Susan Williamson
Nagoya Math. J.
Vol. 41 (1971), 149–168

RAMIFICATION THEORY FOR EXTENSIONS OF DEGREE p

SUSAN WILLIAMSON

Introduction. The notions of tame and wild ramification lead us to make the following definition.

DEFINITION. *The quotient field extension of an extension of discrete rank one valuation rings is said to be fiercely ramified if the residue class field extension has a nontrivial inseparable part.*

The purpose of this paper is to study ramification in Galois extensions $K \supset k$ of degree p. The ground field k is the quotient field of a complete discrete rank one valuation ring R of unequal characteristic, and p denotes the characteristic of $\bar{R}$. Assume furthermore that R contains a primitive p^{th} root of unity, from which it follows that the absolute ramification index a of R is divisible by $p-1$.

Observe that a Galois extension of degree p may be unramified, wild, or fierce. In order to study the properties of such an extension relative to ramification we established a technique for computing the integral closure S of R in K.

The computation of S is facilitated by a judicious choice of the element of k whose p^{th} root defines the extension. Let $U^{(i)}$ for $i \geq 0$ denote the usual filtration on $U(R)$, and let $U^{(-1)}$ denote the set of prime elements of R. In Section 1 we associate to each Galois extension $K \supset k$ of degree p an integer x with $-1 \leq x \leq p$ called the *field exponent* of the extension such that $K = k(b^{1/p})$ for some element b of $U^{(x)}$ (see Prop. 1.6).

The ring $R[b^{1/p}]$ where b is in $U^{(x)}$ is contained in the integral closure S, but equality need not hold. In Section 2 we present a technique for computing S which entails the construction of a chain (S_i) with $0 \leq i \leq g$ of simple ring extensions S_i of R where $S_0 = R[b^{1/p}]$, $S_{i-1} \subset S_i$, and $S_g \subseteq S$. The integer g satisfies the inequality $0 \leq g \leq (a/p-1)-1$ and is called the

Received, April 21 1969.

conductor number of $K \supset k$. By examining the terminal ring S_g of the chain one can determine if $K \supset k$ is unramified, wild, or fierce and obtain an expression for the integral closure S (see Prop. 2.6).

The importance of the conductor number g of a Galois extension of degree p is demonstrated in Sections 3 and 4.

In Section 3 we obtain an expression for the ramification number i of $K \supset k$ in terms of the conductor number g. Namely, $i = (ap/p-1) - gp - t$ with $0 \leq t \leq p-1$ when $K \supset k$ is wild, and $i = (a/p-1) - g - 1$ when $K \supset k$ is fierce.

In Section 4 we present expressions for the differential exponent $d(K/k)$ of a Galois extension $K \supset k$ of degree p in terms of the conductor number g. From this we obtain the following criterion for ramification in terms of the differential exponent.

PROPOSITION. *Let $d(K/k)$ denote the differential exponent of a Galois extension $K \supset k$ of degree p, let g denote its conductor number, and let a denote the absolute ramification index of k. Then*

i) *$K \supset k$ is unramified if and only if $d(K/k) = 0$*

ii) *$K \supset k$ is fierce if and only if $d(K/k) = a - g(p-1)$*

iii) *$K \supset k$ is wild if and only if $d(K/k) > a - g(p-1)$.*

Finally, in Section 5 we present examples to show that a cyclotomic extension of degree p may be unramified, wild, or fierce.

The following notation shall be in use throughout the paper. The set-theoretic difference of sets X and A shall be denoted by $X - A$. If R is a ring, then its multiplicative group of units shall be denoted by $U(R)$ and its radical by rad R. If t is an element of an overring T of R, then $R[t]$ shall denote the intermediate ring obtained by adjoining t to R; if m is an element of an R-module M, then $R(m)$ denotes the R-submodule of M obtained by adjoining m to R. If R is a local ring, then $\bar{R}$ shall denote its residue class field.

The filtration $U^{(i)}$ on the group of units of a discrete rank one valuation ring R is defined for $i \geq 0$ by $U^{(0)} = U(R)$ and $U^{(i)} = 1 + \pi^i R$ for $i > 0$ where π denotes a prime element of R (see p. 19 of [6]). For convenience of notation (see Section 1), we shall let $U^{(-1)} = \pi U^{(0)}$.

For the definition of the i^{th} ramification group G_i we refer the reader to p. 97 of [6], and for the definition of ramification number to p. 294 of

[8]. The definitions of tame and wild ramification may be found on pp. 88 – 89 of [6], and the definition of differential exponent on p. 298 of [8].

Unless otherwise stated, R shall always denote a complete discrete rank one valuation ring of unequal characteristic containing 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; π shall denote a prime element of R and Π a prime element of S. The definition of the absolute ramification index a of R is given on p. 45 of [5].

1. The field exponent. Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic, and assume that k contains a primitive p^{th} root of unity. The main purpose of this section is to define for each Galois extension $K \supset k$ of degree p an integer x with $-1 \leq x \leq p$ which we shall call the field exponent of $K \supset k$ (for the definition see the end of Section 1). The notion of the field exponent shall be used in the rest of the paper for studying ramification.

Consider an extension $K \supset k$ where $K = k(b^{1/p})$ and b is in R, and let $\beta = b^{1/p}$. Observe that the ring $R[\beta]$ is contained in the integral closure of R in K and that this inclusion may be proper or improper; observe also that $R[\beta]$ is a local ring (see p. 9 and p. 105 of [4]).

In the case when b is in $U^{(1)}$ the unique maximal ideal of $R[\beta]$ is generated by π and $\beta - 1$. The following proposition presents technical information about the ring $R[\beta]$ when $\beta^p = b$ is in $U^{(1)}$ which shall be useful throughout the paper.

PROPOSITION 1.1. *Let b denote an element of $U^{(1)}$ and let $\beta = b^{1/p}$. The element $(\beta - 1)^p$ of $R[\beta]$ is of the form*

$$(\beta - 1)^p = (b - 1) + up(\beta - 1)$$

where u is an element of the R-module $R(1, \beta, \cdots, \beta^{p-2})$ and satisfies the congruence $u \equiv -1$ mod $(p, \beta - 1)R[\beta]$.

Proof. In the case when $p = 2$ an easy computation shows that $(\beta - 1)^2 = (b - 1) + (-1)2(\beta - 1)$. Therefore $\beta - 1$ satisfies an equality of the desired form with $u = -1$.

Assume now that p is an odd (positive) prime number. Expanding $(\beta-1)^p$ according to the binomial theorem one obtains that $(\beta - 1)^p = (b-1) - B_1\beta^{p-1}$

$+\cdots+(-1)^i B_i\beta^{p-i}+\cdots+B_{p-1}\beta$ where B_i denotes the i^{th} binomial coefficient. By combining terms with the same binomial coefficient one obtains the equality $(\beta-1)^p=(b-1)+\sum(-1)^i B_i(\beta^{p-2i}-1)\beta^i$ with $1\leq i\leq(p-1)/2$. Define $A_i=(-1)^i B_i/p$. Expressing $\beta^{p-2i}-1$ in the form $\beta^{p-2i}-1=(\beta^{p-2i-1}+\cdots+1)(\beta-1)$ we get that $(\beta-1)^p=(b-1)+p(\beta-1)\sum A_i(\beta^{p-2i-1}+\cdots+1)\beta^i$ from which it follows that $u=\sum A_i(\beta^{p-i-1}+\cdots+\beta^i)$. Since there are $p-2i$ summands in the expression $\beta^{p-i-1}+\cdots+\beta^i$, the element $(\beta^{p-i-1}+\cdots+\beta^i)-(p-2i)$ is in $(\beta-1)R[\beta]$. For $1\leq i\leq(p-1)/2$ let s_i denote the element of $R[\beta]$ defined by $(\beta^{p-i-1}+\cdots+\beta^i)-(p-2i)=(\beta-1)s_i$. Then $u=(\beta-1)\sum A_i s_i+\sum A_i(p-2i)$. Now $\sum A_i(p-2i)\equiv-1 \bmod (p)$ (see Lemma 2.8 of [7]); we have shown therefore that $(\beta-1)^p$ satisfies an equality of the desired form with $u\equiv-1 \bmod (p,\beta-1)R[\beta]$.

