

# DEDEKIND'S CRITERION AND INTEGRAL BASES

LHOUSSAIN EL FADIL

Dept. of Math., Fac. of Sci. Dhar- El Mahraz, Sidi Mohamed Ben Abdellah University, Atlas-Fez, MOROCCO

ABSTRACT. Let R be a principal ideal domain with quotient field K, and  $L = K(\alpha)$ , where  $\alpha$  is a root of a monic irreducible polynomial  $F(x) \in R[x]$ . Let  $\mathbb{Z}_L$  be the integral closure of R in L. In this paper, for every prime p of R, we give a new efficient version of Dedekind's criterion in R, i.e., necessary and sufficient conditions on F(x) to have p not dividing the index  $[\mathbb{Z}_L : R[\alpha]]$ , for every prime p of R. Some computational examples are given for  $R = \mathbb{Z}$ .

### 1. Introduction

Throughout this paper unless otherwise stated, R is a principal ideal domain with quotient field K. For every prime element p of R, let  $\nu_p$  be the p-adic discrete valuation on R and  $k(p) = \frac{R}{(p)}$  the residue field associated to p. The Gaussian valuation of K(x) which extends  $\nu_p$  and defined by

$$\nu_p\left(\sum_{i=0}^l a_i X^{l-i}\right) = \min\left\{\nu_p(a_i), 0 \le i \le l\right\} \text{ is also denoted by } \nu_p.$$

Let  $L = K(\alpha)$ , where  $\alpha$  is a root of a monic irreducible polynomial  $F(x) \in R[x]$ . Let disc(F) be the discriminant of F,  $\mathbb{Z}_L$  the integral closure of R in L, and  $\operatorname{ind}(\alpha) = [\mathbb{Z}_L : R[\alpha]]$  the index of  $R[\alpha]$  in  $\mathbb{Z}_L$ . A natural question is: when does  $\mathbb{Z}_L = R[\alpha]$ ? If  $R = \mathbb{Z}$ , then for every prime integer p, Dedekind gave a criterion to test whether or not p divides  $\operatorname{ind}(\alpha)$ ; more precisely, he proved that p does not divide  $\operatorname{ind}(\alpha)$  if and only if for every  $i = 1, \ldots, r$ , either  $e_i = 1$  or  $e_i \geq 2$  and  $\overline{\phi_i}(x)$  does not divide  $\overline{M}(x)$ , where

$$M(x) = \frac{F(x) - \prod_{j=1}^r \phi_j^{l_j}(x)}{p} \quad \text{and} \quad \overline{F}(x) = \prod_{j=1}^r \overline{\phi_j}^{l_j}(x) \pmod{p}$$

is the factorization of  $\overline{F}(x)$  in  $\mathbb{F}_p[x]$  (see [5, Theorem 6.1.4] and [8]).

<sup>© 2019</sup> Mathematical Institute, Slovak Academy of Sciences.

<sup>2010</sup> Mathematics Subject Classification: 13A18, 11Y40, 11S05.

Keywords: Dedekind's criterion, integral bases, Power integral bases.

Licensed under the Creative Commons Attribution-NC-ND 4.0 International Public License.

### LHOUSSAIN EL FADIL

This criterion was also proved over any valuation ring R and any algebraic field extension  $L = K(\alpha)$  of K, where L/K is not necessarily separable [7]. In this paper, we give a more efficient version of this criterion for any principal ideal domain R with no separability assumption on the extension L/K. We further give some computational examples in the case  $R = \mathbb{Z}$ .

