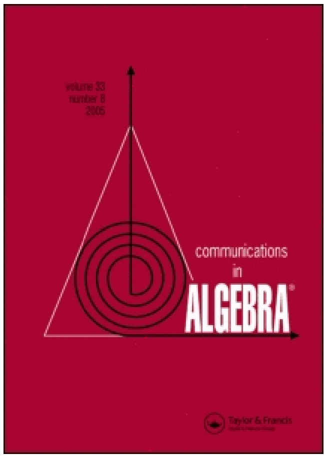

Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713597239

A Generalization of Dedekind Criterion

To cite this Article: , 'A Generalization of Dedekind Criterion', Communications in Algebra, 35:5, 1479 - 1486
To link to this article: DOI: 10.1080/00927870601168897
URL: http://dx.doi.org/10.1080/00927870601168897

Communications in Algebra®, 35: 1479–1486, 2007

ISSN: 0092-7872 print/1532-4125 online
DOI: 10.1080/00927870601168897

A GENERALIZATION OF DEDEKIND CRITERION

Munish Kumar and Sudesh K. Khanduja
Department of Mathematics, Panjab University, Chandigarh, India

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring A_K of algebraic integers of K and $f(x)$ be the minimal polynomial of θ over the field $\mathbb{Q}$ of rational numbers. For a rational prime p, let $\bar{f}(x) = \bar{g}_1(x)^{e_1} \ldots \bar{g}_r(x)^{e_r}$ be the factorization of the polynomial $\bar{f}(x)$ obtained by replacing each coefficient of $f(x)$ modulo p into product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $g_i(x)$ monic. In 1878, Dedekind proved that if p does not divide $[A_K : \mathbb{Z}[\theta]]$, then $pA_K = \wp_1^{e_1} \ldots \wp_r^{e_r}$, where $\wp_1, \ldots, \wp_r$ are distinct prime ideals of A_K, $\wp_i = pA_K + g_i(\theta)A_K$ with residual degree $f(\wp_i/p) = \deg \bar{g}_i(x)$. He also gave a criterion which says that p does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if for each i, we have either $e_i = 1$ or $\bar{g}_i(x)$ does not divide $\overline{M}(x)$ where $M(x) = \frac{1}{p}(f(x) - g_1(x)^{e_1} \ldots g_r(x)^{e_r})$. The analog of the above result regarding the factorization in $A_{K'}$ of any prime ideal $\mathfrak{p}$ of A_K is in fact known for relative extensions K'/K of algebraic number fields with the condition "$p \nmid [A_K : \mathbb{Z}[\theta]]$" replaced by the assumption "every element of $A_{K'}$ is congruent modulo $\mathfrak{p}$ to an element of $A_K[\theta]^{(\dagger)}$". In this article, our aim is to give a criterion like the one given by Dedekind which provides a necessary and sufficient condition for assumption (†) to be satisfied.

Key Words: Factorization of prime ideals; Ramification and extension theory.

2000 Mathematics Subject Classification: 11S15; 11Y05.

1. INTRODUCTION

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ an algebraic integer and $f(x)$ be the minimal polynomial of θ over the field $\mathbb{Q}$ of rational numbers. Let A_K denote the ring of algebraic integers of K. The determination of the prime ideal decomposition in A_K of any rational prime p is one of the major problems in Algebraic Number Theory and is related to the decomposition of the polynomial $\bar{f}(x)$ obtained by replacing each coefficient of $f(x)$ by its residue modulo p. In 1878, Dedekind proved the following result in this direction.

Dedekind's Theorem. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $f(x)$ as the minimal polynomial of the algebraic integer θ over $\mathbb{Q}$. Let p be a rational prime. Let $\bar{f}(x) = \bar{g}_1(x)^{e_1} \ldots \bar{g}_r(x)^{e_r}$ be the factorization of $\bar{f}(x)$ as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, with $g_i(x)$ monic polynomials belonging to $\mathbb{Z}[x]$. Suppose that p does not divide the index of the subgroup $\mathbb{Z}[\theta]$ in A_K;

Received January 3, 2006; Revised February 3, 2006; Communicated by U. Otterbeck.
Address correspondence to Sudesh K. Khanduja, Department of Mathematics, Panjab University, Chandigarh 160014, India; E-mail: skhand@pu.ac.in

then $pA_K = \wp_1^{e_1} \ldots \wp_r^{e_r}$, where $\wp_1, \ldots, \wp_r$ are distinct prime ideals of A_K, $\wp_i = pA_K + g_i(\theta)A_K$ with residual degree $f(\wp_i/p) = \deg \bar{g}_i(x)$ for all i.

