ON THE INTEGRAL CLOSEDNESS OF $R[\alpha]$

ABDULAZIZ DEAJIM and LHOUSSAIN EL FADIL

Communicated by Zaharescu

Let R be a Dedekind ring, K its quotient field, and $L = K(\alpha)$ a finite field extension of K defined by a monic irreducible polynomial $f(x) \in R[x]$. We give an easy version of Dedekind's criterion which computationally improves those versions known in the literature. We further use this result to give a sufficient condition for the integral closedness of $R[\alpha]$ when $f(x) = x^n - a$. In case R is the ring of integers of a number field, we give yet sufficient and necessary conditions for this to hold, generalizing and improving in both cases some known results in this direction. Some highlighting examples are also given.

AMS 2020 Subject Classification: 11Y40, 11S05, 13A18.

Key words: number field, Dedekind's criterion, extension of valuation.

1. INTRODUCTION AND STATEMENTS OF MAIN RESULTS

For a complex number α integral over $\mathbb{Q}$, a criterion that tests the integral closedness of $\mathbb{Z}[\alpha]$ in the number field $\mathbb{Q}(\alpha)$ was given in the milestone paper [4] of R. Dedekind (see also [3] or almost any book in algebraic number theory for a more modern treatment). As is well known, Dedekind's criterion utilizes the irreducible factorization of the reduction modulo prime integres of the minimal polynomial of α. S. Khanduja and M. Kummar, in [10], gave a generalization of this criterion to extensions of Dedekind rings. Ershov, in [6], gave yet a generalization of this criterion to extensions of rings of valuation. This criterion had, and still has, important applications in many relevant areas such as (but not limited to) the study of prime ideal factorizations in Dedekind rings, the computation of discriminants of number fields, and the existence of integral power bases in extensions of Dedekind rings (see for instance [1], [9], [12], [13]).

Let (K, ν) be a valued field with ν a rank-one discrete valuation, R_ν the ring of valuation of ν, $\mathfrak{m}_\nu$ the maximal ideal of R_ν, π a generator of $\mathfrak{m}_\nu$, and $k_\nu = R_\nu/\mathfrak{m}_\nu$ the residue field of ν. We assume, by normalization if necessary, that $\nu(K^*) = \mathbb{Z}$ (so, in particular, $\nu(\pi) = 1$). Denote also by ν the Gaussian extension of ν to the ring $R_\nu[x]$. Let $F(x) \in R_\nu[x]$ be a monic irreducible polynomial, $L = K(\alpha)$ the extension field of K generated by a root α of F, and S_ν the integral closure of R_ν in L. Assume that $\overline{F}(x) \equiv \prod_{i=1}^{r} \overline{\phi}_i(x)^{l_i} \pmod{\mathfrak{m}_\nu}$

is the monic irreducible factorization of $\overline{F}$ in $k_\nu[x]$. For each $i = 1, \ldots, r$, let $\phi_i(x) \in R_\nu[x]$ be a monic lift of $\overline{\phi}_i(x)$, and $Q_i(x), R_i(x) \in R_\nu[x]$, respectively, the quotient and remainder upon the Euclidean division of $F(x)$ by $\phi_i(x)$. So $Q_i(x)$ is monic and either $R_i(x) = 0$ or $\deg(R_i(x)) < \deg(\phi_i(x))$.

Our first theorem (Theorem 1.1) gives a precise and easy criterion for the integral closedness of the ring $R_\nu[\alpha]$ in L.

THEOREM 1.1. *With the above assumptions and notations, $R_\nu[\alpha]$ is integrally closed in L if and only if, for each $i = 1, \ldots, r$, either $l_i = 1$ or $\nu(R_i(x)) = 1$.*

For the next result, let R be a Dedekind ring, K its fraction field, $\mathfrak{p}$ a nonzero prime ideal of R, $\nu_\mathfrak{p}$ the (rank-one) discrete valuation of R associated to $\mathfrak{p}$, $F(x) \in R[x]$ a monic irreducible polynomial, $L = K(\alpha)$ an extension field of K generated by a root α of F, S the integral closure of R in L, and $k_\mathfrak{p}$ the residue field $R/\mathfrak{p}$. Keep the same notations and assumptions as above for the factorization of the reduction of F modulo $\mathfrak{p}$. The following result can be deduced from Theorem 1.1, which dramatically and computationally improves Dedekind's criterion in Dedekind ring extensions (see [6] and [10] for instance).

COROLLARY 1.2. *Keep the assumptions and notations of the paragraph above. Then, $S = R[\alpha]$ if and only if, for every prime ideal $\mathfrak{p}$ of R whose square divides $Disc_R(\alpha)$ and for each $i = 1, \cdots, r$, either $l_i = 1$ or $\nu_\mathfrak{p}(R_i(x)) = 1$.*

In [7, Theorem 3.1], it was shown that if α is a complex root of an irreducible polynomial $x^n - m \in \mathbb{Z}[x]$ such that m is square free and every prime divisor of n divides m, then $\mathbb{Z}[\alpha]$ is integrally closed in $\mathbb{Q}(\alpha)$. In the following theorem, we give yet an easy new proof of a generalization of the aforementioned result. Note that by saying that an element a of a Dedekind ring R is square-free, we mean that the principal ideal aR is not divisible by the square of any prime ideal of R.