## 2. Main results

We recall here the definition of the index  $\operatorname{ind}(\alpha) = [\mathbb{Z}_L : R[\alpha]]$ . Since R is a principal ideal domain,  $\mathbb{Z}_L$  is a free R-module of rank  $n = \deg(F)$ . Let  $\mathbf{B} = \{u_1, \ldots, u_n\}$  be an R-basis of  $\mathbb{Z}_L$  and  $P_B^F$  the transition matrix from  $\mathbf{B}$  to the R-basis  $\mathbf{F} = \{1, \alpha, \ldots, \alpha^{n-1}\}$  of  $R[\alpha]$ . The index  $[\mathbb{Z}_L : R[\alpha]]$  is the principal ideal of R generated by the determinant of  $P_B^F$ . It is well known that this principal ideal  $[\mathbb{Z}_L : R[\alpha]]$  is well defined and is independent on the choice of the bases  $\mathbf{B}$  and  $\mathbf{F}$  of  $\mathbb{Z}_L$  and  $R[\alpha]$ , respectively. Since R is a principal ideal domain, it follows from the invariant factor Theorem that there exists  $\mathbf{B} = \{u_1, \ldots, u_n\}$  an R-basis of  $\mathbb{Z}_L$  and  $(q_1, \ldots, q_n) \in R^n$  such that for every  $i = 1, \ldots, n - 1, q_i$  divides  $q_{i+1}$ , and  $\mathbf{F} = \{q_1u_1, \ldots, q_nu_n\}$  is an R-basis of  $R[\alpha]$ . Since  $P_B^F$  is the diagonal matrix with diagonal elements:  $q_1, \ldots, q_n$ , the index  $[\mathbb{Z}_L : R[\alpha]]$  is then precisely the principal ideal of R generated by  $\prod_{i=1}^n q_i$ . If  $R = \mathbb{Z}$ , then  $\operatorname{ind}(\alpha)$  is the cardinal order of the finite group  $\mathbb{Z}_L/\mathbb{Z}[\alpha]$ .

In this section, let

$$F(x) \equiv \prod_{i=1}^{r} \phi_i^{l_i}(x) \pmod{p}$$

be the factorization of  $\overline{F}(x)$  in k(p)[x], where for every  $i := 1, \ldots, r$ ,  $\phi_i$  is a monic polynomial in R[x]. For every  $i := 1, \ldots, r$ , let  $Q_i(x)$  and  $R_i(x)$  be the quotient and the remainder of the Euclidean division of F(x) by  $\phi_i(x)$ , respectively.

Our next Theorem computationally improves the well known Dedekind's criterion.

**THEOREM 2.1.** Under the above hypotheses, p does not divide the index  $[\mathbb{Z}_L : R[\alpha]]$  if and only if for every i := 1, ..., r, either  $l_i = 1$  or  $l_i \ge 2$  and  $\nu_p(R_i(x)) = 1$ .

Proof. If for every i := 1, ..., r,  $l_i = 1$ , then by the generalized Dedekind's criterion p does not divide  $ind(\alpha)$  (see for example [7]). Otherwise, let

$$M(x) = \frac{F(x) - \prod_{j=1}^{r} \phi_{j}^{l_{j}}(x)}{p}$$

as defined in the Dedekind's criterion and let us show that for every i = 1, ..., r, with  $l_i \ge 2$ ,  $\nu_p(R_i(x)) = 1$  if and only if  $\overline{\phi}_i$  does not divide  $\overline{M}(x)$  in k(p)[x]. Indeed, as

$$F(x) \equiv \prod_{j=1}^{r} \phi_j^{l_j}(x) \pmod{p},$$

then  $\overline{\phi_i}(x)$  divides

$$\overline{F}(x), \quad \overline{R_i}(x) = \overline{0} \pmod{p} \text{ and } \overline{Q_i}(x) = \overline{\phi_i^{l_i - 1}(x) \prod_{j \neq i} \phi_j^{l_j}} \pmod{p}.$$

Thus there exists some  $H_i(x) \in R[x]$  such that

$$Q_i(x) = \phi_i^{l_i - 1}(x) \prod_{j \neq i} \phi_j^{l_j}(x) + pH_i(x).$$

Therefore,

$$F(x) = \left(\phi_i^{l_i-1}(x)\prod_{j\neq i}\phi_j^{l_j} + pH_i(x)\right)\phi_i(x) + R_i(x)$$

and

$$M(x) = \frac{F(x) - \prod_{j=1}^{r} \phi_j^{l_j}(x)}{p} = H_i(x)\phi_i(x) + \frac{R_i(x)}{p}$$

It follows that  $\overline{\phi}_i$  does not divide  $\overline{M}(x)$  in k(p)[x] if and only if  $\frac{R_i(x)}{p} \neq 0 \pmod{p}$ . That is  $\nu_p(R_i(x)) = 1$ .

**COROLLARY 2.2.** If R is a discrete valuation ring with maximal ideal (p), then the equality  $\mathbb{Z}_L = R[\alpha]$  holds if and only if for every  $i := 1, \ldots, r$ , either  $l_i = 1$ or  $l_i \geq 2$  and  $\nu_p(R_i(x)) = 1$ .