It remains to show that u is in the R-module $R(1,\beta,\cdots,\beta^{p-2})$. For each i with $1\leq i\leq(p-1)/2$, the element $\beta^{p-i-1}+\cdots+\beta^i$ is in $R(1,\beta,\cdots,\beta^{p-2})$ because $p-i-1\leq p-2$ when $1\leq i$. Since $u=\sum A_i(\beta^{p-i-1}+\cdots+\beta^i)$, it now follows that u is in $R(1,\beta,\cdots,\beta^{p-2})$ and this completes the proof.

We proceed to prove propositions preliminary to the definition of the field exponent.

LEMMA 1.2. *Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic, and let a denote the absolute ramification index of R. If b is in $U^{(n)}$ for $n=(ap/p-1)+1$, then b has a p^{th} root in k.*

Proof. Let $\beta=b^{1/p}$ where $b=1+\pi^n r$ denotes an element of $U^{(n)}$, and define the element γ of $k(\beta)$ by $\gamma=(\beta-1)/\pi^{a/p-1}$. Since $k(\gamma)=k(\beta)$ it suffices to prove that $\deg_k\gamma<p$ in order to prove the lemma (see Prop. p. 121 of [1]). The equality $(\beta-1)^p=(b-1)+up(\beta-1)$ established in Prop. 1.1 together with the definition of γ implies by an easy computation that $\gamma^p=\pi r+uv\gamma$ where v is the element of $U(R)$ defined by $v\pi^a=p$. Since u is in the R-module $R(1,\beta,\cdots,\beta^{p-2})$ according to Prop. 1.1, it follows at once from the definition of γ that u is in the R-module $R(1,\gamma,\cdots,\gamma^{p-2})$. Therefore the equality $\gamma^p=\pi r+uv\gamma$ gives rise to a monic polynomial $f(X)$ in $R[X]$ with $f(\gamma)=0$. Since $u\equiv-1 \bmod (p,\beta-1)R[\beta]$, and $\overline{R[\beta]}=\bar{R}$, we have that $\bar{f}(X)=X^p+\bar{v}X$ in $\bar{R}[X]$. We have assumed that R is complete; therefore the factorization $\bar{f}(X)=X(X^{p-1}+\bar{v})$ implies that $f(X)$ is reducible over R by Hensel's lemma. Hence $\deg_k\gamma<p$, and so we may conclude that β is in R.

The preceding lemma shall be useful for proving the following existence statement.

PROPOSITION 1.3. *Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic which contains a primitive p^{th} root of unity, and let $K \supset k$ be a Galois extension of degree p where $p = char\ \bar{R}$. Then K is of the form $K = k(b^{1/p})$ for some element b of $U^{(x)} - U^{(x+1)}$ (set-theoretic difference) with $-1 \leq x \leq p$.*

Proof. Since k contains a primitive p^{th} root of unity, a Galois extension $K \supset k$ of degree p is of the form $K = k(c^{1/p})$ for some element c of k. Using the division algorithm it is easy to see that such an element c may always be chosen in $\pi^{\rho}U(R)$ for some ρ with $0 \leq \rho < p$.

We next observe that if c is in $\pi^{\rho}U(R)$ with $1 \leq \rho \leq \rho - 1$, then there exists an element b in $\pi U(R)$ such that $k(c^{1/p}) = k(b^{1/p})$. For there exist integers m and n such that $mp + n\rho = 1$ because ρ and p are relatively prime. Let $b = c^{n}\pi^{mp}$, and observe that b is in $\pi U(R)$. Since n is relatively prime to p we may conclude that $k(c^{1/p}) = k(b^{1/p})$ by Lemma 3 p. 90 of [3].

It remains to consider the case when $\rho = 0$, i.e. when $K = k(c^{1/p})$ with c in $U(R)$. Write c in the form $c = 1 + \pi^{y}t$ with $y \geq 0$ and t in $U(R)$. Observe that $k(c^{1/p}) = k((cd^{p})^{1/p})$ for every non-zero element d of k. The proof shall depend upon the proper choice of the element d. Recall that the absolute ramification index a of k satisfies $a \geq p - 1$ because we have assumed that k contains a primitive p^{th} root of unity. If $a = p - 1$, then the assumption thet $[K : k] = p$ implies that $0 \leq y \leq p$ according to Lemma 1.2. We may therefore restrict our attention to the case when $a > p - 1$ and $y > p$. Let $d = 1 + \pi$ and let $b = cd^{p}$. Since $y > p$ and $a \geq p$, an easy computation yields that b is of the form $b = 1 + \pi^{p}r$ with r in $U(R)$, and this completes the proof.

COROLLARY 1.4. *Let $K \supset k$ be Galois of degree p. If $K = k(b^{1/p})$ for some element b of $U^{(0)}$ such that $\bar{b}$ has a p^{th} root in $\bar{R}$, then there exists an element b_1 in $U^{(x)} - U^{(x+1)}$ with $1 \leq x \leq p$ such that $K = k(b_1{}^{1/p})$.*

Proof. Since b is in $U(R)$ and $\bar{b}$ has a p^{th} root in $\bar{R}$, there exists an element c in $U(R)$ such that $c^{p} \equiv b \bmod \pi R$, and so we may consider an element w of $U(R)$ and a positive integer y such that $b = c^{p} + \pi^{y}w$. Define $c_1 = b/c^{p}$ and observe that c_1 is in $U^{(y)} - U^{(y+1)}$ with $y > 0$. The proof of

Prop. 1.3 shows that there exists an element b_1 in $U^{(x)} - U^{(x+1)}$ with $1 \leq x \leq p$ such that $k(c_1^{1/p}) = k(b_1^{1/p})$.

In order to prove the desired uniqueness property of the integer x whose existence is guaranteed by Prop. 1.3 and Cor. 1.4 we first prove a lemma.

LEMMA 1.5. i) *If b_1 and b_2 are elements of k such that*

$$b_1 \text{ is in } U^{(x_1)} - U^{(x_1+1)} \text{ with } 1 \leq x_1 \leq p$$

$$b_2 \text{ is in } U^{(x_2)} - U^{(x_2+1)} \text{ with } 1 \leq x_2 \leq p$$

and $k(b_1^{1/p}) = k(b_2^{1/p})$, then $x_1 = x_2$.

ii) *If b is in $U^{(-1)}$, then $k(b^{1/p}) \neq k(b_1^{1/p})$ for every b_1 in $U(R)$.*

iii) *If b_1 is in $U^{(0)}$, b_2 is in $U^{(1)}$, and $k(b_1^{1/p}) = k(b_2^{1/p})$, then $\bar{b}_1$ has a p^{th} root in $\bar{R}$.*

Proof. The assumption that $k(b_1^{1/p}) = k(b_2^{1/p})$ implies that $b_1 = b_2^n c^p$ where n denotes a positive integer relatively prime to p and c is in $U(R)$ (see Lemma 3 p. 90 of [3]). It is easy to verify that b_2^n is of the form $b_2^n = 1 + \pi^{x_2} w$ where w is in $U(R)$. The assumptions that b_1 and b_2 are in $U^{(1)}$ imply that c is in $U^{(1)}$ and so we may write c in the form $c = 1 + \pi t$ with t in R. Then $b_1 = (1 + \pi^{x_2} w)(1 + \pi t)^p$ and so b_1 satisfies the congruence $b_1 \equiv 1 + \pi^{x_2} w \bmod \pi^p R$ since the absolute ramification index a of k satisfies $a \geq p - 1$. If $x_2 < p$, it now follows that $x_1 = x_2$. If $x_2 = p$, then the above expression for b_1 implies that $x_1 \geq p$. Since we have assumed that $x_1 \leq p$, we conclude that $x_1 = x_2 = p$.