Dedekind also gave a criterion (stated below) to verify when the condition "p does not divide $[A_K : \mathbb{Z}[\theta]]$" is satisfied (cf. Cohen, 1993, Theorem 6.1.4; Dedekind, 1878; Montes and Nart, 1992).

Dedekind Criterion. Let $K = \mathbb{Q}(\theta)$, $f(x)$, and $g_1(x), \ldots, g_r(x)$ be as in the above theorem. Let $M(x)$ denote the polynomial $\frac{1}{p}(f(x) - g_1(x)^{e_1} \ldots g_r(x)^{e_r})$ with coefficients from $\mathbb{Z}$. Then p does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if for each i, we have either $e_i = 1$ or $\bar{g}_i(x)$ does not divide $\overline{M}(x)$.

It can be easily verified that p does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if $A_K \subseteq \mathbb{Z}_{(p)}[\theta]$, $\mathbb{Z}_{(p)}$ being the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. Keeping this in mind, the following result is a generalization of Dedekind's Theorem stated above (for proof, see Janusz, 1996, Chap. I, Theorem 7.4).

Generalized Dedekind Theorem. Let R be a Dedekind domain with field of fractions K. Let L be a finite separable extension of K and S be the integral closure of R in L. Suppose that θ belonging to S generates the extension L/K and $f(x)$ in $R[x]$ is the minimal polynomial of θ over K. Let $\mathfrak{p}$ be a nonzero prime ideal of R, $R_\mathfrak{p}$ be the localization of R at $\mathfrak{p}$ and $S_\mathfrak{p}$ be the integral closure of $R_\mathfrak{p}$ in L. For any $g(x)$ in $R[x]$, let $\bar{g}(x)$ denote the polynomial obtained by replacing each coefficient of $g(x)$ by its image under the canonical homomorphism from R onto $R/\mathfrak{p}$. Let $\bar{f}(x) = \bar{g}_1(x)^{e_1} \ldots \bar{g}_r(x)^{e_r}$ be the factorization of $\bar{f}(x)$ into powers of distinct irreducible polynomials over $R/\mathfrak{p}$ with each $g_i(x)$ monic. Assume that $S_\mathfrak{p} = R_\mathfrak{p}[\theta]^{(\dagger)}$. Then

$$\mathfrak{p}S = \wp_1^{e_1} \ldots \wp_r^{e_r}$$

where $\wp_1, \ldots, \wp_r$ are distinct prime ideals of S, $\wp_i = \mathfrak{p}S + g_i(\theta)S$ with residual degree $f(\wp_i/\mathfrak{p}) = \deg \bar{g}_i(x)$.

In order to apply the last theorem in an effective way one needs a criterion to decide when a prime ideal $\mathfrak{p}$ of R satisfies assumption ($\dagger$) of this theorem. This has led us to consider the following problem.

How can we formulate a criterion like Dedekind Criterion which gives some necessary and sufficient conditions so that assumption ($\dagger$) is satisfied, that is, $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$? As $R_\mathfrak{p}$ is a discrete valuation ring, a solution to the above problem is given by the following theorem which is the main result of this article.

Theorem 1.1. *Let R be a Dedekind domain with quotient field K. Let $L = K(\theta)$, S and $f(x)$ be as in Generalized Dedekind Theorem. Let $\mathfrak{p}$ be a nonzero prime ideal of R, π_0 be a prime element of the discrete valuation ring $R_\mathfrak{p}$ and let $g(x) \mapsto \bar{g}(x)$ denote the canonical homomorphism from $R_\mathfrak{p}[x]$ onto $(R/\mathfrak{p})[x]$. Let $S_\mathfrak{p}$ the integral closure of $R_\mathfrak{p}$ in L. Suppose that $\bar{f}(x) = \bar{g}_1(x)^{e_1} \ldots \bar{g}_r(x)^{e_r}$ is the factorization of $\bar{f}(x)$ into powers of distinct irreducible polynomials over $R/\mathfrak{p}$ with $g_i(x)$ monic in $R[x]$. If $M(x)$ belonging* *to $R_{\mathfrak{p}}[x]$ is defined by*

$$f(x) = g_1(x)^{e_1} \dots g_r(x)^{e_r} + \pi_0 M(x), \tag{1}$$

then $S_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$ if and only if $\bar{g}_i(x)^{e_i - 1}$ is coprime with $\overline{M}(x)$ for $1 \leq i \leq r$.