THEOREM 1.3. *Let R be a Dedekind ring, K its quotient field, $a \in R$ square-free such that $f(x) = x^n - a$ is irreducible over R, and α a root of $f(x)$. If every prime ideal of R that contains $n.1_K$ also contains a, then $R[\alpha]$ is integrally closed.*

In the case of rings of integers of number fields, the following theorem strongly enhances Theorem 1.3. Besides, Theorem 1.4 generalizes the relevant results in [9] and [13]. For a ring of integers R, by $\nu_\mathfrak{p}(s)$ we mean $\nu_\mathfrak{p}(sR)$ for $s \in R$ and a nonzero prime ideal $\mathfrak{p}$ of R.

THEOREM 1.4. *Let R be the ring of integers of a number field K and $L = K(\alpha)$ be defined by a root of an irreducible polynomial $f(x) = x^n - u \in R[x]$.*

Then $R[\alpha]$ is integrally closed if and only if, for every nonzero prime ideal $\mathfrak{p}$ of R, either of the following holds:

1. $\nu_{\mathfrak{p}}(u) = 1$, *or*
2. $\nu_{\mathfrak{p}}(u) = 0$ *and* $\nu_{\mathfrak{p}}(u^{p^f} - u) = 1$, *where p is the rational prime lying under $\mathfrak{p}$ and f is the residue degree of $\mathfrak{p}$ over p.*

If we let $R = \mathbb{Z}$ and $K = \mathbb{Q}$ in Theorem 1.4, then [9, Thoerem 1.3] can be phrased as follows: $\mathbb{Z}[\alpha]$ is integrally closed if and only if, for every rational prime p, either $\nu_p(u) = 0$ or $\nu_p(u) = 1$ and $\nu_p(u^{p^{\nu_p(n)}} - u) = 1$. The following corollary is an improvement of [9, Theorem 1.3].

Corollary 1.5. *Keep the assumptions of Theorem 1.4 with $R = \mathbb{Z}$ and $K = \mathbb{Q}$. Then $\mathbb{Z}[\alpha]$ is integrally closed if and only if, for every rational prime p, either of the following holds:*

1. $\nu_p(u) = 1$, *or*
2. $\nu_p(u) = 0$ *and* $\nu_p(u^p - u) = 1$.

2. PROOFS OF THE MAIN RESULTS

In the notation of Theorem 1.1, denote by ω a valuation of L extending ν, by S_ω the valuation ring of ω, and by M_ω the maximal ideal of S_ω. Note that $S_\nu = \cap_\omega S_\omega$, where the intersection runs over all valuations ω of L extending ν (see [8, Lemma 3.17]).

We first tackle the following interesting lemma.

Lemma 2.1. *Keep the assumptions and notations of Theorem 1.1.*

(i) *For every $1 \leq i \leq r$, there exists a valuation ω of L extending ν such that $\omega(\phi_i(\alpha)) > 0$.*

(ii) *For every valuation ω of L extending ν, there exists a unique $1 \leq i \leq r$ such that $\omega(\phi_i(\alpha)) > 0$ and $\omega(\phi_j(\alpha)) = 0$ for all $j \neq i$.*

(iii) *For every valuation ω of L extending ν and every nonzero $p(x) \in R_\nu[x]$, $\omega(p(\alpha)) \geq \nu(p(x))$, where equality holds if and only if $\overline{\phi_i}(x)$ does not divide $\overline{(p(x)/\pi^{\nu(p(x))})}$ for some $\phi_i(x)$ satisfying $\omega(\phi_i(\alpha)) > 0$.*

Proof. (i) We know (see [11, Proposition II.8.2]) that the valuations $\omega_1, \cdots, \omega_t$ of L extending ν are in one-to-one correspondence with the irreducible factors $F_1(x), \cdots, F_t(x)$ of $F(x)$ in $K_\nu[x]$, where K_ν is the Henselianization of (K, ν) (i.e. the separable closure of K in the ν-adic completion of K). Note that although [11, Proposition II.8.2] states that the factors $F_i(X)$ are over the ν-adic completion of K, the proposition remains valid if we only assume that the factorization is over the Henselianization of (K, ν). Moreover, if $\overline{\nu}$ is the unique valuation extending ν to the algebraic closure of K_ν, then for any $h(x) \in K[x]$ and every root α_j of $F_j(x)$, $\omega_j(h(\alpha)) = \overline{\nu}(h(\alpha_j))$. Now fix some $1 \leq i \leq r$. As $\overline{\phi_i}(x)$ divides $\overline{F}(x) = \prod_{j=1}^{t} \overline{F_j}(x)$, $\overline{\phi_i}(x)$ divides $\overline{F_j}(x)$ for some j. Since $F_j(x)$ is irreducible over K_ν, it follows by Hensel's Lemma that $\overline{F_j}(x)$ is a power of $\overline{\phi_i}(x)$, say $\overline{\phi_i}(x)^{e_i}$, modulo $\mathfrak{m}_\nu$. Let α_j be a root of $F_j(x)$ and $M_{\overline{\nu}}$ the maximal ideal of the valuation ring of $\overline{\nu}$. Since $F_j(\alpha_j) = 0$ and $\mathfrak{m}_\nu \subseteq M_{\overline{\nu}}$, $\phi_i(\alpha_j)^{e_i} \in M_{\overline{\nu}}$. So, $\phi_i(\alpha_j) \in M_{\overline{\nu}}$ and thus $\omega_j(\phi_i(\alpha)) = \overline{\nu}(\phi_i(\alpha_j)) > 0$ as claimed.

