PACIFIC JOURNAL OF MATHEMATICS
Vol. 86, No. 2, 1980

A NOTE ON TAMELY RAMIFIED POLYNOMIALS

J. P. BUHLER

Let $f(x)$ be a monic polynomial with coefficients in a Dedekind ring A. If P is a prime ideal and A_P denotes the completion of A at P then $f(x)$ is said to be integrally closed at P if $A_P[X]/(f(X))$ is isomorphic to a product of discrete valuation rings. The purpose of this note is to show that if $f(x)$ appears to be tamely ramified and integrally closed at P (in terms of its discriminant and factorization mod P) then in fact it is.

If $f(\alpha) = 0$, where $f(x)$ is a monic irreducible polynomial with coefficients in $\boldsymbol{Z}$, then the ring $\boldsymbol{Z}[\alpha]$ is of finite index in the ring R of algebraic integers in $\boldsymbol{Q}(\alpha)$. The full ring of integers can be obtained by applying a very general algorithm due to Zassenhaus ([6]). There are well known cases where this is unnecessary. If, for instance, $f(x)$ is an Eisenstein polynomial at p, or if p^2 does not divide the discriminant of $f(x)$, then the polynomial $f(x)$ is integrally closed at p (which is equivalent to saying that p does not divide the index $[R: \boldsymbol{Z}[\alpha]]$). The theorem below asserts that if the power of p that divides the discriminant of $f(x)$ is consistent with the factorization of $f(x)$ mod P and the hypothesis that R is tamely ramified at p, then $f(x)$ is integrally closed at p.

If P is a prime ideal in the Dedekind ring A let $v_P: A \rightarrow \boldsymbol{Z} \cup \{\infty\}$ denote the corresponding normalized valuation. Let $d(g)$ and $\operatorname{Disc}(g)$ denote the degree and discriminant of a polynomial $g(x)$.

THEOREM. *Suppose that $f(x) \in A[x]$ is a monic polynomial that satisfies*

(a) $f(x) \equiv \Pi g_i(x)^{e_i} \bmod P$

(b) $v_P(\operatorname{Disc}(f)) = \Sigma_i (e_i - 1) d(g_i)$

where the $g_i(x) \in (A/P)[x]$ are distinct monic, irreducible and separable polynomials. Then $f(x)$ is integrally closed at P. Moreover, $p \nmid e_i$ and $A_P[x]/(f(x))$ is isomorphic to a product of discrete valuation rings that are tamely ramified over A_P.

The proof given in the third section is an easy consequence of a purely local result given in the second section. The first section recalls some basic formulas concerning resultants.

REMARKS. (1) It is a standard fact that if $f(x)$ is integrally closed and tamely ramified at P then conditions (a) and (b) must hold. If the characteristic of A/P is larger than $n = d(f)$ then the ramification has to be tame. Thus the test above usually determines the power of P in the discriminant of the root field in the case in which char $(A/P) > n$: it can fail only if $v_P(\mathrm{Disc}\,(f)) \geqq 4$.

(2) The condition that $f(x)$ be integrally closed at P is equivalent to saying that every ideal in $A[x]/(f(x))$ lying over P is invertible, or to saying that the index (in the sense of [2], p. 10) of $A[x]/(f(x))$ in the maximal order in $K[x]/(f(x))$ is prime to P (where K is the fraction field of A).

1. Resultants. Let $f(x)$ and $g(x)$ be polynomials with coefficients in any ring and let $R(f, g)$ denote their resultant (which could be defined, for instance, as the determinant of the "Sylvester matrix" formed from the coefficients). Let $L(g)$ denote the leading coefficient of the polynomial $g(x)$.

The following properties of the resultant $R(f, g)$ are standard and will be used freely below. Proofs can be found in [1] and [5].

R1. $R(f, g) = L(g)^{d(f)} \prod_{i=1}^{d(g)} f(\alpha_i)$ if $\alpha_1, \cdots, \alpha_{d(g)}$ are the roots of $g(x)$
$\quad = L(g)^{d(f)}$ if $d(g) = 0$

R2. $R(g, f) = (-1)^{d(f)d(g)} R(f, g)$

R3. $R(fg, h) = R(f, h)R(g, h)$

R4. $R(f, g) = L(g)^{d(f)-d(r)} R(r, g)$ if $f = qg + r$

R5. there exist polynomials $a(x)$, $b(x)$ such that $R(f, g) = af + bg$

R6. $\mathrm{Disc}\,(f) = (-1)^{d(f)(d(f)-1)/2} R(f, f')$

R7. $\mathrm{Disc}\,(fg) = \mathrm{Disc}\,(f)\,\mathrm{Disc}\,(g) R(f, g)^2$.