Remark. It may be pointed out that our proof of Theorem 1.1 is entirely on different lines from the proof of the particular case of this theorem when $R = \mathbb{Z}$.

2. SOME PRELIMINARY RESULTS

Let R be a Dedekind domain having quotient field K, $L = K(\theta)$ be a finite separable extension of K, with θ in the integral closure S of R in L. Recall that the conductor of $R[\theta]$ in S is given by $\{x \in R[\theta] \mid xS \subseteq R[\theta]\}$. It is a nonzero ideal of S (cf. Narkiewicz, 1990, Proposition 4.12; Neukirch, 1999, Chapter I, Lemma 2.9). Indeed there exist $d \in R$, $d \neq 0$ such that

$$dS \subseteq R[\theta]. \tag{2}$$

3. PROOF OF THEOREM 1.1 FOR COMPLETE DISCRETE RINGS

In what follows for any valuation v of a field K, R_v will denote its valuation ring, m_v the maximal ideal of R_v. The residue field R_v/m_v will be denoted by $\overline{K}$ when the underlying valuation is clear. For any element ξ in R_v, $\bar{\xi}$ will denote its v-residue, that is, the image of ξ under the canonical homomorphism from R_v onto R_v/m_v.

In this section, we will prove Theorem 1.1 when $R = R_v$ is the valuation ring of a complete discrete valuation v of K with value group $\mathbb{Z}$ and $L = K(\theta)$ is a finite separable extension of K of degree n with θ in the valuation ring R_w of the unique prolongation w of v to L. In view of Hensel's lemma, the minimal polynomial $f(x)$ of θ over K can be expressed as

$$f(x) = \phi(x)^e + \pi_0 M(x), \tag{3}$$

where $\phi(x)$ is a monic polynomial in $R_v[x]$ such that $\bar{\phi}(x)$ is irreducible over the residue field of v and π_0 is a prime element of v (see Neukirch, 1999, Chapter II, 4.6). It is required to be shown that

$$R_w = R_v[\theta] \Leftrightarrow \text{either } e = 1 \text{ or } e > 1 \quad \text{and} \quad \bar{\phi}(x) \nmid \overline{M}(x). \tag{4}$$

Observe that $\bar{\phi}(x)$ being the minimal polynomial of the w-residue $\bar{\theta}$ of θ over $\overline{K}$, does not divide $\overline{M}(x)$ if and only if $\overline{M}(\bar{\theta}) \neq \bar{0}$, which is the same as saying that $w(M(\theta)) = 0$. Therefore, on substituting $x = \theta$ in (3), it is clear that

$$\bar{\phi}(x) \nmid \overline{M}(x) \Leftrightarrow w(\phi(\theta)) = \frac{w(\pi_0)}{e} = \frac{1}{e}. \tag{5}$$

If $e = 1$, then $\bar{\theta}$ is a root of the irreducible polynomial $\bar{f}(x) \in \overline{K}[x]$ and $\{\bar{1}, \bar{\theta}, \dots, \bar{\theta}^{n-1}\}$ is a linearly independent set over $\overline{K}$. This shows that for any element $\sum_{i=0}^{n-1} a_i\theta^i$ belonging to $K(\theta)$, $a_i \in K$, we have $w(\sum_{i=0}^{n-1} a_i\theta^i) = \min_i v(a_i)$; consequently, $R_w = R_v[\theta]$ in this case.