The proof of part ii) is by contradiction. Assume that $k(b^{1/p}) = k(b_1^{1/p})$ for some element b_1 of $U(R)$. Then $b = b_1^n c^p$ for some element c of R and some integer n relatively prime to p. So $c^p = b/b_1^n$ is in $\pi U(R)$ from which it follows that c is in πR and b is in $\pi^p R$ which contradicts the assumption on b.

It remains to prove part iii). Since $k(b_1^{1/p}) = k(b_2^{1/p})$ and b_1 and b_2 are in $U(R)$ we may consider an integer n relatively prime to p and an element c of $U(R)$ such that $b_1 = b_2^n c^p$. Now $\bar{b}_2 = \bar{1}$ because b_2 is in $U^{(1)}$. Therefore $\bar{b}_1 = \bar{c}^p$.

The next proposition follows at once from the preceding lemma and Prop. 1.3 together with its corollary.

PROPOSITION 1.6. *Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic and let $p = \text{char } \bar{R}$. Assume that k contains a primitive p^{th} root of unity, and let $K \supset k$ denote a Galois extension of degree p. Then there exists a unique integer x such that $K \supset k$ is of one of the following forms:*

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

ii) *$K = k(b^{1/p})$ for some b in $U^{(x)} - U^{(x+1)}$ with $x = 0$ and such that the polynomial $X^p - \bar{b}$ is irreducible over $\bar{R}$*

iii) *$K = k(b^{1/p})$ for some b in $U^{(x)} - U^{(x+1)}$ with $1 \leq x \leq p$.*

DEFINITION. *Let $K \supset k$ denote a Galois extension of degree p. The unique integer $x(K/k) = x$ between -1 and p defined by Prop. 1.6 is called the field exponent of $K \supset k$.*

2. The conductor number. Consider a Galois extension $K \supset k$ of degree p where $K = k(\beta)$ and $\beta^p = b$ is in k. According to Section 1 we may assume that the element b is in $U^{(x)}$ where $x = x(K/k)$ denotes the field exponent of $K \supset k$.

In this section we present a method for computing the integral closure S of R in K by constructing a sequence (S_i) $(0 \leq i \leq g)$ of ring extensions of R in S such that $S_0 = R[\beta]$, $S_{i-1} \subset S_i$, and $S_g \subseteq S$. The number g satisfies the inequality $0 \leq g \leq (a/p-1) - 1$ and shall be called the conductor number $g(K/k)$ of $K \supset k$. Its importance shall be seen in the results of Sections 2, 3, and 4 of this paper.

We proceed to define the chain of rings (S_i) which shall be used for the construction of S. For the sake of clarity we shall consider separately the cases $x < p$ and $x = p$.

DEFINITION. *If the field exponent $x = x(K/k)$ of $K \supset k$ is such that $x < p$, we define the conductor number $g = g(K/k)$ to be zero.*

When $x(K/k) < p$ we therefore have $S_g = R[\beta] \subseteq S$. In Prop. 2.6 A we construct S from S_g for such x.

We now restrict our attention to the case of an extension $K \supset k$ for which $x = x(K/k) = p$. The construction of the integral closure S is facilitated by a separate consideration of the case when the absolute ramification index a of k equals $p-1$. When $a = p-1$ and $x(K/k) = p$ we shall define the conductor number $g(K/k)$ to be zero. In Prop. 2.6 B we construct S for the case when $x = p$ and $a = p - 1$ and prove that such an extension is always unramified.

It remains to consider extensions $K \supset k$ with field exponent p for which the absolute ramification index a of k satisfies $a \geq p$. The following lemma shall be used for proving Prop. 2.2. which is technical in nature.

LEMMA 2.1. *Let R denote a discrete rank one valuation ring of unequal characteristic whose absolute ramification index a satisfies the inequality $a \geq p$ where $p = char\ \bar{R}$. If $X^p - \bar{r} = \bar{0}$ has a solution in $\bar{R}$, then there exists an element r_1 in R such that $r_1^p - r$ is in $\pi^t R - \pi^{t+1} R$ with $1 \leq t \leq p$.*

Proof. Let $\bar{r}_0$ denote a solution of the equation $X^p - \bar{r} = \bar{0}$. If $r_0^p - r$ is in $\pi^t R - \pi^{t+1} R$ for some t with $1 \leq t \leq p$, then we may take $r_1 = r_0$. If $r_0^p - r \equiv 0 \bmod \pi^{p+1} R$, then we may write $r_0^p - r = \alpha \pi^{p+1}$ with α in R. Define $r_1 = r_0 + \pi$ and observe that $r_1^p - r = r_0^p - r + \pi^p + \pi p \gamma$ for some element γ in $U(R)$. So $r_1^p - r = \alpha \pi^{p+1} + \pi^p + \pi^{a+1} v \gamma$ where v is the element of $U(R)$ defined by $\pi^a v = p$. The assumption that $a \geq p$ now implies that $r_1^p - r$ is in $\pi^p R - \pi^{p+1} R$.

PROPOSITION 2.2. *Let $K \supset k$ denote a Galois extension of degree p whose field exponent $x(K/k)$ is p, and for which the absolute ramification index a of k satisfies $a \geq p$. There exists a pair of sequences (c_i) and (ϕ_i) with $0 \leq i \leq g$ such that*

i) *each c_i is in $U(R)$, $c_0 = -b$, and $c_1 = -r$ where $b = 1 + \pi^p r$*

ii) *each ϕ_i is in $U(S)$, $\phi_0 = \beta$, and $\phi_1 = (\phi_0 - 1)/\pi$*

iii) $1 \leq g \leq (a/p - 1) - 1$

and such that for every $i > 0$ the pair of elements ϕ_i and c_i satisfy a congruence of the form

$$\phi_i^p \equiv - c_i + B_i \pi^{a-i(p-1)+1} + A_i \pi^{a-i(p-1)} \phi_i \ mod\ \pi^{a-p+1} \phi_i R(\phi_{i-1})$$

where A_i is in $U(R[\beta])$, B_i is in $R[\phi_i]$, and $R(\phi_{i-1})$ denotes the R-module $R(1, \phi_{i-1}, \cdots, \phi_{i-1}^{p-2})$.

Proof. Observe that when $i = 0$ we have $\phi_0^p = - c_0$. For $i = 1$, Prop. 1.1 implies that $\phi_1^p = [(\beta - 1)/\pi]^p = [\pi^p r + up(\beta - 1)]/\pi^p = r + uv\pi^{a-p+1}\phi_1$ where v is the element of $U(R)$ defined by $\pi^a v = p$ and u is in $U(R[\beta])$. Therefore

$\phi_1{}^p = -c_1 + A_1\pi^{a-(p-1)}\phi_1$ with $A_1 = uv$, and so ϕ_1 satisfies a congruence of the desired form with $B_1 = 0$.

