p$ may be obtained by the adjunction of a $p^{th}$ root.

The purpose of this paper is to assign to each Galois extension $K \supset k$ of degree $p$ an integer $f$ with $-1 \leq f \leq ep/p-1$ from which the ramification-theoretic properties of $K \supset k$ can be determined. Specifically, $f$ shall determine the unramified, wildly ramified, or fiercely ramified character of $K \supset k$, (see Thm. 1.11); moreover, the ramification number $i$ of $K \supset k$ shall have an expression in terms of $f$, (see Prop. 2.1).

Let $U^{(i)}$ for $i \geq 0$ denote the usual filtration on the units of $R$, and let $U^{(-1)}$ denote the set of prime elements of $R$. In a recent publication, ([5]), the author has studied the ramification-theoretic properties of a Galois extension $K \supset k$ of degree $p$ by constructing the integral closure $S$ of $R$ in $K$ from a judiciously chosen element $b$ of $U^{(x)}$ $(-1 \leq x \leq p)$ whose $p^{th}$ root defines $K$. The method for computing $S$ in [5] entails the construction of a chain of $g+1$ ring extensions of $R$ in $S$; the number $g$ is unique for $K \supset k$, satisfies the inequality $0 \leq g \leq (e/p-1)-1$, and is called the conductor number of $K \supset k$.

The present paper makes use of the fact that $R$ is an Eisenstein extension of an unramified complete discrete rank one valuation ring in order to determine an alternate method for the construction of the integral closure $S$. In Section 1 we associate to each Galois extension $K \supset k$ of degree $p$ an integer $f$ with $-1 \leq f \leq ep/p-1$ called its absolute field exponent such that

Received June 2, 1971.

$K$ may be obtained from $k$ by the adjunction of a judiciously chosen element $b$ of $U^{(f)}$. By computing $S$ from such an element $b$ of $R$, we prove the following main result.

THEOREM. *Let $f$ denote the absolute field exponent of a Galois extension $K \supset k$ of degree $p$. Then*

i) *$K \supset k$ is wild if and only if $f$ is relatively prime to $p$*

ii) *$K \supset k$ is fierce if and only if $p$ divides $f$ and $f < ep/p-1$*

iii) *$K \supset k$ is unramified if and only if $f = ep/p-1$.*

In Section 2 we relate the results of the present paper to those of [5]. More specifically, we relate the notions of absolute field exponent and conductor number by computing an expression for the ramification number of $K \supset k$ in terms of the absolute field exponent $f$, and then applying the results of Section 3 of [5].

The author's recent paper and her present paper provide a choice of two significantly different methods for computing the integral closures $S$ of $R$ in a Galois extension $K \supset k$ of degree $p$. Available information concerning an element $b$ whose $p^{th}$ root defines the extension determines the proper choice of method.

The following notation shall be used throughout the paper. The multiplicative group of units of a ring $R$ shall be denoted by $U(R)$; the intermediate ring obtained by adjoining to $R$ an element $t$ of an overring of $R$ shall be denoted by $R[t]$; and, the residue class field of a local ring $R$ shall be denoted by $\bar{R}$.

Unless otherwise stated, $R$ shall always denote a complete discrete rank one valuation ring of unequal characteristic which contains a primitive $p^{th}$ root of unity where $p$ denotes the characteristic of $\bar{R}$, and $S$ shall denote the integral closure of $R$ in a Galois extension $K$ of degree $p$ over the quotient field $k$ of $R$; $\prod$ shall denote a prime element of $R$, $\prod$ a prime element of $S$, and $e$ the absolute ramification index of $R$. The usual filtration on $U(R)$ shall be denoted by $U^{(i)}$ $(i \geq 0)$ and $U^{(-1)}$ shall denote the set of prime elements of $R$.

In [5], the author has defined the quotient field extension of an extension of discrete rank one valuation rings to be fiercely ramified if the residue class field extension has a non-trivial inseparable part. For further details, the reader may refer to [5].

**1. The absolute field exponent.** Throughout this section $K \supset k$ shall always denote a $p^{th}$ root extension, where $k$ is the quotient field of a complete discrete rank one valuation ring $R$ of unequal characteristic containing a primitive $p^{th}$ root of unity and $p$ is the characteristic of $\bar{R}$, and $S$ shall always denote the integral closure of $R$ in $K$. The purpose of this section is to define for each Galois extension $K \supset k$ of degree $p$ an integer $f$ with $-1 \leq f \leq ep/p - 1$ called its absolute field exponent, and to establish a criterion for determining if $K \supset k$ is unramified, wild, or fierce in terms of its absolute field exponent.

In [5], the author has assigned to each such extension $K \supset k$ an integer $x$ with $-1 \leq x \leq p$ called its field exponent; the notions of field exponent and absolute field exponent coincide in the case when $k$ has absolute ramification index $p-1$. We shall make use of results established in [5] in our study of the absolute field exponent.

The first three lemmas concern elements $b$ whose $p^{th}$ roots define the extension $K \supset k$. Lem. 1.1 follows at once from Prop. 1.3 of [5].