**COROLLARY 2.3.** Under the hypotheses of theorem 2.1, if R is a Dedekind domain, then for every prime ideal  $\mathfrak{p}$  of R,  $\mathfrak{p}$  does not divide the index  $[\mathbb{Z}_L : R[\alpha]]$  if and only if for every  $i := 1, \ldots, r$ , either  $l_i = 1$  or  $l_i \geq 2$  and  $R_i(x) \in \mathfrak{p}[X] - \mathfrak{p}^2[X]$ .

**Remark.** A similar result holds with applications in more general rings, namely Prüfer domains (cf. [9]). In This work, we are interested in another way, namely computation of integral bases.

**THEOREM 2.4.** Let  $L = K(\alpha)$ , where  $\alpha$  is any root of  $F(x) = \phi(x)^n - a \in R[x]$ such that  $\nu_p(a)$  and n are coprime and  $\phi(x) \in R[x]$  is a monic polynomial whose reduction modulo p is irreducible. Then  $\{\alpha^i \theta^j, 0 \le i < m-1 \text{ and } 0 \le j < n-1\}$ is a p-integral basis of  $\mathbb{Z}_L$ , where  $m = \deg(\phi)$ ,  $\theta = \frac{\phi(\alpha)^u}{p^v}$ , u and v are nonnegative integers satisfying  $\nu_p(a)u - nv = 1$  such that  $0 \le u < n$ .

Proof. First,  $L = F(\alpha)$ , where  $F = K(\phi(\alpha))$ ,  $g(x) = x^n - a$  is the minimal polynomial of  $\phi(\alpha)$  over K, and  $h(x) = \phi(x) - \phi(\alpha)$  is the minimal polynomial of  $\alpha$  over F. As  $\nu_p(a)$  and n are coprime, using the Euclid's algorithm, there exists a unique solution of non-negative integers (u, v) of  $\nu_p(a)u - nv = 1$ 

#### LHOUSSAIN EL FADIL

such that  $0 \leq u < n$ . Consider  $g_1(x) = x^n - \frac{a^u}{p^{nv}}$ . Then  $g_1(x) \in R[x]$  and  $g_1(\theta) = 0$ . Since  $\nu_p(\frac{a^u}{p^{nv}}) = \nu_p(a)u - nv = 1$ , by Eisenstein's criterion  $g_1(x)$  is irreducible in R[x]. By Theorem 2.1, p does not divide the index  $[\mathbb{Z}_F = R[\theta]]$ ;  $\{\theta^j, 0 \leq j < n-1\}$  is a p-integral basis of  $\mathbb{Z}_F$  over R. Thus  $p\mathbb{Z}_F = \mathfrak{p}^n$ , where  $\mathfrak{p} = (p, \theta)$ . As  $\overline{h}(x) = \overline{\phi}(x) \pmod{\mathfrak{p}}, \overline{\phi}(x)$  is irreducible over k(p), and  $f(\mathfrak{p}/p) = 1$ ;  $k(\mathfrak{p}) = k(p)$ , we have  $\overline{h}(x) = \overline{\phi}(x)$  is irreducible over  $k(\mathfrak{p})$ . Again by Theorem 2.1,

$$\left[\mathbb{Z}_L = \mathbb{Z}_F[\alpha]\right] \not\subset \mathfrak{p}; \qquad \{\alpha^i, \, 0 \le i < m-1\}$$

is a p-integral basis of  $\mathbb{Z}_L$  over  $\mathbb{Z}_F$ , where  $m = \deg(\phi)$ . Finally,

$$\{\alpha^i \theta^j, \ 0 \le i < m-1 \quad \text{and} \quad 0 \le j < n-1\}$$

is a *p*-integral basis of  $\mathbb{Z}_L$  over *R*.

In particular, if  $\phi(x) = x$ , then we have the following corollaries:

**COROLLARY 2.5.** Let p be a prime of R,  $L = K(\alpha)$ , where  $\alpha$  is a root of an irreducible polynomial  $F(x) = x^n - a \in R[x]$  such that  $\nu_p(a \text{ and } n \text{ are co-prime. Let } \theta = \frac{\alpha^u}{p^v}$ , where u and v are the unique non-negative integers satisfying  $\nu_p(a)u - nv = 1$  and  $0 \le u < n$ . Then p does not divide the index  $[\mathbb{Z}_L : R[\theta]]$ .