We proceed to define the pair of sequences (ϕ_i) and (c_i) inductively. So assume that ϕ_i and c_i have been defined for some i with $1 \leq i \leq (a/p-1)-1$, and that an R-module congruence of the form

$$\phi_i{}^p \equiv -c_i + B_i\pi^{a-i(p-1)+1} + A_i\pi^{a-i(p-1)}\phi_i \mod \pi^{a-p+1}\phi_i R(\phi_{i-1})$$

holds for some element A_i of $U(R[\beta])$ and some B_i in $R[\phi_i]$.

If the polynomial $X^p + \bar{c}_i$ is irreducible over $\bar{R}$, then we terminate the sequences, i.e. we do not define ϕ_{i+1} and c_{i+1}.

On the other hand, if $X^p + \bar{c}_i$ is reducible over $\bar{R}$, then it has a root in $\bar{R}$ (see Thm. 7 p. 66 of [8]). According to Lemma 2.1 we may therefore consider elements y_i and $\tilde{c}_{i+1}$ of $U(R)$ such that $y_i{}^p + c_i = \tilde{c}_{i+1}\pi^{t_i}$ with $1 \leq t_i \leq p$. Consider the element g_i of $R(1, \phi_{i-1}, \cdots, \phi_{i-1}{}^{p-2})$ defined by

$$\phi_i{}^p = -c_i + B_i\pi^{a-i(p-1)+1} + A_i\pi^{a-i(p-1)}\phi_i + g_i\pi^{a-p+1}\phi_i$$

whose existence is guaranteed by the inductive hypothesis. Form the element $\phi_i - y_i$ of $R[\phi_i]$ and observe that

$$\begin{aligned}(\phi_i - y_i)^p &\equiv \phi_i{}^p - y_i{}^p \mod p(\phi_i - y_i)R(\phi_i)\\ &\equiv -\tilde{c}_{i+1}\pi^{t_i} + B_i\pi^{a-i(p-1)+1} + (A_i + g_i\pi^{(i-1)(p-1)})y_i\pi^{a-i(p-1)}\\ &\quad + (A_i + g_i\pi^{(i-1)(p-1)})\ (\phi_i - y_i)\pi^{a-i(p-1)}\\ &\quad \mod p(\phi_i - y_i)R(\phi_i).\end{aligned}$$

In order to define A_{i+1}, observe that a computation like the one used in the proof of Prop. 2.9 shows that $\pi^{(i-1)(p-1)}R[\phi_{i-1}]$ is contained in $R[\beta]$. Since g_i is in $R[\phi_{i-1}]$ and A_i is in $U(R[\beta])$ it now follows that the element A_{i+1} defined by $A_{i+1} = A_i + g_i\pi^{(i-1)(p-1)}$ is in $U(R[\beta])$. (Note that $A_2 = A_1$ because $g_1 = 0$).

Recall (see the beginning of Section 1) that $R[\beta]$ is a local ring whose maximal ideal is generated by π and $\beta - 1$ and whose residue class field is $\bar{R}$. Since $\phi_1 = (\beta - 1)/\pi$ is in S because we have assumed that $x(K/k) = p$, the element $\beta - 1$ is in $\pi R[\phi_1]$. Therefore we may consider elements a_i of $U(R)$ and $\tilde{A}_i$ of $R[\phi_1]$ such that $A_{i+1}y_i = a_i + \tilde{A}_i\pi$. Define the element $\tilde{B}_i$ of $R[\phi_i]$ by $\tilde{B}_i = B_i + \tilde{A}_i$ and observe that the definitions of A_{i+1} and $\tilde{B}_i$ together with the congruence established above imply that

$$(\phi_i - y_i)^p \equiv - \tilde{c}_{i+1}\pi^{t_i} + a_i\pi^{a-i(p-1)} + \tilde{B}_i\pi^{a-i(p-1)+1}$$
$$+ A_{i+1}\pi^{t_i}(\phi_i - y_i)\pi^{a-i(p-1)} \bmod p(\phi_i - y_i)R(\phi_i).$$

The above congruence shall be denoted by (*).

Now we may complete the definition of the sequences (ϕ_i) and (c_i). If $i = (a/p-1) - 1$ or if $t_i < p$ then we terminate the sequences.

However, if $t_i = p$ and $i < (a/p-1) - 1$ we define $\phi_{i+1} = (\phi_i - y_i)/\pi$. The congruence (*) established above implies at once that

$$\phi_{i+1}{}^p \equiv - \tilde{c}_{i+1} + a_i\pi^{a-i(p-1)-p} + \tilde{B}_i\pi^{a-(i+1)(p-1)}$$
$$+ A_{i+1}\pi^{a-(i+1)(p-1)}\phi_{i+1} \bmod \pi^{a-p+1}\phi_{i+1}R(\phi_i).$$

The ring $R[\phi_i]$ is a local ring with residue class field $\bar{R}$ whose maximal ideal is generated by π and $\phi_i - y_i$. We may therefore consider elements b_i of R and B_{i+1} of $R[\phi_{i+1}]$ such that $\tilde{B}_i = b_i + B_{i+1}\pi$. Define the element c_{i+1} of $U(R)$ by the equality $-c_{i+1} = -\tilde{c}_{i+1} + a_i\pi^{a-i(p-1)-p} + b_i\pi^{a-(i+1)(p-1)}$. Then

$$\phi_{i+1}{}^p \equiv - c_{i+1} + B_{i+1}\pi^{a-(i+1)(p-1)+1} + A_{i+1}\pi^{a-(i+1)(p-1)}\phi_{i+1} \bmod \pi^{a-p+1}\phi_{i+1}R(\phi_i)$$

and this completes the proof.

Statement (*) of the above proof shall be useful for the construction of S and so we present it as a corollary.

COROLLARY 2.3. *If the polynomial $X^p + \bar{c}_i$ is reducible over $\bar{R}$ for some $i \geq 1$, then the element $\phi_i - y_i$ of S satisfies a congruence of the form*

$$(\phi_i - y_i)^p \equiv - \tilde{c}_{i+1}\pi^{t_i} + a_i\pi^{a-i(p-1)} + \tilde{B}_i\pi^{a-i(p-1)+1}$$
$$+ A_{i+1}(\phi_i - y_i)\pi^{a-i(p-1)} \ \mathit{mod}\ p(\phi_i - y_i)R(\phi_i)$$

where a_i is in $U(R)$, $\tilde{B}_i$ is in $R[\phi_i]$ and $1 \leq t_i \leq p$.

Prop. 2.2 enables us to define the conductor number of an extension with field exponent p.

DEFINITION. *Let $K \supset k$ denote a Galois extension of degree p whose field exponent x is p. If $a = p-1$ we define the conductor number $g(K/k)$ to be zero. If $a \geq p$, consider a sequence (ϕ_i) $(0 \leq i \leq g)$ of elements whose existence is guaranteed by Prop. 2.2. The integer g depends only upon the extension $K \supset k$ (see Cor. 3.2) and we call $g = g(K/k)$ the conductor number of $K \supset k$.*

We have now defined the notion of conductor number for each Galois extension $K\supset k$ of degree p. Note that $g(K/k)>0$ if and only if $x(K/k)=p$ and $a\geq p$. In the case when $g=0$ we define $\phi_0=\beta$.