LEMMA 1.1. *If $K \supset k$ is a Galois extension of degree $p$, then $K = k(b^{1/p})$ for some element $b$ in $U^{(-1)}$ or in $U^{(0)}$.*

LEMMA 1.2. i) *If $b$ is in $U^{(-1)}$, then $k(b^{1/p}) \supset k$ is wild of degree $p$, and $k(b^{1/p}) \neq k(b_1{}^{1/p})$ for every element $b_1$ of $U^{(0)}$.*

ii) *If $b$ is in $U^{(0)}$, $b_1$ is in $U^{(1)}$, and $k(b^{1/p}) = k(b_1{}^{1/p})$, then $\bar{b}$ has a $p^{th}$ root in $\bar{R}$.*

iii) *If $b$ is in $U^{(0)}$ and $X^p - \bar{b}$ is irreducible over $\bar{R}$, then $k(b^{1/p}) \supset k$ is fierce of degree $p$.*

*Proof.* If $b$ is in $U^{(-1)}$ then $b^{1/p}$ is a root of an Eisenstein polynomial of degree $p$, from which it follows that $K \supset k$ is wild of degree $p$. If $b$ is in $U^{(0)}$ and $X^p - \bar{b}$ is irreducible over $\bar{R}$, then $\bar{S} \supset \bar{R}$ is purely inseparable of degree $p$. The remaining assertions are restatements of parts ii) and iii) of Lem. 1.5 of [5].

*Remark* 1.3. If $b$ is in $U^{(-1)}$, then the integral closure $S$ of $R$ in $k(b^{1/p})$ is $S = R[b^{1/p}]$. If $b$ is in $U^{(0)}$ and $X^p - \bar{b}$ is irreducible over $\bar{R}$, then the integral closure $S$ of $R$ in $k(b^{1/p})$ is $S = R[b^{1/p}]$.

The above expressions for the integral closure have been established in

Prop. 2.6 *A* of [5]; we shall make use of them in our study of the ramification number of $K \supset k$ in Section 2.

Lemma 1.6 pertains to extensions $K \supset k$ of degree $p$ obtained by the adjunction of a $p^{th}$ root of an element $b$ of $R$ present in $U^{(1)}$. Recall that the complete discrete rank one valuation ring $R$ is an Eisenstein extension of an unramified complete discrete rank one valuation ring $R_0$ (see Thm. 31.12 p. 111 of [3]). Let $e$ denote the ramification index of the totally ramified extension $R \supset R_0$; then $R = R_0[\pi]$ where $\pi$ denotes a prime element of $R$, $\{1, \pi, \cdots, \pi^{e-1}\}$ is a free basis for $R$ over $R_0$, $\pi^e R = pR$, and $\bar{R} = \bar{R}_0$, (see Thm. 1 p. 23 of [2]). Moreover, $e$ is the absolute ramification index of $R$.

Facts 1.4 and 1.5 shall be used in the proof of Lem. 1.6.

FACT 1.4. *If $b_1$ and $b_2$ are elements of $U(R)$ such that $b_1 \equiv b_2 \bmod \pi^{(ep/p-1)+1}R$, then $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$.*

*Proof.* Since $b_1$ and $b_2$ are in $U(R)$, the congruence $b_1 \equiv b_2 \bmod \pi^{(ep/p-1)+1}R$ implies that $b_1/b_2 \equiv 1 \bmod \pi^{(ep/p-1)+1}R$, from which it follows that $b_1/b_2$ has a $p^{th}$ root in $R$ according to Lem. 1.2 of [5]. The fact that $b_1$ and $b_2$ differ multiplicatively by a $p^{th}$ power from $k$ implies that $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$.

FACT 1.5. *If $b$ is an element of $R$, then there exists an element $c$ of $R$ of the form $c = \sum y_i \pi^i$ $(0 \leq i \leq ep/p-1)$ with each $y_i$ in $U(R_0) \cup \{0\}$ which satisfies the congruence $c \equiv b \bmod \pi^{(ep/p-1)+1}R$. If $b$ is in $U^{(1)}$, then $c$ may be chosen so that $y_0 = 1$.*

*Proof.* Since $\{1, \pi, \cdots, \pi^{e-1}\}$ is an $R_0$-module basis for $R$, the element $b$ may be written in the form $b = \sum b_i \pi^i$ $(0 \leq i \leq e-1)$ with each $b_i$ in $R_0$. If each $b_i$ is in $U(R_0) \cup \{0\}$, then $c = b$ satisfies the assertion. Otherwise, we may consider the least positive integer $h$ such that $b_h$ is not in $U(R_0) \cup \{0\}$. Since $b_h$ is in $pR_0$, the element $b$ satisfies the congruence $b \equiv \sum b_i \pi^i \bmod \pi^{h+1}R$ $(0 \leq i \leq h-1)$; we may consider therefore an element $\tilde{b}$ of $R$ of the form $\tilde{b} = \sum \tilde{b}_i \pi^i$ $(0 \leq i \leq ep/p-1)$ with each $\tilde{b}_i$ in $R_0$, $\tilde{b}_i = b_i$ for $0 \leq i \leq h-1$, and $\tilde{b}_h = 0$, which satisfies the congruence $\tilde{b} \equiv b \bmod \pi^{(ep/p-1)+1}R$. If each $\tilde{b}_i$ is in $U(R_0) \cup \{0\}$ for $0 \leq i \leq ep/p-1$, then $c = \tilde{b}$ satisfies the assertion. Otherwise, we may consider the least positive integer $m$ such that $\tilde{b}_m$ is not in $U(R_0) \cup \{0\}$. Observe that $h < m$, so that by proceeding in this way we may obtain, after finitely many steps, an element which $c$ satisfies the statement of our assertion.