(ii) Let ω be a valuation of L extending ν. Assume for the moment that the first assertion of part (iii) is true. Since $\prod_{i=1}^{r} \phi_i(\alpha)^{l_i} \equiv f(\alpha) \equiv 0 \pmod{M_\omega}$, $\omega(\prod_{i=1}^{r} \phi_i(\alpha)^{l_i}) > 0$. So, $\omega(\phi_i(\alpha)) > 0$ for some $1 \leq i \leq r$. For any $j \neq i$, let $s_j(x), t_j(x) \in R_\nu[x]$ be such that $\overline{s_j}(x)\overline{\phi_i}(x) + \overline{t_j}(x)\overline{\phi}_j(x) \equiv 1 \pmod{\mathfrak{m}_\nu}$. Then, $s_j(\alpha)\phi_i(\alpha) + t_j(\alpha)\phi_j(\alpha) = 1 + h(\alpha)$ for some $h(x) \in \mathfrak{m}_\nu[x]$. As $\nu(h(x)) > 0$, it follows from the first assertion of part (iii) that $\omega(h(\alpha)) > 0$ and, thus, $h(\alpha) \in M_\omega$. Since $\phi_i(\alpha) \in M_\omega$ (because $\omega(\phi_i(\alpha)) > 0$) and $s_j(\alpha) \in R_\nu[\alpha] \subseteq S_\nu \subseteq S_\omega$, $s_j(\alpha)\phi_i(\alpha)) \in M_\omega$. So, $t_j(\alpha)\phi_j(\alpha) - 1 \in M_\omega$ and, thus, $t_j(\alpha)\phi_j(\alpha) \in S_\omega - M_\omega$. So $\omega(t_j(\alpha)\phi_j(\alpha)) = 0$ and, thus, $\omega(\phi_j(\alpha)) = 0$, and the uniqueness of i such that $\omega(\phi_i(\alpha)) > 0$ follows.

(iii) Let ω be a valuation of L extending ν, $p(x) \in R_\nu[x]$ be nonzero, and set $p_1(x) = p(x)/\pi^u$, where $u = \nu(p(x))$. As $\nu(p_1(x)) = 0$, $p_1(x) \in R_\nu[x]$. Thus, $p_1(\alpha) \in S_\nu \subseteq S_\omega$ and $\omega(p(\alpha)) = \omega(\pi^u p_1(\alpha)) = u + \omega(p_1(\alpha)) \geq u$ as claimed. Now define the map $\psi : k_\nu[x] \to S_\omega/M_\omega$ by $\overline{p}(x) \mapsto p(\alpha) + M_\omega$. This is a well-defined map since $\mathfrak{m}_\nu \subseteq M_\omega$. It can also be checked that ψ is a ring homomorphism. For a nonzero $p(x) \in R_\nu[x]$ and $p_1(x) = p(x)/\pi^u$ with $u = \nu(p(x))$, we have $\omega(p(\alpha)) = u + \omega(p_1(\alpha))$. So, $\omega(p(\alpha)) = u$ if and only if $\omega(p_1(\alpha)) = 0$ if and only if $p_1(\alpha) \in S_\omega - M_\omega$ if and only if $\overline{p_1}(x) \notin \ker\psi$. From part (ii), let $\phi_i(x)$ be such that $\omega(\phi_i(\alpha)) > 0$. Then, $\phi_i(\alpha) \in M_\omega$ and, thus, $\overline{\phi_i}(x) \in \ker\psi$. Since $\ker\psi$ is principal (as k_ν is a field) and $\overline{\phi_i}(x)$ is irreducible over k_ν, $\ker\psi$ is generated by $\overline{\phi_i}(x)$. It now follows that $\omega(p(\alpha)) = u$ if and only if $\overline{\phi_i}(x)$ does not divide $\overline{p_1}(x)$ as claimed. $\square$

Proof of Theorem 1.1. We prove first that if $R_\nu[\alpha]$ is integrally closed in L, then $l_i = 1$ or $\nu(R_i(x)) = 1$ for each $i = 1, \ldots, r$. Assume that there exists some $k \in \{1, \ldots, r\}$ such that $l_k > 1$ and $\nu(R_k(x)) > 1$. Set

$$\theta_k = Q_k(\alpha)/\pi = -R_k(\alpha)/(\pi\phi_k(\alpha));$$

we show that θ_k is an element of $S_\nu - R_\nu[\alpha]$ and, thus, $R_\nu[\alpha]$ is not integrally closed. Since $Q_i(x)$ is monic, $\theta_k \notin R_\nu[\alpha]$ as, otherwise, $1/\pi$ would be an element of R_ν, which is absurd. To show that $\theta_k \in S_\nu$, we show that $\theta_k \in S_\omega$ for each valuation ω of L extending ν (as $S_\nu = \cap_\omega S_\omega$). Let ω be such a valuation. By LEMMA 2.1 (ii), let $i \in \{1, \ldots, r\}$ be such that $\omega(\phi_i(\alpha)) > 0$ and $\omega(\phi_j(\alpha)) = 0$ for all $j \neq i$. Note, by LEMMA 2.1 (iii), that $\omega(R_k(\alpha)) \geq \nu(R_k(x)) > 1$. If $k \neq i$, then

$$\omega(Q_k(\alpha)) = \omega(\phi_k(\alpha)) + \omega(Q_k(\alpha)) = \omega(\phi_k(\alpha)Q_k(\alpha)) = \omega(R_k(\alpha)) > 1.$$

So, $\omega(\theta_k) = \omega(Q_k(\alpha)) - 1 > 0$. Thus, $\theta_k \in S_\omega$ in this case. If $k = i$, we consider two possibilities. If $0 < \omega(\phi_k(\alpha)) \leq 1$, then

$$\omega(\theta_k) = \omega(R_k(\alpha)) - \omega(\pi) - \omega(\phi_k(\alpha)) \geq 2 - 1 - 1 = 0.$$