Assume now that $e > 1$ and $\bar{\phi}(x) \nmid \overline{M}(x)$, hence $w(\phi(\theta)) = 1/e$ in view of (5). As the value group of v is $\mathbb{Z}$, we see that the index of ramification $e(w/v) \geq e$ and residue degree $f(w/v) \geq \deg \bar{\phi}(x)$. Since $n = e(\deg \bar{\phi}(x))$, it follows that $e(w/v) = e$ and $f(w/v) = \deg \bar{\phi}(x)$. So $\phi(\theta)$ is a prime element of w and the residue field of w is $\overline{K}(\bar{\theta}) = \overline{K}[\bar{\theta}]$. In particular the polynomial ring $R_v[\theta]$ contains a set of representatives of R_w/m_w. Therefore, any element u belonging to the complete discrete valuation ring R_w can be written as

$$u = h_0(\theta) + h_1(\theta)\phi(\theta) + h_2(\theta)\phi(\theta)^2 + \cdots, \qquad h_i(\theta) \in R_v[\theta]. \tag{6}$$

By virtue of (2), we see that there exists a non-negative integer j such that the set $\{\alpha \in R_w \mid w(\alpha) \geq \frac{j}{e}\}$ is contained in $R_v[\theta]$. It now follows from (6) that any element u of R_w belongs to $R_v[\theta]$ as desired.

Conversely, assume that $R_w = R_v[\theta]$ and $e > 1$. It is to be shown that $\bar{\phi}(x) \nmid \overline{M}(x)$ which in view of (5) is equivalent to requiring that

$$w(\phi(\theta)) = \frac{1}{e}. \tag{7}$$

By hypothesis $R_w = R_v[\theta]$, so $\bar{\theta}$ will generate the residue field $\overline{L}/\overline{K}$. It follows that $e(w/v) = \frac{[L:K]}{\deg \bar{\phi}(x)} = e$. Therefore (7) is proved as soon as we show that $e'w(\phi(\theta)) < 1$ for all positive integers $e' < e$. Suppose to the contrary that there exists an integer $e' < e$ such that $e'w(\phi(\theta)) \geq 1$, that is, $w(\frac{\phi(\theta)^{e'}}{\pi_0}) \geq 0$, which is impossible as $R_w = R_v[\theta]$ and $\frac{\phi(\theta)^{e'}}{\pi_0}$ does not belong to $R_v[\theta]$. This completes the proof of (7) and hence the proof of Theorem 1.1 in case R_v is a complete discrete valuation ring.

4. REDUCTION OF THE PROBLEM TO COMPLETE BASE FIELDS

For any valued field (K, v), $(\widehat{K}, \hat{v})$ will denote its completion. In this section, v is a fixed discrete valuation of a field K and A is the algebraic closure of the completion $\widehat{K}$ of K with respect to v. The unique prolongation of $\hat{v}$ to A will again be denoted by $\hat{v}$. For ξ belonging to A with $\hat{v}(\xi) \geq 0$, $\bar{\xi}$ will denote its image in the residue field of the valuation of A extending $\hat{v}$. For a polynomial $F(x)$ with coefficients in the valuation ring $R_{\hat{v}}$ of $\hat{v}$, $\overline{F}(x)$ will have its usual meaning.

With the above notations, we prove the following theorem.

Theorem 4.1. *Let (K, v) be a discrete valued field and $L = K(\theta)$ be a finite separable extension of K, with θ in the integral closure S of R_v in L. Suppose that the minimal polynomial $f(x)$ of θ over K has the factorization $f(x) = \prod_{i=1}^{s} F_i(x)$ into monic irreducible polynomials over $\widehat{K}$. Let θ_i be a root of $F_i(x)$ and w_i be the prolongation of v to L defined by*

$$w_i\Big(\sum_j a_j\theta^j\Big) = \hat{v}\Big(\sum_j a_j\theta_i^j\Big), \qquad a_j \in K. \tag{8}$$

Then $S = R_v[\theta]$ *if and only if* $\overline{F}_i(x)$ *and* $\overline{F}_j(x)$ *are coprime polynomials for* $i \neq j$ *and* $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$ *for* $1 \leq i \leq s$.