If $b$ is in $U^{(1)}$, then $b = 1 + r\pi$ for some element $r$ of $R$. By applying the first part of this fact to $r$, we may produce an element $c$ of the desired form which satisfies the congruence $c \equiv b \bmod \pi^{(ep/p-1)+1}R$.

LEMMA 1.6. *Assume the notation introduced above. Let $K \supset k$ be an extension of degree $p$ defined by $K = k(b^{1/p})$ for some element $b$ of $U^{(1)}$. Then $K = k(b_1{}^{1/p})$ for some element $b_1$ of $U^{(1)}$ of the form $b_1 = 1 + \sum x_i\pi^i$ $(1 \leq i \leq ep/p-1)$ where the $x_i$ are elements of $R_0$ such that*

i) *each $x_i$ is in $U(R_0) \cup \{0\}$, and the $x_i$ are not all zero*

ii) *$X^p - \bar{x}_i$ is irreducible over $\bar{R}_0$ for each $i$ divisible by $p$ such that $i < ep/p-1$ and $x_i \neq 0$.*

*Proof.* By combining Facts 1.4 and 1.5 we may consider an element $c$ of $R$ of the form $c = 1 + \sum y_i\pi^i$ $(1 \leq i \leq ep/p-1)$ with the $y_i$ in $U(R_0) \cup \{0\}$ such that $k(c^{1/p}) = k(b^{1/p})$. Observe that the $y_i$ are not all zero; for if $y_i = 0$ for each $i$, then $k(c^{1/p}) = k$, which contradicts the assumption that $K \supset k$ has degree $p$. If $X^p - \bar{y}_i$ is irreducible over $\bar{R}_0$ for every $i$ divisible by $p$ and less than $ep/p-1$ for which $y_i \neq 0$, then $b_1 = c$ satisfies the assertion of this lemma.

Otherwise, we may consider the least positive integer $h$ divisible by $p$, less than $ep/p-1$, for which $y_h \neq 0$ and $X^p - \bar{y}_h$ is reducible over $\bar{R}_0$. We proceed to show that $c$ can be replaced by an element $c_1$ of $U^{(1)}$ of the form $c_1 = \sum \gamma_i\pi^i$ $(1 \leq i \leq ep/p-1)$, where the $\gamma_i$ are in $U(R_0) \cup \{0\}$ and are not all zero, such that for every $i \leq h$ divisible by $p$ for which $\gamma_i \neq 0$, the polynomial $X^p - \bar{\gamma}_i$ is irreducible over $\bar{R}_0$. Since $X^p - \bar{y}_h$ is reducible over $\bar{R}_0$, we may consider an element $y$ of $R_0$ such that $\bar{y}^p = \bar{y}_h$, i.e. such that $y^p \equiv y_h \bmod pR$. Define the element $\tilde{c}$ of $R$ by $\tilde{c} = c(1 - y\pi^{h/p})^p$, and observe that $k(\tilde{c}^{1/p}) \equiv k(c^{1/p})$ because $\tilde{c}$ and $c$ differ multiplicatively by a $p^{th}$ power from $k$. By expanding $(1 - y\pi^{h/p})^p$ according to the binomial theorem, we obtain the congruence $\tilde{c} \equiv c(1 - y^p\pi^h) \bmod \pi^{e+(h/p)}R$ since $pR = \pi^eR$. It is easy to verify that $h + 1 \leq e + h/p$ if and only if $h < ep/p-1$. Therefore the fact that $h < ep/p-1$ now implies that $\tilde{c} \equiv c - y^p\pi^h \bmod \pi^{h+1}R$, because $c$ is in $U^{(1)}$. Since $c = 1 + \sum y_i\pi^i$ $(1 \leq i \leq ep/p-1)$ and $y^p = y_h \bmod pR$, it now follows that $\tilde{c} \equiv 1 + \sum y_i\pi^i + (y_h - y^p)\pi^h \bmod \pi^{h+1}R$ $(1 \leq i \leq h-1) \equiv 1 + \sum y_i\pi^i \bmod \pi^{h+1}R$ $(1 \leq i \leq h-1)$. Now we may define he desired element $c_1$. According to the preceeding congruences we may write $\tilde{c}$ in the form $\tilde{c} = 1 + \sum \gamma_1\pi^i + r\pi^{h+1}$ $(1 \leq i \leq h)$ for some element $r$ of $R$, where $\gamma_i = y_i$