So, $\theta_k \in S_\omega$ in this case too. If, on the other hand, $\omega(\phi_k(\alpha)) > 1$, we let $q_k(x)$, $r_k(x) \in R_\nu[x]$ be, respectively, the quotient and remainder upon the Euclidean division of $Q_k(x)$ by $\phi_k(x)$ with $q_k(x)$ monic. We now have

$$\overline{F}(x) \equiv \overline{q_k}(x)\overline{\phi_k}^2(x) + \overline{r_k}(x)\overline{\phi_k}(x) + \overline{R_k}(x) \pmod{m_\nu}.$$

Since $\overline{\phi_k}^2(x)$ divides $\overline{F}(x)$ (as $l_k \geq 2$) and $\overline{R_k}(x) \equiv 0 \pmod{m_\nu}$, it follows that $\overline{\phi_k}^2(x)$ divides $\overline{r_k}(x)\overline{\phi_k}(x)$ and, therefore, $\overline{\phi_k}(x)$ divides $\overline{r_k}(x)$. Since $\deg(\overline{r_k}(x)) < \deg(\overline{\phi_k}(x))$, $\overline{r_k}(x) \equiv 0 \pmod{m_\nu}$ and $\nu(r_k(x)) \geq 1$. Now (using LEMMA 2.1 (iii) in the third inequality below), we have

$$\begin{aligned}
\omega(Q_k(\alpha)) &= \omega(q_k(\alpha)\phi_k(\alpha) + r_k(\alpha)) \\
&\geq \min\{\omega(q_k(\alpha)) + \omega(\phi_k(\alpha)), \omega(r_k(\alpha))\} \\
&\geq \min\{\omega(\phi_k(\alpha)), \omega(r_k(\alpha))\} \\
&\geq \min\{\nu(\phi_k(x), \nu(r_k(x))\} \\
&\geq 1.
\end{aligned}$$

Thus, $\omega(\theta_k) = \omega(Q_k(\alpha)) - 1 \geq 0$ and, hence, $\theta_k \in S_\omega$ in this case as well.

For the converse, assume that for every $1 \leq i \leq r$, either $l_i = 1$ or $\nu(R_i(x)) = 1$. We proceed in three steps.

Step 1: We show that if, for some i, $l_i = 1$, then we can always assume that $\nu(R_i(x)) = 1$ too. Suppose that $\nu(R_i(x)) > 1$. Note that

$$F(x) = Q_i(x)\phi_i(x) + R_i(x) = Q_i(x)(\phi_i(x) + \pi) - \pi Q_i(x) + R_i(x).$$

Let $H_i(x), T_i(x) \in R_\nu[x]$ be such that $Q_i(x) = H_i(x)\phi_i(x) + T_i(x)$ with $\deg(T_i(x)) < \deg(\phi_i(x))$. Set $\phi_i^*(x) = \phi_i(x) + \pi$, $Q_i^*(x) = Q_i(x) - \pi H_i(x)$ and $R_i^*(x) = R_i(x) - \pi T_i(x) + \pi^2 H_i(x)$. Then, $F(x) = Q_i^*(x)\phi_i^*(x) + R_i^*(x)$. Note that $Q_i^*(x)$ and $R_i^*(x)$ are, respectively, the quotient and remainder upon the Euclidean division of $F(x)$ by $\phi_i^*(x)$. As $\overline{T_i}(x)$ is nonzero (as $l_i = 1$), $\nu(\pi T_i(X)) = 1$. Since also $\nu(R_i(x)) > 1$ and $\nu(\pi^2 H_i(x)) \geq 2$, it must follow that $\nu(R_i^*(x)) = 1$. So, up to replacing the lifting of $\overline{\phi_i}(x)$ by $\phi_i^*(x)$ instead of $\phi_i(x)$ if necessary, we can assume that $\nu(R_i(x)) = 1$ as claimed.

Step 2: Based on Step 1, we can assume that $\nu(R_i(x)) = 1$ for every $1 \le i \le r$. Let ω be a valuation of L extending ν and $i \in \{1, \cdots, r\}$, we show that if $\omega(\phi_i(\alpha)) > 0$ then $\omega(\phi_i(\alpha)) = 1/l_i$. If $l_i = 1$, then $\overline{\phi_i}(x)$ does not divide $\overline{Q_i}(x)$. So, by Lemma 2.1 (iii), $\omega(Q_i(\alpha)) = 0$ and $\omega(\phi_i(\alpha)) = \omega(Q_i(\alpha)\phi_i(\alpha)) = \omega(-R_i(\alpha)) = \nu(R_i(x)) = 1 = 1/l_i$. If $l_i > 1$, then set

$$F(x) = G_i(x)\phi_i^{l_i}(x) + S_i(x)\phi_i(x) + R_i(x),$$

for some $G_i(x), S_i(x) \in R_\nu[x]$ with $\nu(G_i(x)) = 0$ and $\nu(S_i(x)) > 1$. It then follows that $\omega(G_i(\alpha)\phi_i^{l_i}(\alpha)) = \omega(S_i(\alpha)\phi_i(\alpha) + R_i(\alpha)) = 1$. Thus, $\omega(\phi_i^{l_i}(\alpha)) = 1$ and, therefore, $\omega(\phi_i(\alpha)) = 1/l_i$.