The elements ϕ_i defined above give rise to a sequence of subrings (S_i) of S in the following way. Let $S_0=R[\beta]$, and let $S_{i+1}=S_i[\phi_{i+1}]$ for $0\leq i<g$; observe that $S_i=R[\phi_i]$ for each i. We have now defined for each Galois extension $K\supset k$ of degree p a chain of rings

$$R\subset S_0\subset\cdots\subset S_i\subset S_{i+1}\subset\cdots\subset S_g\subseteq S.$$

The inclusion $R\subset S_0$ is strict and so is each inclusion $S_i\subset S_{i+1}$. However, S_g may equal S.

The rest of this section is devoted to the task of computing S from its subring S_g and to studying the ramification properties of $K\supset k$. The reader may refer to the introduction for the definition of fierce ramification.

LEMMA 2.4. *Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic, let $p=\text{char }\bar{R}$, and let S denote the integral closure of R in an extension $K\supset k$ of degree p.*

i) *If there exists an element α in S such that $\alpha^p=A\pi^{p-1}\alpha+C\pi^p$ where A is an element of $U(S)$ present in the R-module $R(1,\alpha,\cdots,\alpha^{p-2})$ and C is an element of $R[\alpha]$, then $K\supset k$ is unramified and $S=R[\theta]$ where $\theta=\alpha/\pi$.*

ii) *If there exists an element α in S such that α^p is in $\pi^yU(S)$ where y is a positive integer relatively prime to p, then $K\supset k$ is wildly ramified and $S=R[\Pi]$ where $\Pi=\alpha^n\pi^m$ and m and n are integers satisfying $mp+ny=1$.*

iii) *If θ is an element of S such that $\bar{\theta}$ is not in $\bar{R}$ but $\bar{\theta}^p$ is in $\bar{R}$, then $K\supset k$ is fiercely ramified and $S=R[\theta]$.*

Proof. The definition of θ together with the assumption on α implies that $\theta^p=A\theta+C$. Since A is in $R(1,\alpha,\cdots,\alpha^{p-2})$ and $\alpha=\pi\theta$, the equality $\theta^p=A\theta+C$ gives rise to an irreducible monic polynomial $f(X)$ having θ as a root. Consider the polynomial $\bar{f}(X)$ of $\bar{R}[X]$ and observe that $\bar{f}(X)=X^p-\bar{A}X-\bar{C}$. Since $\bar{f}'(X)=-\bar{A}$ and $\bar{A}\neq 0$ because A is in $U(S)$, the polynomial $\bar{f}(X)$ can have no repeated roots. If $\bar{f}(X)$ were reducible over $\bar{R}$ it would follow by Hensel's lemma (since R is complete) that $f(X)$ is reducible over R which is a contradiction. Therefore $\bar{f}(X)$ is an irreducible separable polynomial over $\bar{R}$, and $\bar{S}=\bar{R}(\bar{\theta})$. Prop. 1 p. 25 of [3] now implies that $K\supset k$ is unramified and $S=R[\theta]$. This completes the proof of part i).

The assumption on α in part ii) implies that we may consider an element s of $U(S)$ such that $\alpha^p = \pi^y s$. Since $ny + mp = 1$, an easy computation shows that $\Pi^p = \pi s^n$ where $\Pi = \alpha^n \pi^m$. Therefore Π is a prime element of S, the extension $K \supset k$ is wild, and $S = R[\Pi]$ (see Cor. 3-3-2 of [6]).

The hypothesis of part iii) implies at once that $\bar{S} \supset \bar{R}$ is purely inseparable of degree p and that $\bar{S} = \bar{R}(\bar{\theta})$. Therefore $K \supset k$ is fiercely ramified, and so π is a prime element of S. The fact that $\bar{S} = S/\pi S$ together with the fact that R is a local ring implies that $S = R[\theta]$ (see for example p. 270 of [2]).

COROLLARY 2.5. *If $K \supset k$ is an extension of degree p, then the extension $S \supset R$ is simple; i.e. there exists an element θ of S such that $S = R[\theta]$.*

The main result of the paper is presented in the three statements of Prop. 2.6. Recall that k denotes the quotient field of a complete discrete rank one valuation ring R of unequal characteristic which contains a primitive p^{th} root of unity where $p = \text{char } \bar{R}$. Recall that a Galois extension $K \supset k$ of degree p may be written $K = k(\beta)$ where $\beta^p = b$ is in $U^{(x)}$ and x denotes the field exponent of $K \supset k$.

PROPOSITION 2.6 A. *Let $K \supset k$ be Galois extension of degree p with $x(K/k) < p$.*

i) *If $x(K/k) = -1$, then $K \supset k$ is wildly ramified and $S = R[\beta]$.*

ii) *If $x(K/k) = 0$, then $K \supset k$ is fiercely ramified and $S = R[\beta]$.*

iii) *If $1 \leq x(K/k) < p$, then $K \supset k$ is wildly ramified and $S = R[\Pi]$ where $\Pi = (\beta - 1)^n \pi^m$ and m and n are integers satisfying $nx + mp = 1$.*

Proof. If $x(K/k) = -1$ then $\beta^p = \pi r$ for some element r of $U(R)$, so that β is a prime element of S, the extension $K \supset k$ is wildly ramified, and $S = R[\beta]$.

If $x(K/k) = 0$, then $X^p - \bar{b}$ is irreducible over $\bar{R}$ according to the definition of the field exponent. By applying Lemma 2.4 we conclude that $K \supset k$ is fiercely ramified and $S = R[\beta]$.

In the case when $1 \leq x < p$, an application of Prop. 1.1 shows that $(\beta - 1)^p$ is in $\pi^x U(S)$. The desired result now follows from Lemma 2.4.

PROPOSITION 2.6 B. *Let $K \supset k$ be a Galois extension of degree p such that $x(K/k) = p$ and $a = p-1$. Then $K \supset k$ is unramified and $S = R[\theta]$ where $\theta = (\beta - 1)/\pi$.*

Proof. Since $x = p$ we may write b in the form $b = 1 + \pi^p r$ with r in $U(R)$, and since $a = p - 1$ we may write $p = \pi^{p-1} v$ with v in $U(R)$. Let

$\alpha = \beta - 1$. Prop. 1.1 implies that $\alpha^p = uv\pi^{p-1}\alpha + \pi^p r$ where u is a unit present in $R(1, \beta, \cdots, \beta^{p-2})$. Since uv is in $R(1, \alpha, \cdots, \alpha^{p-2})$ we may now conclude from Lemma 2.4 that $K \supset k$ is unramified and that $S = R[\alpha/\pi]$.

The notation used in the statement and proof of Prop. 2.6 C has been introduced in Prop. 2.2.