$(1 \leq i \leq h-1)$ and $\gamma_h = 0$. An application of Fact 1.5 yields the existence of an element of the form $\sum \gamma_i \pi^i$ $(h+1 \leq i \leq ep/p-1)$ with the $\gamma_i$ in $U(R_0) \cup \{0\}$ which satisfies the congruence $\sum_{i=h+1}^{ep/p-1} \gamma_i \pi^i \equiv r\pi^{h+1} \bmod \pi^{(ep/p-1)+1}R$. Define the element $c_1$ of $U^{(1)}$ by $c_1 = 1 + \sum \gamma_i \pi^i$ $(1 \leq i \leq ep/p-1)$. Observe that $c_1 = \tilde{c} \bmod \pi^{(ep/p-1)+1}R$, so that $K = k(c_1^{1/p})$ according to Fact 1.4 because $K = k(\tilde{c}^{1/p})$. Since $\gamma_h = 0$ and $\gamma_i = y_i$ for $1 \leq i \leq h-1$, it is true that the polynomial $X^p - \bar{\gamma}_i$ is irreducible over $\bar{R}_0$ for each $i$ $(1 \leq i \leq h)$ divisible by $p$ such that $\gamma_i \neq 0$. An argument similar to the one at the beginning of the proof shows that the elements $\gamma_i$ $(1 \leq i \leq ep/p-1)$ are not all zero. If $X^p - \bar{\gamma}_i$ is irreducible over $\bar{R}_0$ for every $i < ep/p-1$ which is divisible by $p$ and for which $\gamma_i \neq 0$, then $b_1 = c_1$ satisfies the assertion of this lemma.

Otherwise, we may consider the least positive integer $m$ less than $ep/p-1$ and divisible by $p$ such that $\gamma_m \neq 0$ and $X^p - \bar{\gamma}_m$ is reducible over $\bar{R}_0$; observe that $h < m$. By means of the same technique used above to produce $c_1$ from $c$, we may produce an element $c_2$ of $U^{(1)}$ of the form $c_2 = 1 + \sum \delta_i \pi^i$ $(1 \leq i \leq ep/p-1)$ such that $k(c_2^{1/p}) = k(c_1^{1/p})$, where the $\delta_i$ are in $U(R_0) \cup \{0\}$ and are not all zero, and the polynomials $X^p - \bar{\delta}_i$ are irreducible over $\bar{R}_0$ for every $i \leq m$ divisible by $p$ for which $\delta_i \neq 0$.

It follows from the inequality $h < m$, that by proceeding in this way we may finally obtain an element $b_1$ of $U^{(1)}$ which satisfies the assertion of this lemma.

Definition. An element $b$ of $U^{(1)}$ of the form $b = 1 + \sum x_i \pi^i$ $(1 \leq i \leq ep/p-1)$ with the $x_i$ in $R_0$ is said to be in *normal form* if the $x_i$ satisfy statements i) and ii) of Lem. 1.6.

The usefulness of Lem. 1.6 for the definition of the absolute field exponent motivates its name.

The following proposition concerning elements of $U^{(1)}$ shall be used to establish the main result (Thm. 1.11); its corollary (Lem. 1.9) shall be used to establish the uniqueness of the absolute field exponent in Prop. 1.10.

Proposition 1.7. *Let $b = 1 + \sum x_i \pi^i$ $(1 \leq i \leq ep/p-1)$ denote an element of $U^{(1)}$ in normal form, and let $f$ denote the least integer for which $x_f \neq 0$; let $K = k(b^{1/p})$. Then*

i) *$K \supset k$ is wild of degree $p$ if and only if $f$ is relatively prime to $p$*

ii) *$K \supset k$ is fierce of degree $p$ if and only if $p$ divides $f$ and $f < ep/p-1$*

iii) *$K \supset k$ is unramified if and only if $f = ep/p-1$. Moreover, $K \supset k$ is*

https://doi.org/10.1017/S0027763000014793 Published online by Cambridge University Press

*unramified of degree* $p$ *if and only if* $f = ep/p-1$ *and the polynomial* $X^p + \bar{v}X - \bar{x}_f$ *is irreducible over* $\bar{R}_0$, *where* $v$ *is the element of* $U(R)$ *defined by* $v\pi^e = p$.

*Proof.* Recall (see Prop. 1.1 of [5]) that a $p^{th}$ root $\beta$ of an element $b$ of $U^{(1)}$ satisfies an equality of the form $(\beta-1)^p = (b-1) + uv\pi^e(\beta-1)$ where $u$ is an element of the $R$-module $R(1, \beta, \cdots, \beta^{p-2})$ which satisfies the congruence $u \equiv -1 \bmod (p, \beta-1)R[\beta]$, and $v$ is the element of $U(R)$ defined by $v\pi^e = p$. The proceeding equality shall be used for establishing the asserted relationships between $f$ and the ramification-theoretic character of $K \supset k$.