Step 3: Now assume that $R_\nu[\alpha]$ is not integrally closed. So, there exists some monic $p(x) \in R_\nu[x]$ with $\deg(p(x)) < \deg(F(x))$ such that $p(\alpha)/\pi$ is integral over R_ν. Note then that $p(\alpha)/\pi \in S_\nu - R_\nu[\alpha]$. Let $r_i \ge 0$ be such that $\overline{\phi_i}^{r_i}(x)$ is the highest power of $\overline{\phi_i}(x)$ that divides $\overline{p}(x)$. Since $\deg(p(x)) < \deg(F(x))$, $r_{i_0} < l_{i_0}$ for some $i_0 \in \{1, \cdots, r\}$. Let $M_{i_0}(x), L_{i_0}(x) \in R_\nu[x]$ be, respectively, the quotient and remainder upon the Euclidean division of $p(x)$ by $\phi_{i_0}^{r_{i_0}}(x)$. So

$$p(x) = \phi_{i_0}^{r_{i_0}}(x)M_{i_0}(x) + L_{i_0}(x),$$

$\overline{\phi_{i_0}}(x) \nmid \overline{M_{i_0}}(x)$, and $\nu(L_{i_0}(x)) \ge 1$. Since $p(x)$ and $\phi_{i_0}(x)$ are monic, $M_{i_0}(x)$ is monic and, therefore, $\nu(M_{i_0}(x)) = 0$. By LEMMA 2.1 (i), let ω be a valuation of L extending ν such that $\omega(\phi_{i_0}(\alpha)) > 0$. Then, by Step 2 above, $\omega(\phi_{i_0}(\alpha)) = 1/l_{i_0}$. Since $\overline{\phi_{i_0}}(x) \nmid \overline{M_{i_0}}(x)$ and $\nu(M_{i_0}(x)) = 0$, it follows from LEMMA 2.1 (iii) that $\omega(M_{i_0}(\alpha)) = \nu(M_{i_0}(x)) = 0$. Also, by LEMMA 2.1 (iii), $\omega(L_{i_0}(\alpha)) \ge \nu(L_{i_0}(x)) \ge 1$. As $r_{i_0}/l_{i_0} < 1$, $r_{i_0}/l_{i_0} < \omega(L_{i_0}(\alpha))$. We, thus, have

$$\begin{aligned}
\omega(p(\alpha)) &= \min\{\omega(\phi_{i_0}^{r_{i_0}}(\alpha)M_{i_0}(\alpha)), \omega(L_{i_0}(\alpha))\} \\
&= \min\{r_{i_0}\omega(\phi_{i_0}(\alpha)) + \omega(M_{i_0}(\alpha)), \omega(L_{i_0}(\alpha))\} \\
&= \min\{r_{i_0}/l_{i_0}, \omega(L_{i_0}(\alpha))\} \\
&= r_{i_0}/l_{i_0} < 1.
\end{aligned}$$

Thus, $\omega(p(\alpha)/\pi) < 0$ and, therefore, $p(\alpha)/\pi \notin S_\nu$, a contradiction. □

Remark. Checking that $\nu(R_i(x)) = 1$ is needed only if $l_i \ge 2$. In this case, note that the requirement that $\nu(R_i(x)) = 1$ is independent of the choice of the monic lifting of $\overline{\phi_i}(x)$. Indeed, if $l_i \ge 2$, then we show that $\nu(R_i(x)) = 1$ if and only if $\nu(r_i(x)) = 1$ for the remainder $r_i(x)$ upon the Euclidean division of $f(x)$ by any other monic lifting of $\overline{\phi_i}(x)$. Let $\nu(R_i(x)) = 1$, $P_i(x) = \phi_i(x) + \pi H(x)$ be another monic lifting of $\overline{\phi_i}(x)$, with $H(x) \in R_\nu[x]$. Let $q_i(x), r_i(x) \in R_\nu[x]$ be, respectively, the quotient and remainder upon the Euclidean division of $f(x)$ by $P_i(x)$. Let ω be a valuation of L extending ν such that $\omega(\phi_i(\alpha)) > 0$.

By the proof of Theorem 1.1, $\omega(\phi_i(\alpha)) = 1/l_i$. We have

$$f(x) = Q_i(x)\phi_i(x) + R_i(x) = q_i(x)P_i(x) + r_i(x).$$

As $\omega(\phi_i(\alpha)) = 1/l_i < 1$ and $\omega(\pi H(\alpha)) \geq 1$,

$$\omega(P_i(\alpha)) = \omega(\phi_i(\alpha) + \pi H(\alpha)) = 1/l_i.$$

Let $M_i(x), S_i(x) \in R_\nu[x]$ be, respectively, the quotient and remainder upon the Euclidean division of $f(x)$ by $P_i^{l_i}(x)$. Since $\overline{\phi_i}(x)$ does not divide $\overline{M_i}(x)$, $\omega(M_i(\alpha)) = \nu(M_i(x)) = 0$ (by Lemma 2.1). Therefore,

$$\omega(S_i(\alpha)) = \omega(M_i(\alpha)P_i^{l_i}(\alpha)) = 1.$$

Note that $S_i(x) = N_i(x)P_i(x) + r_i(x)$ for some $N_i(x) \in \mathfrak{m}[x]$. It thus follows that $\omega(r_i(\alpha)) = \omega(S_i(\alpha)) = 1$ because $\omega(N_i(\alpha)P_i(\alpha)) \geq 1 + 1/l_i > 1$. Since $\overline{\phi_i}(x)$ does not divide $\overline{r_i}(x)$, $\nu(r_i(x)) = \omega(r_i(\alpha)) = 1$.