Proof. It is known that $w_1, \ldots, w_s$ are all the distinct prolongations of v to L (cf. Neukirch, 1999, Chapter II, 8.1, 8.2). Also S is a Dedekind domain with unique factorization having s maximal ideals, say $\wp_1, \ldots, \wp_s$ with $\wp_i = m_{w_i} \cap S$ (see Borevich and Shafarevich, 1966, Chapter 3, Sec. 4, Theorem 7). Since $F_i(x)$ is an irreducible polynomial over the completion $\widehat{K}$, in view of Hensel's Lemma there exists a positive integer e_i and a monic polynomial $\phi_i(x) \in R_v[x]$, with $\bar{\phi}_i(x)$ irreducible over the residue field of v such that $\overline{F}_i(x) = \bar{\phi}_i(x)^{e_i}$.

Suppose first that $S = R_v[\theta]$. We now show that $\overline{F}_i(x)$ and $\overline{F}_j(x)$ are relatively prime polynomials when $i \neq j$. By Chinese Remainder Theorem, there exists an element $\alpha \in S$ such that $\alpha \equiv 0 \pmod{\wp_i}$ and $\alpha \equiv 1 \pmod{\wp_j}$. Since $S = R_v[\theta]$, there exists $h(x) \in R_v[x]$ such that $\alpha = h(\theta)$. Then

$$w_i(h(\theta)) > 0, \qquad w_j(h(\theta) - 1) > 0. \tag{9}$$

Keeping in mind (8), we can rewrite (9) as $\hat{v}(h(\theta_i)) > 0$ and $\hat{v}(h(\theta_j) - 1) > 0$, that is,

$$\bar{h}(\bar{\theta}_i) = \bar{0}, \qquad \bar{h}(\bar{\theta}_j) = \bar{1}. \tag{10}$$

As each $\bar{\phi}_l(x)$ is irreducible over the residue field of v and has $\bar{\theta}_l$ as a root, it follows from (10) that $\bar{\phi}_i(x)$ divides $\bar{h}(x)$ and $\bar{\phi}_j(x)$ does not divide $\bar{h}(x)$. Therefore $\bar{\phi}_i(x) \neq \bar{\phi}_j(x)$, which proves that $\overline{F}_i(x)$ and $\overline{F}_j(x)$ are relatively prime.

It remains to be shown that $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$, $1 \leq i \leq s$. Keeping in mind that $S = R_v[\theta]$, the homomorphism from $R_v[\theta]$ induced by mapping θ to θ_i indeed gives an isomorphism from $S/\wp_i$ onto the residue field of $\hat{w}_i$. Therefore the ring $R_v[\theta_i]$ contains a prime element π_i (say) of $\hat{w}_i$ and a set of representatives for the residue field of $\hat{w}_i$. Consequently, any element $u \in R_{\hat{w}_i}$ can be written as

$$u = h_0(\theta_i) + h_1(\theta_i)\pi_i + h_2(\theta_i)\pi_i^2 + \cdots, \qquad h_l(\theta_i) \in R_v[\theta_i], \quad l \geq 0. \tag{11}$$

By virtue of (2), there exists an integer $t \geq 0$ such that the set $\{\alpha \in R_{\hat{w}_i} \mid \hat{w}_i(\alpha) \geq t\hat{v}(\pi_i)\}$ is contained in $R_{\hat{v}}[\theta_i]$. It now follows from (11) that

$$u = h_0(\theta_i) + \cdots + h_t(\theta_i)\pi_i^t + \beta, \qquad \beta \in R_{\hat{v}}[\theta_i].$$

As π_i and $h_l(\theta_i)$ belong to $R_{\hat{v}}[\theta_i]$, we conclude that $u \in R_{\hat{v}}[\theta_i]$, which proves the desired equality.

Conversely, suppose that $\overline{F}_i(x), \overline{F}_j(x)$ are relatively prime and $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$ for $1 \leq i \neq j \leq s$. To establish $R_v[\theta] = S$, we prove that none of the ideals $\wp_i$ divides the conductor $\mathfrak{C}$ of $R_v[\theta]$ in S. This will prove that the conductor $\mathfrak{C}$ is a unit ideal.