For any element  $\theta \in \mathbb{Z}_L$ , we say that  $\theta$  generates a power integral basis of  $\mathbb{Z}_L$  over R if  $(1, \theta, \dots, \theta^{n-1})$  is a R-basis of  $\mathbb{Z}_L$ , where n is the degree [L : K];  $\mathbb{Z}_L = R[\theta]$ . When a field L has a power integral basis, the field L is said to be monogenic. It is called a problem of Hasse to characterize whether the ring of integers in an algebraic number field has a power integral basis or does not [1–3]. The following corollaries give a condition on a in order to have the monogeneses of any field L defined by  $F(x) = x^n - a$ .

**COROLLARY 2.6.** Keep the assumptions and notations of Corollary 2.5, if R is a discrete valuation ring with maximal ideal (p), then  $\mathbb{Z}_L = R[\theta]$ , where  $\theta = \frac{\alpha^u}{p^v}$ and  $\alpha$  is a root of  $F(x) = x^n - a$ . We say that  $\theta$  generates a power integral basis of  $\mathbb{Z}_L$  over R.

**COROLLARY 2.7.** Let  $L = \mathbb{Q}(\alpha)$  be a pure prime number field;  $\alpha$  a complex root of an irreducible polynomial  $F(x) = x^p - a \in \mathbb{Z}[x]$ , where p is an odd prime. Assume that  $a = m^e$  with 0 < e < p and let  $\theta = \frac{\alpha^u}{m^v}$ , where u and v are the unique non-negative integers satisfying eu - nv = 1 and  $0 \le u < n$ . Then we have the following:

- If p divides m or p does not divide m and ν<sub>p</sub>(m<sup>p-1</sup> − 1) = 1, then Z<sub>L</sub> is monogenic. Especially Z<sub>L</sub> = Z[θ].
- (2) If p does not divide m and  $\nu_p(m^{p-1}-1) \ge 2$ , then  $(1, \theta, \dots, \theta^{p-2}, \frac{\theta^{p-1}}{p})$  is an integral basis of  $\mathbb{Z}_L$ .

**THEOREM 2.8.** Let  $L = \mathbb{Q}(\alpha)$  be a pure prime number field;  $\alpha$  is a complex root of an irreducible polynomial  $F(x) = x^p - a \in \mathbb{Z}[x]$ , where p is an odd prime. We can assume that  $\nu_q(a) < p$  for every prime integer q; set  $a = \mp \prod_{i=1}^r p_i^{e_i}$ the factorization of a into powers of positive prime integers such that for every  $i = 1, \ldots, r, e_i < p$ . Then we have the following:

(1) If p divides a or p does not divide a and  $\nu_p(a^{p-1}-1) = 1$ , then

$$\left(\frac{\alpha^k}{\prod_{i=1}^r p_i^{\lfloor \frac{ke_i}{p} \rfloor}}, \ 0 \le k < p\right) \quad is \ a \ \mathbb{Z}\text{-integral basis of } \mathbb{Z}_L.$$

(2) If p does not divide a and  $\nu_p(a^{p-1}-1) \ge 2$ , then

$$\left\{ \frac{\alpha^k}{\prod_{i=1}^r p_i^{\lfloor \frac{ke_i}{p} \rfloor}}, \ 0 \le k < p-1 \right\} \cup \left\{ \frac{\alpha^{p-1}}{p \prod_{i=1}^r p_i^{\lfloor \frac{(p-1)e_i}{p} \rfloor}} \right\}$$

is a  $\mathbb{Z}$ -integral basis of  $\mathbb{Z}_L$ .

Proof. (1) We have to check that for every positive prime integer q dividing  $\operatorname{disc}(F) = \mp p^p \cdot a^{p-1}$ , if q does not divide the index  $[\mathbb{Z}_L : \mathbb{Z}[\theta]]$ . Let  $p_i$  be a prime integer dividing a. Then  $\overline{F}(x) = x^p \pmod{p_i}$ , the Newton polygon  $N_x(F) = S$  is one sided of slope  $e_i/p$ , and its attached residual polynomial is  $F_S(y)$  is of degree 1 (because  $\operatorname{gcd}(l(S), h(S)) = 1$ , where l(S) and h(S) are the length and the height of S, respectively). Thus, by [6, Prop 2.1],

$$\left( \left\{ \frac{\alpha^k}{p_i^{\lfloor \frac{ke_i}{p} \rfloor}} \right\}, \ 0 \le k$$

If p does not divide a and  $\nu_p(a^{p-1}-1) = 1$ , then  $\overline{F}(x) = (x-a)^p \pmod{p}$ . Let  $H(x) = F(x+a) = x^p + \dots + pa^{p-1}x + a^p - a.$ 

Then

 $\overline{H}(x) = x^p \pmod{p}.$ 

As  $a^p - a$  is the remainder of H(x) by x and  $\nu_p(a^{p-1} - 1) = 1$ , by Theorem 2.1, q does not divide the index  $[\mathbb{Z}_L : \mathbb{Z}[\alpha]]$ .