Proof of Corollary 1.2. On the one hand, it is known that $R[\alpha]$ is integrally closed (i.e. $S = R[\alpha]$) if and only if $R_\mathfrak{p}[\alpha]$ is integrally closed for every nonzero prime ideal $\mathfrak{p}$ of R (see [1]). On the other hand, the generalized discriminant-index formula "$\mathrm{Disc}_R(F) = \mathrm{Ind}_R(\alpha)^2 \mathrm{D}_R(S)$" was shown in [2]. It is thus obvious that for the equality $S = R[\alpha]$ to hold, we need only to consider those prime ideals $\mathfrak{p}$ of R whose squares divide $\mathrm{Disc}_R(F)$. For such a prime ideal, (K, ν) is a valued field of rank 1 with discrete valuation $\nu_\mathfrak{p}$ and ring of valuation $R_\mathfrak{p}$. Applying Theorem 1.1 yields the desired conclusion. □

Proof of Theorem 1.3. In order to use Corollary 1.2, and since $\mathrm{disc}(f) = \pm n^n a^{n-1}$, we need only to consider those prime ideals of R containing $n.1_K$ or a. Since any prime ideal $\mathfrak{p}$ that contains $\mathrm{disc}(f)$ must contain a (by our assumption on n), we let $\mathfrak{p}$ be a prime ideal of R containing a, Then $x^n - a \equiv x^n \pmod{\mathfrak{p}}$. By the Euclidean division of $x^n - a$ by x, the remainder is $-a$. Since a is square-free, $\nu_\mathfrak{p}(-a) = 1$. Thus, by Corollary 1.2, $R[\alpha]$ is integrally closed in $K(\alpha)$. □

Proof of Theorem 1.4. It is known that $R[\alpha]$ is integrally closed in L if and only if $R_\mathfrak{p}[\alpha]$ is integrally closed in L for every nonzero prime ideal $\mathfrak{p}$ of R that divides the discriminant of $f(x)$. Since the discriminant of $f(x)$ is $n^n u^{n-1}$, we seek to show the integral closedness of $R_\mathfrak{p}[\alpha]$ in L for every nonzero prime ideal $\mathfrak{p}$ of R that contains nu. Let $\mathfrak{p}$ be such a prime ideal. If $u \in \mathfrak{p}$, then it follows from Theorem 1.3 that $R_\mathfrak{p}[\alpha]$ is integrally closed in L if and only if $u \notin \mathfrak{p}^2$. Assume that $u \notin \mathfrak{p}$. So, $n1_K \in \mathfrak{p}$ and n is thus divisible by p. Let

$n = mp^r$ with $m \in \mathbb{N}$ not divisible by p. If, on the one hand, $f \le r$, then set $r = s + f$. So,

$$f(x) = x^{mp^r} - u \equiv x^{mp^s p^f} - u^{p^f} \equiv (x^{mp^s} - u)^{p^f} \pmod{\mathfrak{p}}.$$

We also have,

$$\begin{aligned} f(x) &= (x^{mp^s})^{p^f} - u = (x^{mp^s} - u + u)^{p^f} - u \\ &= \sum_{k=0}^{p^f-1} \binom{p^f}{k} u^k (x^{mp^s} - u)^{p^f-k} + u^{p^f} - u \\ &= H(x)(x^{mp^s} - u) + u^{p^f} - u, \end{aligned}$$

$H(x) \in R[x]$. If $\overline{x^{mp^s} - u} = \prod_{i=1}^{t} \overline{g_i}^{e_i}(x)$ is the monic irreducible factorization of $x^{mp^s} - u$ module $\mathfrak{p}$, then $\overline{f}(x) = \prod_{i=1}^{t} \overline{g_i}^{e_i p^f}(x)$ is the monic irreducible factorization of $f(x)$ modulo $\mathfrak{p}$. Letting $g_i(x) \in R[x]$ be a monic lift of $\overline{g_i}(x)$ for each i, it follows that the remainder upon the Euclidean division of $f(x)$ by each $g_i(x)$ is $u^{p^f} - u$. If, on the other hand, $r < f$, then set $f = s + r$. So,

$$f(x) = x^{mp^r} - u \equiv x^{mp^r} - u^{p^f} \equiv (x^m - u^{p^s})^{p^r} \pmod{\mathfrak{p}}.$$

We also have,

$$\begin{aligned} f(x) &= (x^m)^{p^r} - u = (x^m - u^{p^s} + u^{p^s})^{p^r} - u \\ &= \sum_{k=0}^{p^r-1} \binom{p^r}{k} u^{kp^s} (x^m - u^{p^s})^{p^r-k} + u^{p^f} - u \\ &= M(x)(x^m - u^{p^s}) + u^{p^f} - u, \end{aligned}$$

$M(x) \in R[x]$. If $\overline{x^m - u^{p^s}} = \prod_{i=1}^{v} \overline{h_i}^{l_i}(x)$ is the monic irreducible factorization of $x^m - u^{p^s}$ module $\mathfrak{p}$, then $\overline{f}(x) = \prod_{i=1}^{v} \overline{h_i}^{l_i p^r}(x)$ is the monic irreducible factorization of $f(x)$ modulo $\mathfrak{p}$. Letting $h_i(x) \in R[x]$ be a monic lift of $\overline{h_i}(x)$ for each i, it follows that the remainder upon the Euclidean division of $f(x)$ by each $h_i(x)$ is $u^{p^f} - u$. In either case, it follows from Theorem 1.1 that $R_{\mathfrak{p}}[\alpha]$ is integrally closed if and only if $\nu_{\mathfrak{p}}(u^{p^f} - u) = 1$. $\square$

Remark. In case (ii) of Theorem 1.4, any $r \in \mathbb{N}$ with $\nu_{\mathfrak{p}}(u^{p^r} - u) = 1$ suffices for the same conclusion to hold.

