On a Theorem of Dedekind

Sudesh K. Khanduja[*], Munish Kumar
Department of Mathematics, Panjab University, Chandigarh-160014, India.
E-mail: skhand@pu.ac.in, msingla79@yahoo.com

Abstract

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 $\bar{f}(x) = \bar{g}_1(x)^{e_1}....\bar{g}_r(x)^{e_r}$ 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 monic irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$. Dedekind proved that if p does not divide $[A_K : \mathbb{Z}[\theta]]$, then the factorization of pA_K as a product of powers of distinct prime ideals is given by $pA_K = \mathfrak{p}_1^{e_1}....\mathfrak{p}_r^{e_r}$, with $\mathfrak{p}_i = pA_K + g_i(\theta)A_K$, and residual degree $f(\mathfrak{p}_i/p) = deg\ \bar{g}_i(x)$. In this paper we prove that if the factorization of a rational prime p in A_K satisfies the above mentioned three properties, then p does not divide $[A_K : \mathbb{Z}[\theta]]$. Indeed the analogue of the converse is proved for general Dedekind domains. The method of proof leads to a generalization of one more result of Dedekind which characterizes all rational primes p dividing the index of K.

2000 Subject Classification No: 11Y05, 11S15.
Key words and phrases: Factorization of prime ideals, Ramification and extension theory.

[*]All correspondence may be addressed to this author.

1. Introduction.

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. The problem of establishing effectively the decomposition of a rational prime p in A_K using the decomposition of $f(x)$ modulo p goes back to Kummer. For a rational prime p, let $\bar{f}(x) = \bar{g}_1(x)^{e_1}....\bar{g}_r(x)^{e_r}$ 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 [1] proved that if p does not divide $[A_K : \mathbb{Z}[\theta]]$, then $pA_K = \mathfrak{p}_1^{e_1}....\mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_1, ..., \mathfrak{p}_r$ are distinct prime ideals of A_K, $\mathfrak{p}_i = pA_K + g_i(\theta)A_K$ with residual degree $f(\mathfrak{p}_i/p) = deg\ \bar{g}_i(x)$. Dedekind also characterized those primes p which divide the index of $\mathbb{Z}[\theta]$ in A_K (henceforth referred to as index of θ) for all generating elements θ in A_K of the extension $K/\mathbb{Q}$. In this direction, he proved the following theorem (cf. [1], [6, Theorem 4.34]).

Theorem A. *Let K be an algebraic number field. Let $i(K)$ denote the greatest common divisor of the indices of all generating elements in A_K of the extension $K/\mathbb{Q}$. A rational prime p divides $i(K)$ if and only if for some natural number f, the number of prime ideals of A_K lying over p with residual degree f, is strictly greater than the number of monic irreducible polynomials of degree f over the field with p elements.*

It can be easily verified that for a generating element θ of $K/\mathbb{Q}$, a rational prime p does not divide the index of θ 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 theorem stated below is a generalization of the result of Dedekind stated in the opening lines of the paper (see [2, Chapter I, Theorem 7.4]).

Theorem B. *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. Let $f(x)$ in $R[x]$ be the minimal polynomial of a generating element $\theta \in S$ of L/K. Let $\mathfrak{p}$ be a non-zero 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. Let $\bar{f}(x) = \bar{g}_1(x)^{e_1}....\bar{g}_r(x)^{e_r}$ be the factorization of the polynomial $\bar{f}(x)$ obtained by replacing each coefficient of $f(x)$ modulo $\mathfrak{p}$ into powers of distinct irreducible polynomials over $R/\mathfrak{p}$ with each $g_i(x)$ monic. If $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$, then*

$$\mathfrak{p}S = \wp_1^{e_1}....\wp_r^{e_r}, \ \wp_i = \mathfrak{p}S + g_i(\theta)S, \ f(\wp_i/\mathfrak{p}) = deg\ g_i(x) \tag{1}$$

with $\wp_1, ..., \wp_r$ distinct prime ideals of S.

The following question naturally arises.

Does the result of Theorem B hold with a hypothesis weaker than $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$?