First we shall prove that if $f$ is relatively prime to $p$, then $K \supset k$ is wild of degree $p$ by constructing a prime element $\prod$ of the integral closure $S$ of $R$ in $K$. By applying the division algorithm to $f$ and $p$ we may obtain (unique) integers $q$ and $t$ such that $f = qp + t$ where $0 \leq t < p$. Observe that $q \geq 0$ because $f \geq 1$, and that $0 < t$ because $(f, p) = 1$. The element $\theta$ of $K$ defined by $\theta = (\beta-1)\pi^q$ shall be useful for constructing $\prod$. We proceed to show that $\theta$ is a non-unit of $S$ and that $\theta^p$ is in $\pi^t U(S)$. Consider the element $x$ of $U(R)$ defined by $b - 1 = x\pi^f$. The definition of $\theta$ and the equality $(\beta-1)^p = (b-1) + uv\pi^e(\beta-1)$ yield the equality $\theta^p = x\pi^t + uv^{e-qp+q}\theta$ by an easy computation. Observe that $e - qp + q \geq 1$. For, $e - qp + q \geq 1$ if and only if $q < e/p-1$, which holds if and only if $qp < ep/p-1$; therefore the inequalities $qp < f < ep/p-1$ imply that $e - qp + q \geq 1$. The above expression for $\theta^p$ now shows that $\theta$ satisfies a monic polynomial with coefficients in $S$, from which it follows that $\theta$ is itself in $S$. Observe moreover that $\theta$ is a non-unit of $S$ because $t \geq 1$ and $e - qp + q \geq 1$. In order to show that $\theta^p$ is in $\pi^t U(S)$, it sufficies to show that $e - qp + q \geq t$ since $\theta$ is a non-unit of $S$. Now $e - qp + q \geq t$ if and only if $f \leq e + q$ if and only if $fp \leq ep + f - t$ if and only if $f \leq (ep/p-1) - t/p-1$. Since $0 < t/p-1 \leq 1$, we now have that $t \leq e - qp + q$ if and only if $f \leq (ep/p-1) - 1$ if and only if $f < ep/p-1$. The assumption that $(f, p) = 1$ guarantees that $f < ep/p-1$, and so we may conclude at last that $t \leq e - qp + q$. The equality $\theta^p = x\pi^t + uv\pi^{e-qp+q}\theta$, together with the inequality $e - qp + q \geq t$ and the fact that $\theta$ is a non-unit, now implies that $\theta^p$ is in $\pi^t U(S)$ because $x$ is in $U(R)$. Now we may show that $K \supset k$ is wild of degree $p$ by showing that $K \supset k$ has ramification index $p$. Since we have assumed that $f$ and $p$ are relatively prime, we may consider integers $m$ and $n$ such that $mp + nt = 1$. An easy computation shows that the element $\prod$ of $K$ defined by $\prod = \theta^n\pi^m$ has the property that $\prod^p$ is in $\pi U(S)$, from which it follows that $\Pi$ is an element of $S$, that $K \supset k$ has ramification index $p$, and that $K \supset k$ is wild of degree $p$.

The next step is to show that if $f$ is divisible by $p$ and less than $ep/p-1$, then $K \supset k$ is fiercely ramified of degree $p$. Consider the element $\theta$ of $K$ defined by $\theta = (\beta - 1)/\pi^q$ where $q = f/p$, and observe that $1 \leq q < e/p - 1$. In order to prove the assertion we shall show that $\theta$ is an element of $S$ with the property that $\bar{R}(\bar{\theta}) \supset \bar{R}$ is purely inseparable of degree $p$. Let $x$ denote the element of $U(R)$ defined by $b - 1 = x\pi^f$ and observe that $\bar{x} = \bar{x}_f$. The equality $(\beta - 1)^p = (b - 1) + uv\pi^e(\beta - 1)$ (see the beginning of the proof) together with the definition of $\theta$ implies that $\theta^p = x + uv\pi^{e-qp+q}\theta$, where $e - pq + q > 0$ because $q < e/p - 1$; therefore $\theta$ is in $S$ because it satisfies a monic polynomial equation with coefficients in $S$. Since $b$ is in normal form by assumption, the fact that $p$ divides $f$ implies that $X^p - \bar{x}_f$ is irreducible over $\bar{R}_0 = \bar{R}$. Therefore $\bar{R}(\bar{\theta}) \supset \bar{R}$ is purely inseparable of degree $p$ because $\bar{\theta}^p = \bar{x} = \bar{x}_f$. We may now conclude that $\bar{S} = \bar{R}(\bar{\theta})$ and that $K \supset k$ is fierce of degree $p$. (Moreover, $S = R[\theta]$ according to part iii) of Lem. 2.4 of [5].)

We show finally that if $f = ep/p - 1$ then $K \supset k$ is unramified and we establish necessary and sufficient conditions for $K \supset k$ to have degree $p$. Consider the element $\theta$ defined by $\theta = (\beta - 1)/\pi^{e/p-1}$ and observe that $K = k(\theta)$. We shall show that $\theta$ is in $S$, and that $\bar{S} = \bar{R}(\bar{\theta})$ with $\bar{\theta}$ separable over $\bar{R}$. For convenience of notation let $x = x_f = x_{ep/p-1}$. Then the definition of $\theta$ together with the equality $(\beta - 1)^p = (b - 1) + uv\pi^e(\beta - 1)$ (see the beginning of the proof) implies that $\theta^p = x + uv\theta$. It follows from the definition of $\theta$ together with the fact that $u$ is in the $R$-module $R(1, \beta, \cdots, \beta^{p-2})$ that $u$ is in $R(1, \theta, \cdots, \theta^{p-2})$; therefore, the equality $\theta^p - uv\theta - x = 0$ gives rise to a monic polynomial $f(X)$ in $R[X]$ having $\theta$ as a root, from which it follows that $\theta$ is in $S$. Observe that $\bar{f}(X) = X^p + \bar{v}X - \bar{x}$ in $\bar{R}[X]$ because $\bar{u} = -\bar{1}$, and that $\bar{f}(X)$ is a separable polynomial because $\bar{f}'(X) = \bar{v} \neq \bar{0}$. We proceed to show that $[K : k] = p$ if and only if $\bar{f}(X)$ is irreducible over $\bar{R} = \bar{R}_0$, and that $K = k$ otherwise. If $\bar{f}(X)$ is reducible over $\bar{R}$, then $f(X)$ is reducible over $R$ by Hensel's lemma because $R$ is complete and $\bar{f}(X)$ is separable; the reducibility of $f(X)$ over $R$ implies that $\deg_k\theta < p$ from which it follows that $\beta$ is in $k$ and that $K = k$. If, on the other hand, $\bar{f}(X)$ is irreducible over $\bar{R}$, then the separability of $\bar{f}(X)$ implies that $K \supset k$ is unramified of degree $p$ (with $\bar{S} = \bar{R}(\bar{\theta})$ and $S = R[\theta]$) according to Prop. 1 p. 25 of [2].