Proof of Corollary 1.5. Just apply Theorem 1.4 noting that $f = 1$. $\square$

3. APPLICATIONS AND EXAMPLES

COROLLARY 3.1. *Keep the notations and assumptions of Theorem 1.1. Let* $f(x) = \sum_{i=0}^{n} a_i x^i \in R_\nu[x]$ *be monic with* $\nu(a_k) \geq 1$ *for* $1 \leq k \leq n-1$, *and* $\nu(a_0) = 1$. *Let* $L = K(\alpha)$ *a field extension of* K *with* α *a root of* $f(x)$. *Then* $f(x)$ *is irreducible over* K *and* $R_\nu[\alpha]$ *is integrally closed in* L.

Proof. By the well-known Eisenstein's Criterion, $f(x)$ is irreducible over R_ν. By Gauss' Lemma (see [5, Proposition 9.3.5]), $f(x)$ is also irreducible over K as well. As $\overline{f}(x) \equiv x^n \pmod{\mathfrak{m}_\nu}$ and the remainder when dividing $f(x)$ by x is a_0 with $\nu(a_0) = 1$, it follows from Theorem 1.1 that $R_\nu[\alpha]$ is integrally closed in L. $\square$

With the notation of Theorem 1.1, assume that $f(x), \phi(x) \in R_\nu[x]$ are monic polynomials such that $\deg(\phi(x)) \leq \deg(f(x))$ and $\overline{\phi}(x) \in k[x]$ is monic and irreducible. Let $f(x) = \sum_{i=0}^{l} a_i(x)\phi(x)^{l-i}$ be the ϕ-adic expansion of $f(x)$. This entails, in particular, that, for each i, either $a_i(x) = 0$ or $\deg(a_i(x)) < \deg(\phi(x))$. We say that $f(x)$ is (ϕ, ν)-Eisenstein if $\nu(a_i(x)) \geq 1$ for $i = 1, \ldots, l-1$ and $\nu(a_l(x)) = 1$.

COROLLARY 3.2. *Keep the above notations and assumptions. Let* $L = K(\alpha)$ *be a field extension of* K *with* α *a root of* $f(x)$. *If* $\overline{f}(x) \equiv \overline{\phi}(x)^l \pmod{\mathfrak{m}_\nu}$ *and* $f(x)$ *is* (ϕ, ν)*-Eisenstein, then* $f(x)$ *is irreducible over* R_ν *and* $R_\nu[\alpha]$ *is integrally closed in* L.

Proof. Assume that $f(x) = g(x)h(x)$ for some monic $g(x), h(x) \in R_\nu[x]$. Then $\overline{g}(x) \equiv \overline{\phi}(x)^{l_1}$, $\overline{h}(x) \equiv \overline{\phi}(x)^{l_2} \pmod{\mathfrak{m}_\nu}$, with $l_1 + l_2 = l$. Note that $l_i \geq 1$ for $i = 1, 2$ as both $g(x)$ and $h(x)$ are monic. Let $g(x) = \sum_{i=0}^{l_1} g_i(x)\phi(x)^{l_1-i}$ and $h(x) = \sum_{i=0}^{l_2} h_i(x)\phi(x)^{l_2-i}$ be the ϕ-adic expansions of $g(x)$ and $h(x)$, respectively. As $g(x)$ and $h(x)$ are monic, $g_0(x) = h_0(x) = 1$. Since $l_i \geq 1$ and $\overline{g}(x) \equiv \overline{\phi}(x)^{l_1}$, $\overline{h}(x) \equiv \overline{\phi}(x)^{l_2} \pmod{\mathfrak{m}_\nu}$, $\nu(g_{l_1}(x)) \geq 1$ and $\nu(h_{l_2}(x)) \geq 1$. By the uniqueness of the ϕ-adic expansion of $f(x)$, $a_l(x) = g_{l_1}(x)h_{l_2}(x)$. Thus, $\nu(a_l(x)) \geq 2$, a contradiction. Thus, $f(x)$ is irreducible over R_ν. Hence, $f(x)$ is irreducible over R_ν. Now, since $\nu(a_l(x)) = 1$, it follows from Theorem 1.1 that $R_\nu[\alpha]$ is integrally closed in L. $\square$

COROLLARY 3.3. *Consider the above notation and assumptions, and let* $f(x) = x^n + a \in R_\nu[x]$ *be monic such that* $\nu(a) = m \geq 1$ *with* m *and* n *relatively prime. Let* $L = K(\alpha)$ *be a field extension of* K *with* α *a root of* $f(x)$ *and* S *the integral closure of* R_ν *in* L. *Then* $f(x)$ *is irreducible over* K *and* $\theta = \alpha^s/\pi^t$ *generates a power basis for* S *over* R_ν, *where* $s, t \in \mathbb{Z}$ *such that* $ms - nt = 1$.

Proof. As $\theta^n = \alpha^{ns}/\pi^{nt} = a^s/\pi^{nt}$, $\nu(\theta^n) = ms - nt = 1$ and, therefore, $F(x) = x^n - \theta^n \in R_\nu[x]$ is ν-Eisenstein. Hence, by Corollary 3.1, $F(x)$ is irreducible over K and $R_\nu[\theta]$ is integrally closed in $K(\theta)$. But $\theta = \alpha^s/\pi^t \in L$. On the other hand, $\alpha = \alpha^{ms-nt} = \alpha^{ms}/\alpha^{nt} = (\pi^{mt}\theta^m)/a^t \in K(\theta)$. Thus, $L = K(\theta)$. This, on the one hand, implies that $R_\nu[\theta]$ is integrally closed in L as claimed. On the other hand, as $f(x)$ and $F(x)$ are of the same degree and $F(x)$ is irreducible over K, $f(x)$ is irreducible over K as well. $\square$

Example 1. In this example we use Corollary 1.2 to give a much easier proof of the very well-know monogenity of nth cyclotomic number fields. By [14, p. 11], it suffices to prove the monogenity of p^rth cyclotomic number fields for rational primes p.