In this paper, it is shown that the answer to the above question is the negative. Indeed we prove

Theorem 1.1. *Let $R, S, \mathfrak{p}, f(x)$ and $g_1(x), ..., g_r(x)$ be as in Theorem B. If $\mathfrak{p}S = \wp_1^{e_1}....\wp_r^{e_r}$ is the factorization of $\mathfrak{p}S$ into powers of distinct prime ideals of S with $\wp_i = \mathfrak{p}S + g_i(\theta)S$ and $f(\wp_i/\mathfrak{p}) = \deg g_i(x)$, then $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$.*

Let $\bar{f}(x) = \bar{g}_1(x)^{e_1}....\bar{g}_r(x)^{e_r}$ be as in Theorem B. Then there exists a polynomial $M(x)$ with coefficients in the localization $R_\mathfrak{p}$ of R at the prime ideal $\mathfrak{p}$ such that $f(x) = g_1(x)^{e_1}...g_r(x)^{e_r} + \pi_0 M(x)$, where π_0 is a prime element of $R_\mathfrak{p}$. It has been recently proved (as a generalization of the well known Dedekind Criterion stated in [5]) that the condition $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$ is the same as saying that for each i, $1 \leq i \leq r$, either $e_i = 1$ or $\bar{g}_i(x)$ does not divide $\bar{M}(x)$ (see [3]).

It may be pointed out that as shown in Lemma 2.1, the condition $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$ is equivalent to saying that $\mathfrak{p}$ does not divide $N_{L/K}(\mathfrak{C}_\theta)$, where the conductor $\mathfrak{C}_\theta$ of

$R[\theta]$ is defined by

$$\mathfrak{C}_\theta = \{x \in R[\theta] | \ \ xS \subset R[\theta]\}. \tag{2}$$

Using the method of proof of Theorem 1.1, we have extended Theorem A to all Dedekind domains with finite norm property. We shall denote by $i_{S/R}$ the greatest common divisor of the ideals $N_{L/K}(\mathfrak{C}_\theta)$, where θ runs over all generating elements belonging to S of the extension L/K and $\mathfrak{C}_\theta$ is as defined by (2).

In section 3, the following theorem is proved.

Theorem 1.2. *Let R be a Dedekind domain with finite norm property having quotient field K and S be the integral closure of R in a finite separable extension L of K. Let $\mathfrak{p}$ be a non-zero prime ideal of R with factorization $\wp_1^{e_1}....\wp_t^{e_t}$ as a product of powers of distinct prime ideals of S. Then $\mathfrak{p}$ does not divide $i_{S/R}$ if and only if there exist distinct monic irreducible polynomials $V_1, ..., V_t$ over $R/\mathfrak{p}$ satisfying* $\deg V_i =$ *residual degree of $\wp_i/\mathfrak{p}$ for $1 \leq i \leq t$.*

It may be remarked that in the particular case when $K = \mathbb{Q}(\theta)$ is an algebraic number field with discriminant d_K and $f(x)$ is the minimal polynomial of θ over $\mathbb{Q}$, then as is well known (see [6, Proposition 4.18])

$$N_{K/\mathbb{Q}}(\mathfrak{C}_\theta) = \frac{N_{K/\mathbb{Q}}(f'(\theta))}{d_K}\mathbb{Z} = [A_K : \mathbb{Z}[\theta]]^2\mathbb{Z};$$

consequently $i_{A_K/\mathbb{Z}}$ is the ideal of $\mathbb{Z}$ generated by $i(K)^2$ and hence Theorem 1.2 indeed generalizes Theorem A.

We shall apply Theorem 1.2 to obtain the following results, the analogues of which are already known for absolute extensions $K/\mathbb{Q}$ (cf. [6, Proposition 4.36]).

Theorem 1.3. *Let R, S, K, L be as in Theorem 1.2 and $\mathfrak{p}$ be a non-zero prime ideal of R. If $\mathfrak{p}$ divides $i_{S/R}$, then $\mid R/\mathfrak{p} \mid < [L : K]$.*

Corollary 1.4. *With R, S, K, L as above, assume in addition that L/K is a cubic extension. If $\mathfrak{p}$ is a prime ideal of R dividing $i_{S/R}$, then $\mid R/\mathfrak{p} \mid = 2$. A prime ideal $\mathfrak{p}$ of R divides $i_{S/R}$ if and only if $\mathfrak{p}S$ is a product of three distinct prime ideals of S.*

2. Proof of Theorem 1.1.

In what follows, R is a Dedekind domain with quotient field K and S the integral closure of R in finite separable extension L of K of degree n, $\mathfrak{p}$ is a non-zero prime ideal of R and $R_\mathfrak{p}, S_\mathfrak{p}$ are as in Theorem B.