Let n_i denote the residue degree of w_i/v and π_0 a prime element of v, so that

$$\pi_0 S = \wp_1^{n_1} \ldots \wp_s^{n_s}. \tag{12}$$

We first verify that ideals $\phi_i(\theta)S$ for $1 \leq i \leq s$ are proper ideals which are pairwise comaximal. Since $\overline{F}_i(x) = \bar{\phi}_i(x)^{e_i}$, and $\overline{F}_j(x) = \bar{\phi}_j(x)^{e_j}$ are relatively prime, there exists $u_i(x)$, $u_j(x)$ in $R_v[x]$ such that

$$\bar{\phi}_i(x)\bar{u}_i(x) + \bar{\phi}_j(x)\bar{u}_j(x) = \bar{1};$$

consequently, $\phi_i(\theta)u_i(\theta) + \phi_j(\theta)u_j(\theta) = 1 + \pi_0 u_{ij}(\theta)$ for some $u_{ij}(x) \in R_v[x]$ which proves that $\phi_i(\theta)S + \phi_j(\theta)S = S$. Using the equalities $\overline{F}_i(x) = \bar{\phi}_i(x)^{e_i}$ and $F_i(\theta_i) = 0$, we see that $\bar{\phi}_i(\bar{\theta}_i) = \bar{0}$. Therefore, it follows from (8) that $w_i(\phi_i(\theta)) = \hat{v}(\phi_i(\theta_i)) > 0$; consequently, there exist positive integers t_i such that

$$\phi_i(\theta)S = \wp_i^{t_i}, \qquad 1 \leq i \leq s. \tag{13}$$

Set

$$I = \wp_2^{n_2} \ldots \wp_s^{n_s}, \qquad \xi = \phi_2^{n_2}(\theta) \ldots \phi_s^{n_s}(\theta). \tag{14}$$

It is clear from (13) that the element ξ of $R_v[\theta]$ belongs to $I \backslash \wp_1$. Keeping in mind (2), there exists a non-negative integer m such that

$$\pi_0^m S \subset R_v[\theta]. \tag{15}$$

Our claim is that $\xi^m \in \mathfrak{C}$; since ξ does not belong to $\wp_1$, this will imply that $\wp_1$ does not divide $\mathfrak{C}$. Arguing similarly for other $\wp_i$, $i \geq 2$, we shall conclude that $\mathfrak{C}$ is not divisible by any $\wp_i$, so $\mathfrak{C}$ will be the unit ideal, that is, $S = R_v[\theta]$.

It only remains to verify the claim. Let α be any element of S. Using the hypothesis $R_{\hat{w}_1} = R_{\hat{v}}[\theta_1]$ and the fact that R_v is dense in $R_{\hat{v}}$, we see that there exists $\beta \in R_v[\theta]$ such that $w_1(\alpha - \beta) \geq n_1 m$, consequently $\alpha - \beta$ belong to $\wp_1^{n_1 m}$. It follows from (12), (14), and (15) that

$$(\alpha - \beta)\xi^m \in \wp_1^{n_1 m} I^m = (\pi_0 S)^m \subset R_v[\theta].$$

Since β and ξ^m are in $R_v[\theta]$, we see that $\alpha\xi^m \in R_v[\theta]$ as desired.

5. DEDUCTION OF THEOREM 1.1

Let v be a discrete valuation of the field K with valuation ring $R_\mathfrak{p}$ and π_0 be a prime element of v. We retain the notations introduced in the opening lines of Section 4. Let

$$f(x) = F_1(x) \ldots F_s(x) \tag{16}$$

be the factorization of $f(x)$ into monic irreducible polynomials over $\widehat{K}$. Let θ_i be a root of $F_i(x)$ and w_i denote the prolongation of v to L defined by (8). On applying Theorem 4.1, we see that $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$ if and only if $r = s$ and $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$ for $1 \leq i \leq s$. In case $r = s$, if necessary after permuting the indices, we can write

$$F_i(x) = g_i(x)^{e_i} + \pi_0 M_i(x), \qquad M_i(x) \in R_{\hat{v}}[x];$$

consequently, in view of (16) and (1), there exists $\psi(x) \in R_{\hat{v}}[x]$ such that

$$M(x) = \sum_{i=1}^{r} \left(\prod_{j=1, j\neq i}^{r} g_j(x)^{e_j} \right) M_i(x) + \pi_0 \psi(x). \tag{17}$$

By virtue of the result proved in the third section, we have $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$ for any $i \geq 1$ if and only if $\bar{g}_i(x)^{e_i - 1}$ and $\overline{M}_i(x)$ are coprime. Therefore it now follows from (17) that when $r = s$, then $R_{\hat{w}_i} = R_{\hat{v}}[\theta_i]$ if and only if $\bar{g}_i(x)^{e_i-1}$ and $\overline{M}(x)$ are coprime for $1 \leq i \leq r$. Thus the theorem is proved once we show that in case $r < s$, then there exists an index i such that $e_i > 1$ and $\bar{g}_i(x)$ divides $\overline{M}(x)$.