Let $K_{p^r} = \mathbb{Q}(\zeta)$ be the p^rth cyclotomic field with $\zeta = \zeta_{p^r} = \exp(2\pi i/p^r)$. It is known that the minimal polynomial of ζ is

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{\phi(p^r)} + x^{\phi(p^r)-p^{r-1}} + \cdots + x^{\phi(p^r)-(p-2)p^{r-1}} + 1$$

and p is the only rational prime whose square divides $\operatorname{disc}(\Phi_{p^r})$ (in fact, $\operatorname{disc}(\Phi_{p^r})$ is a power of p). Reducing $\Phi_{p^r}(x) = \dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$ modolo p yields

$$\overline{\Phi_{p^r}}(x) \equiv \overline{(x-1)}^{\,\phi(p^r)} \pmod{p}.$$

Let $Q(x), R(x) \in \mathbb{Z}[x]$ be, respectively, the quotient and remainder upon the Euclidean division of $\Phi_{p^r}(x)$ by $x-1$. Since $\deg(x-1) = 1$, $R(x) = a$ for some constant $a \in \mathbb{Z}$. Thus, $\Phi_{p^r}(x) = (x-1)Q(x) + a$. Evaluating both sides at 1 yields $p = \Phi_{p^r}(1) = a$. Since $\nu_p(p) = 1$, it now follows from Corollary 1.2 that $\mathbb{Z}_{K_{p^r}} = \mathbb{Z}[\zeta]$, which is what we need to show.

Example 2. Let $R = \mathbb{Z}_K$, where K is the quadratic number field defined by $x^2 - 3$. It is well known that $R = \mathbb{Z}[\sqrt{3}]$ and $3R = \mathfrak{p}^2$, where $\mathfrak{p} = \sqrt{3}R$. Let $(m, n) \in \mathbb{Z} \times \mathbb{N}$ be two integers such $f(x) = x^n - m$ is irreducible over K and 3 divides n. Let $L = K(\alpha)$, where α is a root of $f(x)$. We show that $R[\alpha]$ is not integrally closed. If 3 divides m, then as 3 is a square in R, m is not square free in R. So, by Theorem 1.4, $R[\alpha]$ is not integrally closed. If 3 does not divide m, then as $m^3 \equiv m \bmod 3$, 3 divides $m^3 - m$ in R and, thus, $\nu_{\mathfrak{p}}(m^3 - m) \geq 2$. Again, by Theorem 1.4, $R[\alpha]$ is not integrally closed in this case either.

Acknowledgments. The authors deeply thank the anonymous referee for the constructive comments which helped in improving the paper. The authors also extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through the General Research Project under grant number GRP/360/42.

REFERENCES

[1] M. E. Charkani and A. Deajim, *Generating a power basis over a Dedekind ring*. J. Number Theory **132** (2012), 2267–2276.

[2] M. E. Charkani and A. Deajim, *Relative index in extensions of Dedekind rings*. JP J. of Algebra, Number Theory, and Appl. **27** (2012), 73–84.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1996.

[4] R. Dedekind, *Über den Zussamenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*. Abh. Akad. Wiss. Gottingen, Math.-Phys. KL **23** (1878), 1–23.

[5] D. Dummit and R. Foote, *Abstract Algebra*, 2nd Edition. Prentice Hall, 1999.

[6] Y. Ershov, *A Dedekind criterion for arbitrary valuation rings*. Dokl. Math. **74** (2006), *2*, 650–652.

[7] A. Hameed, T. Nakahara, S. Husnine, and S. Ahmad, *On existence of canonical number system in certain classes of pure algebraic number fields*. J. Prime Res. Math **7** (2011), 19–24.

[8] G. Janusz, *Algebraic Number Fields*. 2nd Edition, Academic Press, 1995.

[9] K. Khanduja and B. Jhorar, *When is $R[\theta]$ integrally closed?*. J. Algebra and Appl. **15** (2016), *5*, 1650091.

[10] K. Khanduja and M. Kumar, *A generalizaiton of Dedekind Criterion*. Commun. Algebra **35** (2007), *5*, 1479–1486.

[11] J. Neukirch, *Algebraic Number Theory*. Springer-Verlag, 1999.

[12] P. Schmid, *On criteria by Dedekind and Ore for integral ring extensions*. Arch. Math. **84** (2005), 304–310.

[13] K. Uchida, *When is $\mathbb{Z}[\alpha]$ the ring of the integers?*. Osaka J. Math **14** (1977), 155–157.

[14] L. Washington, *Introduction to Cyclotomic Fields*. Springer-Verlag, 1997.

Received September 9, 2018

Abdulaziz Deajim
King Khalid University
Department of Mathematics
P.O. Box 9004, Abha, Saudi Arabia
deajim@kku.edu.sa, deajim@gmail.com

Lhoussain El Fadil
Sidi Mohamed Ben Abdellah University
Faculty of Sciences Dhar-Mahraz
Department of Mathematics
B.P. 1796, Fes, Morocco
lhouelfadil2@gmail.com