The following lemma is already known (cf. [6, Lemma 4.32]). For reader's convenience, we prove it here.

Lemma 2.1. *Let θ belonging to S be a generating element of L/K and $\mathfrak{C}_\theta$ be the conductor of $R[\theta]$ defined by (2). The following conditions are equivalent for a non-zero prime ideal $\mathfrak{p}$ of R.*

(i) $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$;

(ii) $\mathfrak{p}$ *does not divide the ideal* $N_{L/K}(\mathfrak{C}_\theta)$;

(iii) $\mathfrak{p}S \cap R[\theta] = \mathfrak{p}[\theta]$.

Proof. It is known that S is a finite R-module (cf. [7, Chapter I, p. 45]). Let $\{u_1, ..., u_m\}$ be a system of generators of S as an R-module.

(i)⇒(ii) Keeping in mind the assumption $S_\mathfrak{p} = R_\mathfrak{p}[\theta]$, we can write

$$u_i = \sum_{j=0}^{n-1} a_{ij}\theta^j,\ a_{ij} \in R_\mathfrak{p},\ 1 \leq i \leq m,\ 0 \leq j \leq n-1.$$

So there exists $c \in R \backslash \mathfrak{p}$ such that $cu_i \in R[\theta]$ for $1 \leq i \leq m$. Hence $cS \subseteq R[\theta]$. As c belongs to $\mathfrak{C}_\theta \cap (R\backslash\mathfrak{p})$, it follows that $N_{L/K}(\mathfrak{C}_\theta)$ is not divisible by $\mathfrak{p}$, which proves that (i)⇒(ii).

(ii)⇒(i) We first show that

$$\mathfrak{C}_\theta \cap R \not\subseteq \mathfrak{p}. \tag{3}$$

Write $\mathfrak{C}_\theta = \mathfrak{Q}_1^{a_1}...\mathfrak{Q}_s^{a_s}$ as a product of powers of distinct prime ideals of S. Let $\mathfrak{q}_i$ denote the prime ideal of R lying below $\mathfrak{Q}_i$. By our assumption, $\mathfrak{p}$ does not divide $N_{L/K}(\mathfrak{C}_\theta)$ and thus none of the $\mathfrak{q}_i$ is $\mathfrak{p}$. As $\mathfrak{C}_\theta \cap R$ contains (and hence divides) $\mathfrak{q}_1^{a_1}...\mathfrak{q}_s^{a_s}$, it follows that $\mathfrak{p}$ does not divide $\mathfrak{C}_\theta \cap R$, which proves (3). So we can choose an element c belonging to $\mathfrak{C}_\theta \cap R$ which does not belong to $\mathfrak{p}$. Recall that $\{u_1, ..., u_m\}$ is a system of generators of S as an R-module. By choice, c belongs to $\mathfrak{C}_\theta \backslash \mathfrak{p}$, therefore the elements $cu_i \in R[\theta]$ and thus $u_i \in R_{\mathfrak{p}}[\theta]$ for $1 \leq i \leq m$. This proves that $S \subseteq R_{\mathfrak{p}}[\theta]$ and hence $S_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$ as desired.

(iii)⇒(i) Let $v_{\mathfrak{p}}$ denote the discrete valuation of K with valuation ring $R_{\mathfrak{p}}$. Suppose to the contrary that (i) does not hold. Then there exists $\xi = \sum_{i=0}^{n-1} a_i\theta^i \in S,\ a_i \in K$ such that ξ does not belong to $R_{\mathfrak{p}}[\theta]$. So there exists an index i for which a_i does not belong to $R_{\mathfrak{p}}$, i.e., $\min_i\{v_{\mathfrak{p}}(a_i)\} < 0$. Let $b \in \mathfrak{p}$ be such that

$$v_{\mathfrak{p}}(b) = -\min_i\{v_{\mathfrak{p}}(a_i)\} = -v_{\mathfrak{p}}(a_j) \quad (say).$$

Then $b\xi = \sum_{i=0}^{n-1} a_i b\theta^i$ belongs to $R_{\mathfrak{p}}[\theta]$ and $v_{\mathfrak{p}}(a_j b) = 0$. Choose $c \in R\backslash\mathfrak{p}$ such that $a_i bc \in R$ for all i, then $a_j bc \in R\backslash\mathfrak{p}$. Recall that $b \in \mathfrak{p}$, so $bc\xi = \sum_{i=0}^{n-1} a_i bc\theta^i \in \mathfrak{p}S \cap R[\theta]$ but does not belong to $\mathfrak{p}[\theta]$, which contradicts (iii). This completes the proof of (iii)⇒(i).