PROPOSITION 2.6 C. *Let $K \supset k$ be a Galois extension of degree p such that $x(K/k) = p$ and $a \geq p$, and let g denote the conductor number of $K \supset k$.*

i) *If $X^p + \bar{c}_g$ is irreducible over $\bar{R}$, then $K \supset k$ is fiercely ramified and $S = S_g$.*

ii) *If $X^p + \bar{c}_g$ is redcible over $\bar{R}$ and $g < (a/p - 1) - 1$, then $K \supset k$ is wildly ramified and $S = R[\Pi]$ where $\Pi = (\phi_g - y_g)^n \pi^m$ and m and n are integers satisfying $nt_g + mp = 1$.*

iii) *If $X^p + \bar{c}_g$ is reducible over $\bar{R}$ and $g = (a/p - 1) - 1$, then $K \supset k$ may be either wild or unramified. In particular, if $t_g = p - 1$ and $-\tilde{c}_{g+1} + a_g$ is a non-unit of R than $K \supset k$ is unramified and $S = R[\theta]$ where $\theta = (\phi_g - y_g)/\pi$. Otherwise $K \supset k$ is wildly ramified and $S = R[\Pi]$ where $\Pi = (\phi_g - y_g)^n \pi^m$ for suitable integers m and n (see the proof below).*

Proof. Note first of all that the congruence established in Prop. 2.2 implies that $\bar{\phi}_i^p + \bar{c}_i = \bar{0}$ for each i because $a - i\ (p-1) > 0$ when $0 \leq i \leq (a/p - 1) - 1$. The assumption that $X^p + \bar{c}_g$ is irreducible over $\bar{R}$ implies that $\bar{\phi}_g$ is not in $\bar{R}$ since $\bar{\phi}_g{}^p + \bar{c}_g = \bar{0}$. Lemma 2.4 now implies that $K \supset k$ is fiercely ramified and that $S = R[\phi_g]$. This completes the proof of part i).

The hypothesis for part ii) implies that $t_g < p$. For, if t_g were equal to p, then ϕ_{g+1} would be defined because $g < (a/p - 1) - 1$ and $X^p + \bar{c}_g$ is reducible over $\bar{R}$ (see the proof of Prop. 2.2). Also, the assumption that $g < (a/p - 1) - 1$ implies that $a - g(p-1) \geq p$ and so $(\phi_g - y_g)^p$ is in $\pi^{t_g} U(S)$ by Cor. 2.3. Since $1 \leq t_g \leq p - 1$, an application of Lemma 2.4 gives the desired result.

In part iii) the assumption that $g = (a/p - 1) - 1$ implies that $a - g(p-1) = p - 1$. Define the integer t by $t = t_g$ if $t_g \leq p - 1$ and $t = p - 1$ if $t_g = p$. If $t_g \neq p - 1$, then Cor. 2.3 implies that $(\phi_g - y_g)^p$ is in $\pi^t U(S)$. An application of Lemma 2.4 now shows that $K \supset k$ is wildly ramified and that $S = R[\Pi]$ where $\Pi = (\phi_g - y_g)^n \pi^m$ and $nt + mp = 1$.

If $t_g = p - 1$ and $-\tilde{c}_{g+1} + a_g$ is in $U(R)$, them Cor. 2.3 implies that $(\phi_g - y_g)^p$ is in $\pi^{p-1}U(S)$. So $K \supset k$ is wildly ramified and $S = R[\Pi]$ where $\Pi = (\phi_g - y_g)^n \pi^m$ and $n(p-1) + mp = 1$ according to Lemma 2.4.

Finally, in the case when $t_g = p - 1$ and $-\tilde{c}_{g+1} + a_g$ is a non-unit of R, let $\alpha = \phi_g - y_g$ and note that α satisfies an equation of the form $\alpha^p = A\pi^{p-1}\alpha + C\pi^p$ with $A = A_{g+1}$ in $U(S_g)$ and C in S_g according to Cor. 2.3. In order to apply part i) of Lemma 2.4 it remains to verify that A_{g+1} is in the R-module $R(1, \phi_g, \cdots, \phi_g^{p-2})$. Since $A_1 = uv$ is in $R(1, \beta, \cdots, \beta^{p-2})$ (see Prop. 1.1) and A_{i+1} is defined by $A_{i+1} = A_i + g_i\pi^{(i-1)(p-1)}$, one can show by an inductive argument that each A_{i+1} for $0 \leq i \leq g$ is in $R(1, \beta, \cdots, \beta^{p-2})$ because each g_i is in $R(1, \phi_{i-1}, \cdots, \phi_{i-1}^{p-2})$ according to its definition in the proof of Prop. 2.2. The inclusion $R(1, \beta, \cdots, \beta^{p-2}) \subset R(1, \phi_g, \cdots, \phi_g^{p-2})$ now implies that $\alpha = \phi_g - y_g$ satisfies an equation of the desired form because $R(1, \alpha, \cdots, \alpha^{p-2}) = R(1, \phi_g, \cdots, \phi_g^{p-2})$. We conclude therefore by Lemma 2.4 that $K \supset k$ is unramified and that $S = R[(\phi_g - y_g)/\pi]$.

The statements of Cor. 2.7 follow at once from Prop. 2.6.

COROLLARY 2.7. *Let $K \supset k$ denote a Galois extension of degree p.*

i) *If $K \supset k$ is unramified, then the conductor number $g(K/k)$ is $(a/p - 1) - 1$.*

ii) *If the field exponent $x(K/k)$ is relatively prime to p, then $K \supset k$ is wildly ramified.*

iii) *If $K \supset k$ is fiercely ramified, then $S = S_g$.*

The next proposition motivates the naming of the conductor number of an extension.

PROPOSITION 2.8. *Let g denote the conductor number of a Galois extension $K \supset k$ of degree p. Then $C_R = \pi^{g(p-1)}R$ where C_R is the ideal of R defined by $C_R = \{c \text{ in } R \mid cS_g \subset S_0\}$.*

Proof. If $g = 0$ then $C_R = R$ and the assertion is true. It follows by an easy computation from the definitions $\phi_i = (\phi_{i-1} - y_{i-1})/\pi$ for $1 \leq i \leq g$ (where $y_0 = 1$) that $\phi_g = (1/\pi^g)\phi_0 - \sum y_{g-i}/\pi^i$ with $1 \leq i \leq g$. Observe that an element c of R is in C_R if and only if $c\phi_g^i$ is in S_0 for $1 \leq i \leq p - 1$. By expanding $\phi_g^{p-1} = [(1/\pi^g)\phi_0 - \sum y_{g-i}/\pi^i]^{p-1}$ according to the binomial theorem and using the fact that $\{1, \phi_0, \cdots, \phi_0^{p-1}\}$ is a free basis for K over k, one may conclude that an element c of R has the property that $c\phi_g^{p-1}$ is in S_0 if and only if

c is in $\pi^{g(p-1)}R$. It is easy to see that $c\phi_g^{\,i}$ is in S_0 for $1 \leq i < p-1$ when c is in $\pi^{g(p-1)}R$, and this completes the proof.

3. The ramification number. Consider a Galois extension $K \supset k$ of degree p, where k denotes as usual the quotient field of a complete discrete rank one valuation ring R of unequal characteristic which contains a primitive p^{th} poot of unity where $p = \text{char } \bar{R}$. Let i denote the ramification number of $K \supset k$; i.e. let i denote the discontinuity in the sequence of ramification groups of $K \supset k$. (Explicitly, i is the integer with $i \geq -1$ for which $G = G_i$ and $G_{i+1} = (1)$ where G is the Galois group of $K \supset k$ and G_j denotes the j^{th} ramification group of $K \supset k$.)

The purpose of this section is to give an expression for the ramification number i in terms of the conductor number. (In the case when $x(K/k) = -1$ hte ramification number of $K \supset k$ is well known (see Exercise 4 p. 79 of [5])).

In the following proposition, g denotes the conductor number of $K \supset k$, x denotes the field exponent of $K \supset k$, and a denotes the absolute ramification index of k.

PROPOSITION 3.1. *Let i denote the ramification number of a Galois extension $K \supset k$ of degree p.*

i) *If $K \supset k$ is unramified then $i = -1$.*

ii) *If $K \supset k$ is wildly ramified then $i = ap/p-1$ when $x = -1$, and $i = (ap/p-1) - gp - t$ when $x \neq -1$ where $1 \leq t \leq p-1$ and rad $S_g = (\pi, \Pi^t S \cap S_g)S_g$. Furthermore, $t = x$ when $1 \leq x \leq p-1$.*

iii) *If $K \supset k$ is fiercely ramified then $i = (a/p-1) - g - 1$.*

Proof. The equality $G_{-1} = G(K/k)$ always holds. When $K \supset k$ is unramified it is well known that $G_0 = (1)$.