The above observations combine to establish the truthfulness of the proposition.

Observe that the equation $X^p + \bar{v}X - \bar{x} = \bar{0}$ of Prop. 1.7 is essentially an Artin-Schreier equation (see p. 80 of [4]). For, consider the elements $v$, $v_1$, and $v_0$ defined by $v\pi^e = p$, $v_1\pi^{e/p-1} = \zeta - 1$, and $v_0(\zeta - 1)^{p-1} = p$ where $\zeta$ denotes as usual a primitive $p^{th}$ root of unity. An easy computation shows that $v = v_1^{p-1}v_0$, so that $\bar{v} = -\bar{v}_1^{p-1}$ because $\bar{v}_0 = -\bar{1}$ (see p. 158 of [1]). The change of variable $Y = X/\bar{v}_1$ yields the Artin-Schreier equation $Y^p - Y - \bar{x}/\bar{v}_1{}^p = \bar{0}$.

The following expressions for the integral closure $S$ of $R$ in $K$ follow at once from the proof of Prop. 1.7.

*Remark* 1.8. Let $b = 1 + \sum x_i\pi^i$ denote an element of $U^{(f)} - U^{(f+1)}$ $(1 \leq f \leq ep/p - 1)$ in normal form. Consider the unique integers $q$ and $t$ for which $f = qp + t$ with $0 \leq t < p$, and define $\theta = (\beta - 1)/\pi^q$.

i) If $f$ is relatively prime to $p$, then $S = R[\Pi]$ where $\Pi = \theta^n\pi^m$ for integers $m$ and $n$ satisfying $mp + nt = 1$.

ii) If $p$ divides $f$, then $S = R[\theta]$.

LEMMA 1.9. *Consider elements $b_1$ and $b_2$ of $U^{(1)}$ in normal form, where $b_1$ is in $U^{(f_1)} - U^{(f_1+1)}$ and $b_2$ is in $U^{(f_2)} - U^{(f_2+1)}$. If $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$, then $f_1 = f_2$.*

*Proof.* Since $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$ by hypothesis, an application of Prop. 1.7 shows that $f_1$ and $f_2$ are both relatively prime to $p$, are both divisible by $p$ and less than $ep/p - 1$, or are both equal to $ep/p - 1$.

Consider an equality $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$ with $f_1$ and $f_2$ relatively prime to $p$. We shall show that $f_1 = f_2$ by contradiction. Assume that $f_1 < f_2$. Since $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$, we may consider an element $c$ of $k$ such that $b_1 = c^p b_2{}^n$ for some integer $n$ relatively prime to $p$, (see Lem. 3 p. 90 of [2]). Observe that $c^p$ is in $U^{(f_1)} - U^{(f_1+1)}$ because $b_1$ is in $U^{(f_1)} - U^{(f_1+1)}$, $b_2^n$ is in $U^{(f_2)}$, and $f_1 < f_2$, so that $k(c) \supset k$ is wild of degree $p$ according to Prop. 1.7. This contradiction shows that $f_1 = f_2$.

Now consider an equality $k(b_1{}^{1/p}) = k(b_2{}^{1/p})$ with $f_1$ and $f_2$ divisible by $p$ and less than $ep/p - 1$, and assume that $f_1 < f_2$. Once again we consider an element $c$ in $k$ such that $b_1 = c^p b_2{}^n$ for some integer $n$ relatively prime to $p$. Since $b_2^n$ is in $U^{(f_2)}$, we have that $c^p \equiv b_1 \bmod \pi^{f_2}R$ from which it follows that $c^p$ is of the form $c^p = 1 + y\pi^{f_1}$ with $\bar{y} = \bar{x}_{f_1}$ because $f_1 < f_2$.

https://doi.org/10.1017/S0027763000014793 Published online by Cambridge University Press

The irreducibility of $X^p - \bar{y}$ over $\bar{R}$ now implies that $k(c) \supset k$ is fierce of degree $p$ by Prop. 1.7. This contradiction shows that $f_1 = f_2$, and this completes the proof.

The following proposition follows at once from the four lemmas established above.