(i)⇒(iii) Clearly $\mathfrak{p}[\theta] \subseteq \mathfrak{p}S \cap R[\theta]$. To prove equality, let $\eta = \sum_{i=0}^{n-1} a_i\theta^i, a_i \in R$ be an element of $\mathfrak{p}S \cap R[\theta]$. By hypothesis $S \subseteq R_{\mathfrak{p}}[\theta]$, so $\eta \in \mathfrak{p}R_{\mathfrak{p}}[\theta]$; consequently $a_i \in \mathfrak{p}R_{\mathfrak{p}} \cap R = \mathfrak{p}$ for each i.

Proof of Theorem 1.1. In view of the hypothesis $\wp_i = \mathfrak{p}S + g_i(\theta)S$, it is clear that if $e_i > 1$, then $\wp_i^2$ does not divide $g_i(\theta)S$. In case $e_i = 1$ and $\wp_i^2$ divides $g_i(\theta)S$, then on replacing $g_i(x)$ by $g_i(x) + \pi_0$, where $\pi_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$, we may assume without loss of generality that $\wp_i^2 \nmid g_i(\theta)S$, $1 \leq i \leq r$.

Suppose to the contrary that $S_{\mathfrak{p}} \neq R_{\mathfrak{p}}[\theta]$. Then by Lemma 2.1, $\mathfrak{p}[\theta] \subsetneqq \mathfrak{p}S \cap R[\theta]$. So there exists a polynomial

$$T(x) \in R[x],\ \ \deg T(x) \leq n-1,\ \ n = [L:K] \tag{4}$$

such that $T(\theta) \in \mathfrak{p}S$ but $T(\theta)$ does not belong to $\mathfrak{p}[\theta]$. In particular, the polynomial $\bar{T}(x)$ with coefficients in $R/\mathfrak{p}$ is non-zero. Set $F(x) = g_1(x)^{e_1}....g_r(x)^{e_r}$. It follows from (1) that

$$F(\theta) \equiv 0 (\text{mod } \mathfrak{p}S). \tag{5}$$

Let $\bar{D}(x)$ denote the g.c.d. of $\bar{F}(x)$ and $\bar{T}(x)$. Write

$$\bar{D}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{d_i}, \qquad 0 \leq d_i \leq e_i. \tag{6}$$

There exist polynomials $A(x), B(x)$ in $R[x]$ and $C(x) \in \mathfrak{p}[x]$ such that

$$A(x)F(x) + B(x)T(x) = D(x) + C(x).$$

Substituting $x = \theta$ in the above equation and keeping in mind (5) as well as the fact $T(\theta) \equiv 0(\text{mod } \mathfrak{p}S)$, we have

$$D(\theta) \equiv 0(\text{mod } \mathfrak{p}S). \tag{7}$$

It follows from (6) and (7) that

$$\prod_{i=1}^{r} g_i(\theta)^{d_i} \equiv 0(\text{mod } \mathfrak{p}S). \tag{8}$$

Note that for $i \neq j$, $\wp_j$ and $g_i(\theta)S$ are coprime, for otherwise $\wp_j$ divides $g_i(\theta)S + \mathfrak{p}S = \wp_i$ which is not so. It now follows from (8) and the factorization of $\mathfrak{p}S$ that $\wp_i^{e_i}$ divides $g_i(\theta)^{d_i}S$. As assumed in the opening lines of the proof, $\wp_i^2$ does not divide $g_i(\theta)S$. Therefore $d_i \geq e_i$ for $1 \leq i \leq r$, which together with (6) gives, $d_i = e_i$ and consequently $\deg \bar{D}(x) = \deg \bar{F}(x) = n$. But $\bar{D}(x)$ being the g.c.d. of $\bar{F}(x)$ and

$\bar{T}(x)$ has degree not exceeding $n-1$ by virtue of (4). This contradiction proves that $S_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$.