If $K \supset k$ is wildly ramified and $x = -1$, then β is a prime element of S and an easy computation shows that the discontinuity in the sequence of ramification groups occurs at $i = ap/p-1$.

In the case when $K \supset k$ is wildly ramified and $x > -1$ (so that β is a unit), recall that the element $\phi_g - y_g$ of S_g has the property that $(\phi_g - y_g)^p$ is in $\pi^t U(S_g)$ for some integer t with $1 \leq t \leq p-1$ (see Props. 2.6 A and 2.6 C). An easy computation shows that $(\phi_g - y_g)S = \Pi^t S$. Since rad S_g is generated by π and $\phi_g - y_g$ we may now conclude that rad $S_g = (\pi, \Pi^t S \cap S_g)$. (Using the assumption that $K \supset k$ is wild together with the fact that

$1 \leq t \leq p-1$, one can show that t is the unique integer satisfying the equality rad $S_g = (\pi, \Pi^t S \cap S_g)S_g$.)

We proceed to compute the ramification number i of $K \supset k$. Consider positive ingeters n and w such that $nt - wp = 1$, and recall that $S = R[\Pi]$ where $\Pi = (\phi_g - y_g)^n/\pi^w$ is a prime element of S. Let ζ denote a primitive p^{th} root of unity and let σ be the element of $G(K/k)$ defined by $\sigma(\beta) = \zeta\beta$. It follows from the definition of Π that σ is in the i^{th} ramification group G_i if and only if

$$[\sigma(\phi_g - y_g) - (\phi_g - y_g)][\sigma(\phi_g - y_g)^{n-1} + \cdots + (\phi_g - y_g)^{n-1}]/\pi^w$$

is in $\Pi^{i+1}S$. Observe that $\sigma(\phi_g - y_g)^{n-1} + \cdots + (\phi_g - y_g)^{n-1}$ is in $n(\phi_g - y_g)^{n-1}U(S)$ because $\sigma(\phi_g - y_g) \equiv \phi_g - y_g \bmod \Pi S_g$. Since n is relatively prime to p, we now have that σ is in G_i if and only if $(\sigma(\phi_g) - \phi_g)(\phi_g - y_g)^n/\pi^w$ is in $(\phi_g - y_g)\Pi^{i+1}S$. The definition of Π together with the fact that $(\phi_g - y_g)S = \Pi^t S$ implies that σ is in G_i if and only if $\sigma(\phi_g) - \phi_g$ is in $\Pi^{t+i}S$. Use the equality $\phi_g = (1/\pi^g)\beta - \sum y_{g-i}/\pi^i$ with $1 \leq i \leq g$ (see the proof of Prop. 2.8) to obtain that $\sigma(\phi_g) - \phi_g$ is in $(\zeta - 1)/\pi^g U(S)$. We may now conclude that σ is in G_i if and only if $i \leq (ap/p-1) - gp - t$ and this completes the proof of part ii).

When $K \supset k$ is fiercely ramified, $S = S_g$ according to Cor. 2.7. Let ζ and σ be as above, and note that σ is in G_i if and only if $\sigma(\phi_g) - \phi_g$ is in $\pi^{i+1}S$. The equality $\phi_g = (1/\pi^g)\beta - \sum y_{g-i}/\pi^i$ with $1 \leq i \leq g$ now implies that σ is in G_i if and only if $(\zeta - 1)/\pi^g$ is in $\pi^{i+1}U(S)$, i.e. if and only if $i \leq (a/p-1) - g - 1$.

COROLLARY 3.2. *The conductor number $g(K/k)$ is uniquely defined.*

Proof. The proof follows at once from Cor. 2.7 and Prop. 3.1.

4. The different. Throughout this section $K \supset k$ shall always denote a Galois extension of degree p 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 where $p = \text{char } \bar{R}$, and S shall denote the integral closure of R in K. The object of this section is the computation of the diferent $D(S/R)$ in terms of the conductor number $g(K/k)$. From this we shall establish a criterion for determining if $K \supset k$ is unramified, wild, or fierce in terms of the differential exponent and the conductor number.

The assumption on the degree of $K \supset k$ implies that $S \supset R$ is a simple extension (see Cor. 2.5). It is well known in the case of an extension with a separable residue class field extension, that the ramification groups yield an expression for the differential exponent. A similar expression holds for any Galois extension $L\supset k$ with the property that the integral closure S of R in L is a simple ring extension of R. The proof of the following lemma may be obtained at once from pp. 33–34 of [3], and for the convenience of the reader we present it here.

LEMMA 4.1. *Let L denote a Galois extension of the quotient field k of a complete discrete rank one valuation ring R such that the integral closure S of R in L is a simple ring extension of R. Then the differential exponent $d = d(L/K)$ is given by*

$$d = \sum(g_i - 1) \text{ with } 0 \leq i < \infty$$

where g_i denotes the order of the i^{th} ramification group of $L\supset k$.

Proof. The assumption that $S\supset R$ is a simple ring extension means that we may write $S = R[\alpha]$ for some element α of S, so that $D(S/R) = g'(\alpha)S$ where $g(X)$ denotes the minimal polynomial of α over k (see Prop. 6 p. 17 of [3]). From this it follows that $d(L/k) = v_L(\Pi(\alpha - \alpha^\sigma))$ where σ ranges over the set $G(L/k) - \{1\}$ and v_L denotes the valuation of L. The homomorphic property of v_L now implies that $d(L/k) = \sum v_L(\alpha^\sigma - \alpha)$ with σ ranging over $G(L/k) - \{1\}$.

Let g_i denote the order of the i^{th} ramification group of $L\supset k$. If an element σ of $G(L/k)$ is in $G_{i-1} - G_i$, then $v_L(\alpha^\sigma - \alpha) = i$. The above expression for $d(L/k)$ now implies that $d(L/k) = \sum i(g_{i-1} - g_i)$. From the equalities $\sum i(g_{i-1} - g_i) = \sum i\,(g_{i-1} - 1) - \sum i\,(g_i - 1) = \sum(g_i - 1)$ with $0 \leq i < \infty$ we may now conclude that $d(L/k) = \sum(g_i - 1)$.

By combining Prop. 3.1 with Lemma 4.1 we may now compute the differential exponent of a Galois extension of degree p. In the following proposition, t denotes the integer between 1 and $p-1$ defined in the statement of Prop. 3.1.

PROPOSITION 4.2. *Let $K\supset k$ denote a Galois extension of degree p with differential exponent d, conductor number g, and field exponent x. Let a denote the absolute ramification index of k.*

i) *If $K\supset k$ is unramified, then $d = 0$.*

ii) *If $K \supset k$ is wildly ramified, then* $d = ap + (p-1)$ *when* $x = -1$, *and* $d = ap - gp(p-1) - (t-1)(p-1)$ *when* $1 \leq x \leq p$.

iii) *If $K \supset k$ is fiercely ramified, then* $d = a - g(p-1)$.

Proof. For the unramified case the assertion is well known.