Assume that $r < s$, so there exist distinct indices k and l such that $\overline{F}_k(x)$ and $\overline{F}_l(x)$ are not coprime. If necessary after renaming, assume that

$$\bar{g}_k(x) \mid \overline{F}_k(x) \qquad \text{and} \qquad \bar{g}_k(x) \mid \overline{F}_l(x). \tag{18}$$

Therefore $e_k > 1$. The proof is complete as soon as it is shown that $\bar{g}_k(x) \mid \overline{M}(x)$. For each i, $1 \leq i \leq s$, there exists $\phi_i(x) \in \{g_1(x), \ldots, g_r(x)\}$ and $H_i(x) \in R_{\hat{v}}[x]$ such that

$$F_i(x) = \phi_i(x)^{d_i} + \pi_0 H_i(x), \qquad d_i \geq 1. \tag{19}$$

Using (1) and (19), we see that there exists $\psi_1(x) \in R_{\hat{v}}[x]$ such that

$$\begin{aligned} \prod_{i=1}^{r} g_i(x)^{e_i} + \pi_0 M(x) &= \prod_{i=1}^{s} \phi_i(x)^{d_i} + \pi_0 \sum_{i=1}^{s} \left(\prod_{j=1, j\neq i}^{s} \phi_j(x)^{d_j} \right) H_i(x) + \pi_0^2 \psi_1(x) \\ &= \prod_{i=1}^{r} g_i(x)^{e_i} + \pi_0 \sum_{i=1}^{s} \left(\prod_{j=1, j\neq i}^{s} \phi_j(x)^{d_j} \right) H_i(x) + \pi_0^2 \psi_1(x) \end{aligned}$$

and hence $M(x) = \sum_{i=1}^{s} (\prod_{j=1, j\neq i}^{s} \phi_j(x)^{d_j}) H_i(x) + \pi_0 \psi_1(x)$. In view of (18) and (19), the last equality clearly shows that $\bar{g}_k(x)$ divides $\overline{M}(x)$ as desired.

Remark. Let $R_{\mathfrak{p}}[\theta]$ and $S_{\mathfrak{p}}$ be as in Theorem 1.1 and $\mathfrak{C}$ be the conductor of $R[\theta]$ in S. One can easily show that $S_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$ if and only if $\mathfrak{p}$ does not divide the norm ideal $N_{L/K}(\mathfrak{C})$. It is known that the above condition is equivalent to saying that every element of S is congruent to an element of $R[\theta]$ modulo $\mathfrak{p}S$ (for proof see Narkiewicz, 1990, Lemma 4.7).

ACKNOWLEDGMENTS

The authors are highly thankful to Dr. Peter Roquette Emeritus Professor Universität Heidelberg for having given us the idea for the proof of the main theorem. The financial support by University Grants Commission, New Delhi and National Board for Higher Mathematics, Mumbai is gratefully acknowledged.

REFERENCES

Borevich, Z. I., Shafarevich, I. R. (1966). *Number Theory*. Academic Press, Inc.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Berlin-Heidelberg: Springer-Verlag.

Dedekind, R. (1878). Uber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Göttingen Abhandlungen* 23:1–23.

Janusz, J. (1996). *Algebraic Number Fields*. Vol. 7. 2nd ed. American Mathematical Society.

Montes, J., Nart, E. (1992). On a theorem of ore. *J. Algebra* 146:318–334.

Narkiewicz, W. (1990). *Elementary and Analytic Theory of Algebraic Numbers*. 2nd ed. Springer-Verlag, Polish Scientific Publishers.

Neukirch, J. (1999). *Algebraic Number Theory*. Berlin Heidelberg: Springer-Verlag.