3. Proof of Theorems 1.2, 1.3 and Corollary 1.4.

Proof of Theorem 1.2. Let n_i denote the residual degree of $\wp_i/\mathfrak{p}$. If a non-zero prime ideal $\mathfrak{p}$ of R does not divide $i_{S/R}$, then there exists a generating element θ for the extension L/K such that $\mathfrak{p}$ does not divide $N_{L/K}(\mathfrak{C}_\theta)$; consequently $S_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$ in view of Lemma 2.1. Theorem B then proves the existence of distinct monic irreducible polynomials over $R/\mathfrak{p}$ of degrees $n_1, ..., n_t$.

To prove the converse, suppose there exist distinct monic irreducible polynomials $V_1(x), ..., V_t(x)$ over $R/\mathfrak{p}$ with $\deg V_i = n_i$. We have to find a generating element $\theta \in S$, such that $\mathfrak{p}$ does note divide $N_{L/K}(\mathfrak{C}_\theta)$. Let $g_i(x) \in R[x]$ be a monic polynomial such that $\bar{g}_i(x) = V_i(x)$. Since R has finite norm property, the finite field $R/\mathfrak{p}$ has only one extension $S/\wp_i$ of degree n_i. Hence every irreducible polynomial over $R/\mathfrak{p}$ of degree n_i has a root in $S/\wp_i$. Therefore there exists an element $\theta_i \in S$ such that $g_i(\theta_i) \equiv 0 (\mathrm{mod}\ \wp_i)$. Since $R/\mathfrak{p}$ is a perfect field, an irreducible polynomial over $R/\mathfrak{p}$ cannot have multiple roots, so $g_i'(\theta_i)$ does not belong to $\wp_i$. If $g_i(\theta_i) \in \wp_i^2$ for some i, then replacing θ_i by $\theta_i + \pi_i$ with $\pi_i \in \wp_i \backslash \wp_i^2$ and keeping in mind that

$$g_i(\theta_i + \pi_i) = g_i(\theta_i) + \pi_i g_i'(\theta_i) + \frac{\pi_i^2}{2!} g_i''(\theta_i) + ...,$$

we see that $g_i(\theta_i + \pi_i)$ does not belong to $\wp_i^2$. So it can be assumed without loss of generality that $g_i(\theta_i)$ does not belong to $\wp_i^2$.

By Chinese Remainder Theorem, there exists $\xi \in S$ satisfying $\xi \equiv \theta_i (\mathrm{mod}\ \wp_i^2)$ for $1 \leq i \leq t$. Choose $\eta \in S$ such that $L = K(\xi, \eta)$. Let l, m denote the degrees of extensions of $K(\xi)/K$ and $L/K(\xi)$ respectively. Let $\xi = \xi^{(1)}, ..., \xi^{(l)}$ be the $K-$conjugates of ξ and $\eta = \eta^{(1)}, ..., \eta^{(m)}$ be the $K(\xi)-$conjugates of η. Choose a non-zero element a of $\mathfrak{p}^2$ which is different from $\frac{\xi^{(i)} - \xi^{(i')}}{\eta^{(j')} - \eta^{(j)}}$ for $1 \leq i \neq i' \leq l$, $1 \leq j \neq j' \leq m$; this is possible because R and hence $\mathfrak{p}^2$ is infinite. Then $\xi^{(i)} + a\eta^{(j)}$, $1 \leq i \leq l, 1 \leq j \leq m$

are distinct. Thus $\theta = \xi + a\eta$ has lm distinct K-conjugates. So θ generates the extension L/K and $\theta \equiv \xi \equiv \theta_i (\text{mod } \wp_i^2),\ 1 \leq i \leq t$. It will be shown that $\mathfrak{p}$ does not divide $N_{L/K}(\mathfrak{C}_\theta)$.