REMARK. The resultant $R(f, g)$ can be efficiently computed by forming a "polynomial remainder sequence" ([3]) $f_1 = f, f_2 = g, f_3, \cdots$ with

$$c_i f_i = d_i f_{i+1} + f_{i+2},\ \deg\,(f_{i+2}) < \deg\,(f_{i+1})\ .$$

The relationship R4 then can be used to express $R(f_i, f_{i+1})$ in terms of $R(f_{i+1}, f_{i+2})$. It is easy to check that this algorithm can be used to compute the discriminant of a polynomial of degree n in $O(n^2)$ steps, as opposed to the usual algorithms (e.g., taking the determinant of the Sylvester matrix or of the power sum matrix) which take $O(n^3)$ steps.

2. A local result. Throughout this section A will be a discrete valuation ring with valuation $v: A \to \boldsymbol{Z} \cup \{\infty\}$, uniformizing parameter π, and residue field k of characteristic p. Moreover let $f(x)$ be a monic polynomial with coefficients in A that satisfies

(a)′ $f(x) \equiv g(x)^e \bmod \pi$, where $\bar{g}(x) \in k[x]$ is irreducible and separable

(b)′ $v(\mathrm{Disc}\,(f)) = d(f) - d(g) = (e-1)d(g)$.

Let B_f denote the ring $A[x]/(f(x))$. It is easy to show ([4], Lemma 4 of Chapter I, § 6) that B_f is a local ring with unique maximal ideal $(\pi, g(x))$ and residue field $k[x]/(\bar{g}(x))$. The goal of this section is to show that (a)′ and (b)′ imply that B_f is a discrete valuation ring.

We follow the pattern of [4] and use the fact that a local noetherian ring is a discrete valuation ring if its maximal ideal is principal and is generated by a nonnilpotent element ([4], Prop. 2 of Chapter I, § 2). In fact we will show that π is in the ideal generated by $g(x)$ so that the maximal ideal is $(\pi, g(x)) = (g(x))$ and the ring must be a discrete valuation ring as claimed.

Use (a)′ to define a polynomial $h(x)$ by

$$f(x) = g(x)^e + \pi h(x) .$$

LEMMA. $v(R(g, h)) = 0$.

Assume this lemma for the moment. By the definition of $h(x)$, R4, and R3 it follows that $v(R(f, h)) = 0$. By R5 it follows that there exist $a(x), b(x) \in A[x]$ such that

$$1 = af + bh .$$

Now work in the ring $B_f = A[x]/(f(x))$. We have

$$1 = b(x)h(x) \qquad g(x)^e = -\pi h(x)$$

so that $\pi = -b(x)g(x)^e$. Hence the maximal ideal in B_f is generated by $g(x)$. This reduces the proof of the assertion that B_f is a discrete valuation ring to the proof of the lemma.

Proof of the lemma. Put $n = d(f)$, $m = d(g)$. By (b)′ together with R6

$$v(R(f, f')) = v(R(g^e + \pi h, eg'g^{e-1} + \pi h')) = n - m .$$

Note that it is clear from this formula that e is prime to p. Indeed, if p divides e then the second term above is divisible by π so that by R1 and R3 the valuation would be at least n.

Without loss of generality we can assume that A is complete. Since

$$f' \equiv eg'g^{e-1} \bmod \pi$$

and since eg' is relatively prime to g^{e-1}($\bar{g}$ is irreducible and separable) it follows from Hensel's lemma that we can find polynomials $a(x)$ and $b(x)$ such that

$$f' = (eg' + \pi a)(g^{e-1} + \pi b)$$

with $d(b) < d(g^{e-1})$. Substituting in * yields

$$** \qquad n - m = v(R(g^e + \pi h, eg' + \pi a)) + v(R(g^e + \pi h, g^{e-1} + \pi b)) .$$