Consider the case when $K \supset k$ is wild. If $x = -1$, then $d = \sum(g_i - 1)$ with $0 \leq i \leq ap/p - 1$ by Lemma 4.1 since $ap/p - 1$ is the ramification number of $K \supset k$ (see Prop. 3.1); therefore $d = ap + (p-1)$ since $g_i = p$ for $0 \leq i \leq ap/p - 1$. If $1 \leq x \leq p$, then the ramification number of $K \supset k$ is $(ap/p - 1) - gp - t$, so that $d = \sum(g_i - 1)$ with $0 \leq i \leq (ap/p - 1) - gp - t$, from which it follows that $d = ap - gp(p-1) - (t-1)(p-1)$.

In the case when $K \supset k$ is fierce, the ramification number is $(a/p - 1) - g - 1$. So $d = \sum(g_i - 1)$ with $0 \leq i \leq (a/p - 1) - g - 1$, from which it follows that $d = a - g(p-1)$.

PROPOSITION 4.3. *Let $d(K/k)$ denote the differential exponent of a Galois extension $K \supset k$ of degree p, let g denote its conductor number, and let a denote the absolute ramification index of k. Then*

i) *$K \supset k$ is unramified if and only if* $d(K/k) = 0$

ii) *$K \supset k$ is fiercely ramified if and only if* $d(K/k) = a - g(p-1)$.

iii) *$K \supset k$ is wildly ramified if and only if* $d(K/k) > a - g(p-1)$.

Proof. Statement i) is well known (for example combine Prop. 1 p. 25, Prop. 6 p. 17, and Thm. 1 p. 21 of [3]).

We proceed to prove that $d(K/k) > a - g(p-1)$ when $K \supset k$ is wild. The proof shall depend upon the expression for $d(K/k)$ presented in part ii) of Prop. 4.2. If the field exponent x of $K \supset k$ is -1 then $g = 0$ (see Section 2) so that the desired inequality holds because $d(K/k) = ap + (p-1)\ a$. If on the other hand, $1 \leq x \leq p$, then $d(K/k) = ap - gp(p-1) - (t-1)(p-1)$ where t satisfies $0 \leq t - 1 \leq p - 2$. An easy computation shows that $d(K/k) > a - g(p-1)$ if and only if $a - g(p-1) - (t-1) > 0$. The inequalities $g \leq (a/p - 1) - 1$ (see Prop. 2.2) and $t - 1 \leq p - 2$ together imply that $a - g(p-1) - (t-1) > 0$, and we may conclude therefore that $d(K/k) > a - g(p-1)$ whenever $K \supset k$ is wild.

If $K \supset k$ is fierce, then $d(K/k) = a - g(p-1)$ by part iii) of Prop. 4.2. Conversely, if $d(K/k) = a - g(p-1)$ then $K \supset k$ cannot be unramified because

$a-g(p-1)>0$ and $K\supset k$ cannot be wildly ramified according to the above observation concerning the differential exponent in the wild case.

To complete the proof of the proposition it suffices to observe that if $d(K/k)>a-g(p-1)$ then $K\supset k$ can be neither unramified nor fierce.

5. Cyclotomic extensions. The following definition may be found on p. 41 of [1].

DEFINITION. *Let k be any field. The extension obtained by adjunction of all roots of unity shall be called the maximal cyclotomic extension of k and any intermediate field a cyclotomic extension of k.*

Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic. Assume that R contains a primitive p^{th} root of unity where $p=\text{char }\bar{R}$ and let $K\supset k$ denote a cyclotomic extension of degree p. Prop. 2.6 gives criteria for detemining the ramification properties of such an extension. The following examples demonstrate the existence of unramified, wildly ramified, and fiercely ramified cyclotomic extensions of degree p.

EXAMPLE 5.1. Let Z denote the ring of integers and let $Z[X]_{(2)}$ denote the localization of the polynomial ring $Z[X]$ at the prime ideal (2). Throughout this example R_0 shall denote the completion of $Z[X]_{(2)}$ and k_0 shall denote the quotient field of R_0.

In order to produce an *unramified* cyclotomic extension of degree p we shall take the ground ring R to be an extension of R_0. Namely, let R be the integral closure of R_0 in the extension $k=k_0(\sqrt{3})$ of k_0. (Observe that $1-\sqrt{3}$ is a prime element of R.) We shall show that the cyclotomic extension $k(i)\supset k$ is unramified of degree 2 where i denotes a primitive fourth root of unity. For consider the element $\theta=(\sqrt{3}-i)/2(2-\sqrt{3})$ of $k(i)$. It is easy to verify that $f(X)=X^2+[(2-\sqrt{3})/(7\sqrt{3}-12)]X+[i/(7\sqrt{3}-12)]$ is the minimal polynomial of θ over k. By applying Prop. 1 on p. 25 of [3] we may now conclude that $k(i)\supset k$ is unramified.

Again let i denote a primitive fourth root of unity. The element $i-1$ of $k_0(i)$ is a root of an Eisenstein polynomial over R_0, from which it follows that $k_0(i)\supset k_0$ is a *wildly* ramified cyclotomic extension of degree 2.

Finally, in order to exhibit the existence of a *fiercely* ramified cyclotomic extension, consider the integral closure R of R_0 in the extension $k=k_0(\sqrt{2X})$

of k_0. Observe that $R = R_0[\sqrt{2X}]$ and that $\sqrt{2X}$ is a prime element of R. The extension $k(i) \supset k$ has residue class field extension $\bar{R}(\bar{X}^{\frac{1}{2}}) \supset \bar{R}$ whose inseparability implies that $k(i) \supset k$ is a fiercely ramified cyclotomic extension.

The above examples motivate us to determine sufficient conditions on the ground ring R in order that a cyclotomic extension obtained by the adjunction of a p^{t} th root of unity be wildly ramified. For this we shall make use of the following definition.

DEFINITION. *Let R be a complete discrete rank one valuation ring of unequal characteristic. Then R is said to be absolutely tamely ramified if a is relatively prime to p where a denotes the absolute ramification index of R and p denotes the characteristic of $\bar{R}$.*

PROPOSITION 5.2. *Let R denote an absolutely tamely ramified complete discrete one valuation ring containing a primitive p^{th} root of unity ζ, and let k denote the quotient field of R. Let ξ denote a primitive p^{t} th root of unity. Then the extension $k(\xi) \supset k$ is wildly ramified of degree p^{t-1}.*

Proof. The hypothesis implies that $a/p-1$ and p^{t-1} are relatively prime where a denotes the absolute ramification index of R. We may therefore consider integers m and n such that $ma/p-1+np^{t-1}=1$. Let π denote a prime element of R, and define the element Π of $k(\xi)$ by $\Pi = (\xi-1)^m\pi^n$. A straightforward computation shows that $\Pi^{p^{t-1}} = \pi u$ for some unit u of $k(\xi)$, from which it follows that $k(\xi) \supset k$ is wildly ramified of degree p^{t-1}.

REFERENCES

[1] E. Artin and J. Tate, *Class field theory*, Benjamin, (1967).
[2] M. Auslander and D. Buchsbaum, *On ramification theory in noetherian rings*, Amer. J. of Math. Vol. **81** (1959), pp. 749–765.
[3] J.W.S. Cassels and A. Frolich, *Algebraic Number Theory*, Thompson, (1967).
[4] M. Nagata, *Local Rings*, Wiley, (1962).
[5] J.P. Serre, *Corps Locaux*, Paris, Hermann, (1962).
[6] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, (1963).
[7] S. Williamson, *Equivalence classes of maximal orders*, Nagoya Math. J. Vol. **31** (1968), pp. 131–171.
[8] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. **1**, Van Nostrand, (1958).

Regis College
Weston, Massachusetts