Set $\mathfrak{P}_i = \mathfrak{p}S + g_i(\theta)S$, we first prove that

$$\wp_i = \mathfrak{P}_i = \mathfrak{p}S + g_i(\theta)S. \tag{9}$$

It is clear that $\wp_i$ divides $\mathfrak{P}_i$ but $\wp_i^2$ does not divide $\mathfrak{P}_i$ (because $g_i(\theta)$ does not belong to $\wp_i^2$). Moreover for $i \neq j$ we have $\wp_j$ does not divide $\mathfrak{P}_i$, since otherwise we would have $g_i(\theta) \equiv 0 (\text{mod } \wp_j)$ which would give $g_i(\theta_j) \equiv 0 (\text{mod } \wp_j)$. But in view of $g_j(\theta_j) \equiv 0 (\text{mod } \wp_j)$, $\bar{g}_i(x)$ and $\bar{g}_j(x)$ would have a common root in $S/\wp_j$, which is not possible, since they are relatively prime. As $\mathfrak{P}_i$ divides $\mathfrak{p}S$, therefore $\mathfrak{P}_i$ is not divisible by prime ideals different from $\wp_1, ..., \wp_t$ and so $\wp_i = \mathfrak{P}_i = \mathfrak{p}S + g_i(\theta)S$, $1 \leq i \leq t$.

Set $F(x) = g_1(x)^{e_1} ... g_t(x)^{e_t}$. Using (9) and proceeding exactly as in the proof of Theorem 1.1, one can show that the assumption $S_\mathfrak{p} \neq R_\mathfrak{p}[\theta]$ leads to a contradiction. Thus $\mathfrak{p}$ does not divide $N_{L/K}(\mathfrak{C}_\theta)$ in view of Lemma 2.1.

Proof of Theorem 1.3. Let q, n denote respectively the number of elements of $R/\mathfrak{p}$ and the degree of the extension L/K. Let $r_q(m)$ stand for the number of monic irreducible polynomials of degree m over the finite field $R/\mathfrak{p}$. It is known that [4, Chapter VII, Exercise 22]

$$r_q(m) = \frac{1}{m} \sum_{d|m} \mu(d) q^{m/d} \tag{10}$$

where μ is the Möbius function. Since a finite field has irreducible polynomials of all degrees, the sum $\sum\limits_{d|m} \mu(d) q^{m/d}$ on the right hand side of (10) is positive and divisible by q, so

$$r_q(m) \geq \frac{q}{m}. \tag{11}$$

Observe that for any k, $1 \leq k \leq n$, in view of the fundamental equality (see [6, Theorem 4.1]), there are atmost n/k prime ideals of S dividing $\mathfrak{p}$ which have residual degree k. Let $\mathfrak{p}$ be a prime ideal dividing $i_{S/R}$. So by Theorem 1.2, there exists a number k, $1 \leq k \leq n$ such that $r_q(k)$ is strictly less than the number of prime ideals of S lying over $\mathfrak{p}$ with residual degree k, which is less than or equal to n/k in view of the above observation. It now follows from (11) that

$$\frac{q}{k} \leq r_q(k) < \frac{n}{k}$$

and hence $q < n$ as desired.

Proof of Corollary 1.4. Applying Theorem 1.3, we see that if $\mathfrak{p}$ divides $i_{S/R}$, then $\mid R/\mathfrak{p} \mid < 3$. Keeping in mind that there are only two linear monic irreducible polynomials over the field of two elements and the fact that a finite field has irreducible polynomials of each degree, the second assertion immediately follows from Theorem 1.2.

Acknowledgements. The problem dealt with in the paper originated during discussions with Professor Kaori Ota while the second author was visiting Department of Mathematics, Tsuda College, Tokyo. The authors are highly thankful to Professor Kaori Ota, Chairperson, Department of Mathematics, Tsuda College for constructive suggestions. The financial support and hospitality by this college are gratefully acknowledged. The research of the second author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, India.

References

[1] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Göttingen Abhandlungen*, **23** (1878) 1-23.

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

[3] S. K. Khanduja and M. Kumar, A Generalization of Dedekind Criterion, *Communications in Algebra* **35**(2007) 1479-1485.

[4] S. Lang, *Algebra*, 2nd ed., (Addison-Wesley publishing company, Inc., 1984).

[5] J. Montes and E. Nart, On a Theorem of Ore, *J. Algebra* **146**(1992) 318-334.

[6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3nd ed., (Springer-Verlag, Polish Scientific Publishers, 2004).

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