PROPOSITION 1.10. *Let $k$ denote the quotient field of a complete discrete rank one valuation ring $R$ containing a primitive $p^{th}$ root of unity, where $p = \mathrm{char}\,\bar{R}$, and consider a Galois extension $K \supset k$ of degree $p$. Then there exists a unique integer $f$ $(-1 \leq f \leq ep/p - 1)$ such that $K \supset k$ is one of the following forms:*

i) *$K = k(b^{1/p})$ for some element $b$ of $U^{(f)}$ with $f = -1$*

ii) *$K = k(b^{1/p})$ for some element $b$ of $U^{(f)}$ with $f = 0$ for which $X^p - \bar{b}$ is irreducible over $\bar{R}$*

iii) *$K = k(b^{1/p})$ for some element $b$ of $U^{(f)} - U^{(f+1)}$ in normal form, (where $1 \leq f \leq ep/p - 1$).*

DEFINITION. The unique integer $f$ satisfying $-1 \leq f \leq ep/p - 1$ defined for each Galois extension $K \supset k$ of degree $p$ by Prop. 1.10 is called the *absolute field exponent* of $K \supset k$ and is denoted by $f(K/k)$.

The following theorem has now been established.

THEOREM 1.11. *Let $f = f(K/k)$ denote the absolute field exponent of a Galois extension $K \supset k$ of degree $p$. Then*

i) *$K \supset k$ is wildly ramified if and only if $f$ is relatively prime to $p$*

ii) *$K \supset k$ is fiercely ramified if and only if $p$ divides $f$ and $f < ep/p - 1$*

iii) *$K \supset k$ is unramified if and only if $f = ep/p - 1$.*

We terminate this section with some observations concerning the relationship between the field exponent $x = x(K/k)$ (see Section 1 of [5]) and the absolute field exponent $f = f(K/k)$ of a Galois extension $K \supset k$ of degree $p$. These observations follow at once from the definitions of $x$ and $f$. Recall that $-1 \leq x \leq p$ and that $-1 \leq f \leq ep/p - 1$.

*Remark* 1.12. Let $x$ denote the field exponent and $f$ the absolute field exponent of a Galois extension $K \supset k$ of degree $p$.

i) If $e = p - 1$, then $x = f$.

ii) If $-1 \leq f \leq p$, then $x = f$.

https://doi.org/10.1017/S0027763000014793 Published online by Cambridge University Press

iii) If $-1 \leq x \leq p-1$, then $x = f$.

**2. The ramification number, the absolute field exponent, and the conductor number.** As usual, $K \supset k$ denotes a Galois extension of degree $p$ where $k$ is the quotient field of a complete discrete rank one valuation ring $R$ which contains a primitive $p^{th}$ root of unity and whose residue class field has characteristic $p$. In Section 2 of [5], the author has assigned to each such extension $K \supset k$ an integer $g$ with $0 \leq g \leq (e/p-1)-1$ called the conductor number of $K \supset k$. Prop. 3.1 of [5] presents expressions for the ramification number $i$ of $K \supset k$ in terms of its conductor number $g$.

The purpose of this section is to determine the relationships between the absolute field exponent of an extension and its ramification and conductor numbers.

PROPOSITION 2.1. *Let $f$ denote the absolute field exponent of a Galois extension $K \supset k$ of degree $p$, and let $i$ denote the ramification number of $K \supset k$.*

i) *If $f = -1$, then $i = ep/p-1$.*

ii) *If $p$ divides $f$, then $i = (e/p-1) - f/p - 1$.*

iii) *If $f > 0$ and $(f, p) = 1$, then $i = (ep/p-1) - f$.*

*Proof.* Let $x = x(K/k)$ denote the field exponent of $K \supset k$ (see Section 1 of [5]). If $f = -1$, then $x = -1$ (see Remark 1.12). According to part ii) of Prop. 3.1 of [5], $i = ep/p-1$ when $x = -1$, and this proves statement i). (Or, the reader may refer to Exer. 4 p. 79 of [4]).

To prove statement ii) we first consider the case when $p$ divides $f$ and $f < ep/p-1$; in this case $K \supset k$ is fierce and the integral closure $S$ of $R$ in $K$ is given by $S = R[\theta]$ where $\theta = (\beta-1)/\pi^q$ and $q = f/p$ (see Prop. 1.7 and Remark 1.8). Consider some primitive $p^{th}$ root of unity $\zeta$ and let $\sigma$ denote the element of the Galois group $G(K/k)$ defined by $\sigma(\beta) = \zeta\beta$; observe that $\sigma$ is in the $i^{th}$ ramification group $G_i$ of $K \supset k$ if and only if $\sigma(\theta) \equiv \theta \bmod \pi^{i+1}S$. An easy computation shows that $\sigma((\beta-1)/\pi^q) \equiv (\beta-1)/\pi^q \bmod \pi^{i+1}S$ if and only if the element $\zeta - 1$ is in $\pi^{i+q+1}S$, which in turn holds if and only if $\pi^{e/p-1}$ is in $\pi^{i+q+1}S$ because $\zeta - 1$ is in $\pi^{e/p-1}U(S)$. The fact that $\pi^{e/p-1}$ is in $\pi^{i+q+1}S$ if and only if $i \leq (e/p-1) - q - 1$ shows that $\sigma$ is in $G_i$ if and only if $i \leq (e/p-1) - q - 1$.

In the case when $f = ep/p-1$, the extension $K \supset k$ is unramified according to Prop. 1.7. It is well known that the ramification number of an unramified extension is $-1$. The observation that $(e/p-1)-f/p-1=-1$ when $f=ep/p-1$ completes the proof of statement ii).