Now apply the obvious fact that if the coefficients of two pairs of monic polynomials are congruent mod π then their resultants are congruent mod π. This shows that the first term on the right of ** is zero since

$$v(R(g, eg')) = 0 .$$

In the second term rearrange to take advantage of R4:

$$\begin{aligned} v(R(g^e + \pi h, g^{e-1} + \pi b)) &= v(R(g(g^{e-1} + \pi b) + \pi(h - bg), g^{e-1} + \pi b)) \\ &= v(R(\pi, g^{e-1} + \pi b)) + v(R(h - bg, g^{e-1} + \pi b)) \\ &= m(e - 1) + v(R(h - bg, g^{e-1} + \pi b)) . \end{aligned}$$

Since $R(h - bg, g^{e-1} + \pi b) \equiv R(h - bg, g)^{e-1} \equiv R(h, g)^{e-1} \bmod \pi$ we are forced to conclude that $v(R(h, g)) = 0$ which finishes the proof of the lemma.

The above results can be summarized as follows:

PROPOSITION. *Suppose that $f(x)$ is a monic polynomial with coefficients in a discrete valuation ring and that $f(x)$ satisfies*

(a)′ $f(x) \equiv g(x)^e \bmod \pi$, *where $g(x)$ is irreducible and separable* mod π,

(b)′ $v(\mathrm{Disc}\,(f)) = (e - 1)d(g)$.

Then $p \nmid e$ and $B_f = A[x]/(f(x))$ is a discrete valuation ring with residue field $k[x]/(\bar{g}(x))$ and maximal ideal $(g(x))$.

COROLLARY. *With the above notation, $f(x)$ is irreducible, B_f is integrally closed, and B_f is tamely ramified over A.*

Proof. As in Chapter I, § 6, corollary to Proposition 15 of [4].

REMARKS. (1) It can be shown that the irreducibility criterion above reduces to the Eisenstein irreducibility criterion if $e = 1$ and $d(f)$ is prime to p.

(2) It is clear from the proof of the lemma that the valuation of the discriminant given in (b)′ is in fact a lower bound on the discriminant of a polynomial that factors mod π as in (a)′.

3. Proof of the theorem. Now let the notation be as in the statement of the theorem: A is a Dedekind ring with prime ideal

P, v_P is the corresponding valuation, A_P is the completion of A at P, and $f(x)$ is a monic irreducible polynomial satisfying (a) and (b).

By Hensel's lemma we can find polynomials $G_i(x) \in A_P[x]$ such that

$$G_i(x) \equiv g_i(x)^{e_i} \bmod P$$
$$f(x) = \Pi G_i(x) .$$

By remark (2) above

$$v_P(\mathrm{Disc}\,(G_i)) \geqq (e_i - 1)d(g_i) .$$

The iteration of R7 shows that the discriminant of a product is divisible by the product of the discriminants so that

$$v_P(\mathrm{Disc}\,(f)) \geqq \Sigma v_P(\mathrm{Disc}\,(G_i)) \geqq \Sigma(e_i - 1)d(g_i) = v_P(\mathrm{Disc}\,(f))$$

(using the hypothesis (b)). Therefore we must have equality throughout and $v_P(\mathrm{Disc}\,(G_i)) = (e_i - 1)d(g_i)$. The proposition of the preceding section applies to the polynomial $G_i(x)$ and we conclude that

$$A_P[x]/(f(x)) \simeq \Pi A_P[x]/(G_i(x))$$

is a product of discrete valuation rings and that $f(x)$ is integrally closed at P. Also the e_i's are prime to p and $f(x)$ is tamely ramified at P. This finishes the proof of the theorem.

ACKNOWLEDGMENT. I would like to thank Bill Waterhouse for several valuable conversations concerning the above material.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.
2. J. W. S. Cassels and A. Frolich, *Algebraic Number Theory*, Academic Press, 1967.
3. G. E. Collins, *Subresultants and reduced polynomial remainder sequences*, J. Assoc. Comput. Math., **14** (1967), 128–142.
4. J. -P. Serre, *Corps Locaux*, Hermann, 1968.
5. R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math., **12** (1962), 1099–1106.
6. H. Zassenhaus, *On Hensel Factorization II*, Symposia Mathematica, vol. XV, (1975), 499–513.

Received December 22, 1978.

PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802