In the case when $f>0$ and $(f,p)=1$, the extension $K\supset k$ is wild according to Prop. 1.7. Let $\theta=(\beta-1)/\pi^q$ where $q$ is defined by $f=qp+t$ with $0\leq t<p$. Recall (Remark 1.8) that the integral closure $S$ of $R$ in $K$ is given by $S=R[\Pi]$ where $\Pi=\theta^n\pi^m$ for integers $m$ and $n$ satisfying $mp+nt=1$. Once again let $\zeta$ denote a primitive $p^{th}$ root of unity and $\sigma$ the element of $G(K/k)$ for which $\sigma(\beta)=\zeta\beta$. Observe that $\sigma$ is in the $i^{th}$ ramification group $G_i$ of $K\supset k$ if and only if $\sigma(\Pi)/\Pi\equiv 1 \bmod \Pi^i S$. By substituting $((\beta-1)/\pi^q)^n\pi^m$ for $\Pi$ one can obtain the equality $\sigma(\Pi)/\Pi=(\sigma(\beta-1)/(\beta-1))^n$, so that $\sigma$ is in $G_i$ if and only if $(\sigma(\beta-1)/(\beta-1))^n\equiv 1 \bmod \Pi^i S$. We proceed to show that $(\sigma(\beta-1)/(\beta-1))^n-1$ is in $\Pi^{(ep/p-1)-f}U(S)$. First observe that $\beta-1$ is in $\Pi^f U(S)$. For, $\theta$ is in $\Pi^t U(S)$ because $\theta^p$ is in $\pi^t U(S)$, (see paragraph two of the proof of Prop. 1.7), and so the definition $\beta-1=\theta\pi^q$ implies that $\beta-1$ is in $\Pi^{qp+t}U(S)=\Pi^f U(S)$. Since $\sigma(\beta-1)-(\beta-1)$ is in $\Pi^{ep/p-1}U(S)$ and $\beta-1$ is in $\Pi^f U(S)$, we have that $\sigma(\beta-1)/(\beta-1)-1$ is in $\Pi^{(ep/p-1)-f}U(S)$. Therefore $(\sigma(\beta-1)/(\beta-1))^n-1$ is in $\Pi^{(ep/p-1)-f}U(S)$ because $n$ is relatively prime to $p$. The above observations combine to give us that $\sigma$ is in $G_i$ if and only if $\Pi^{(ep/p-1)-f}$ is in $\Pi^i S$, i.e. $\sigma$ is in $G_i$ if and only if $i\leq(ep/p-1)-f$, and this completes the proof of part iii).

It remains to study the relationship between the absolute field exponent $f$ and the conductor number $g$. For this the following definition is useful.

DEFINITION. Let $f$ denote the absolute field exponent of a Galois extension $K\supset k$ of degree $p$. If $f\geq 0$, then the *quotient number* $q$ and the *remainder number* $t$ of $K\supset k$ are the unique integers $q$ and $t$ such that $f=qp+t$ with $0\leq t<p$; if $f=-1$, we define $q=0$ and $t=1$.

PROPOSITION 2.2. *Let $q$ denote quotient number and $g$ the conductor number of a Galois extension $K\supset k$ of degree $p$. If $K\supset k$ is unramified then $q=g+1$. Otherwise, $q=g$.*

*Proof.* If $K\supset k$ is unramified, then $f=ep/p-1$ (Thm. 1.11) and so $q=e/p-1$. On the other hand, $g=(e/p-1)-1$ (Cor. 2.7 of [5]); therefore $q=e/p-1=g+1$ in the unramified case.

We shall make use of Prop. 2.1 to prove that $q=g$ when $K\supset k$ is fiercely ramified or wildly ramified.

If $K\supset k$ is fierce, then the ramification number $i$ of $K\supset k$ is given on the one hand by $i = (e/p - 1) - q - 1$ (Prop. 2.1), and on the other hand by $i = (e/p - 1) - g - 1$ (Prop. 3.1 of [5]), from which it follows that $q = g$.

Now let $x$ denote the field exponent of a wildly ramified extension $K \supset k$. If $f = -1$, then $q = 0 = g$. For, $x = -1$ when $f = -1$ (Remark 1.12) so that $g = 0$ (see p. 155 of [5]); and $q = 0$ when $f = -1$ according to the above definition of $q$. If $f \neq -1$, then $i = (ep/p - 1) - f$ by Prop. 2.1; and, the fact that $x \neq -1$ when $f \neq -1$ (Remark 1.12) implies that $i = (ep/p - 1) - gp - h$ where $1 \leq h \leq p - 1$ (Prop. 3.1 of [5]). The equalities $i = (ep/p - 1) - qp - t$ and $i = (ep/p - 1) - gp - h$ together with the inequalities $1 \leq h, t \leq p - 1$ imply that $q = g$ (and $h = t$).

## References

[1] E. Artin and J. Tate, *Class field theory*, Benjamin, (1967).
[2] J.W.S. Cassels and A. Frolich, *Algebraic Number Theory*, Thompson, (1967).
[3] M. Nagata, *Local Rings*, Wiley, (1962).
[4] J.-P. Serre, *Corps Locaux*, Paris, Hermann, (1962).
[5] S. Williamson, *Ramification theory for extensions of degree p*, Nagoya Math. J. Vol. **41** (1971), pp. 149–168.

*Regis College*
*Weston, Massachusetts*