(2) If p does not divide a and  $\nu_p(a^{p-1}-1) \ge 2$ , then  $\overline{H}(x) = x^p \pmod{p}$  and its x-Newton polygon

$$N_x(H) = S_1 + S_2,$$

where  $S_1$  is of height 1 and  $S_2$  is of length 1. Thus [6, Prop 2.1],

$$\left(1, \alpha, \dots, \alpha^{p-2}, \frac{\alpha^{p-1}}{p}\right)$$
 is a *p*-integral basis of  $\mathbb{Z}_L$ .

5

### 3. Examples

(1) Let

$$F(x) = x^{16} + 8x^{15} + 20x^{14} - 70x^{12} - 56x^{11} + 112x^{10} + 120x^9 - 125x^8 - 120x^7 + 112x^6 + 56x^5 - 70x^4 + 20x^2 - 8x - 7.$$

Since

$$F(x) = (x^2 + x - 1)^8 - 8, \quad \overline{\phi}(x) = \overline{x^2 + x - 1} \pmod{2}$$

is irreducible in  $\mathbb{F}_2[x]$ , and  $\nu_2(8)$  is coprime to 8, by [4, Theorem 1.6], F(x) is irreducible over  $\mathbb{Q}$ . Let  $\alpha$  be a complex root of F(x) and  $L = \mathbb{Q}(\alpha)$ . Since

 $\operatorname{disc}(F(x)) = \mp 2^{90}.73.1831$ , for every prime integer  $p \neq 2$ ,

p does not divide  $\operatorname{ind}(\alpha)$ . For p = 2, let  $\theta = \frac{\alpha^3}{2}$ . Then

 $(1, \theta, \dots, \theta^7, \alpha, \alpha\theta, \dots, \alpha\theta^7)$  is an integral basis of  $\mathbb{Z}_L$ .

(2) Let  

$$F(x) = x^{16} + 8x^{15} + 20x^{14} - 70x^{12} - 56x^{11} + 112x^{10} + 120x^9 - 125x^8 - 120x^7 + 112x^6 + 56x^5 - 70x^4 + 20x^2 - 8x - 23.$$

Since

$$F(x) = (x^2 + x - 1)^8 - 24,$$

it is a 3-Eisenstein polynomial. So it is irreducible over  $\mathbb{Q}$ . Let  $\alpha$  be a complex root of F(x) and  $L = \mathbb{Q}(\alpha)$ . Since  $\operatorname{disc}(F(x)) = \mp 2^{90}.3^{14}.163.7253$ , for every prime integer  $q \notin \{2,3\}$ , q does not divide  $\operatorname{ind}(\alpha)$ . For p = 2, let  $\theta = \frac{\alpha^3}{2}$ . Then 2 does not divide  $[\mathbb{Z}_L : \mathbb{Z}[\theta]]$ . For p = 3, since  $\nu_3(24) = 1$ , 3 does not divide  $[\mathbb{Z}_L : \mathbb{Z}[\alpha]]$ .

- (3) Let p be a non-negative prime integer,  $F(x) = x^p a \in \mathbb{Z}[x]$  an irreducible polynomial,  $\alpha$  a complex root of F(x), and  $L = \mathbb{Q}(\alpha)$ .
  - (a) For p = 5 and  $a = 22^2$ , let  $\theta = \frac{\alpha^4}{22^3}$ . Then for every prime integer  $q \notin \{2, 5, 11\}, q$  does not divide  $\operatorname{ind}(\alpha)$ . For  $q \in \{2, 11\}, q$  does not divide  $\operatorname{ind}(\theta)$ , too. For p = 5, since  $v_5(22^4 1) = 1, v_5(\operatorname{ind}(\theta)) = 0$ . Thus  $\mathbb{Z}_L$  is monogenic, with  $\theta = \frac{\alpha^4}{22^3}$  generating a power integral basis.
  - (b) Let p = 11 and  $a = 23^6 \cdot 11^5$ . Since disc $(F) = \pm 11^{11}a^{10}$ , for every prime  $q \notin \{2, 3, 11\}, p$  does not divide disc(F).

#### DEDEKIND'S CRITERION AND INTEGRAL BASES

$$E = \left\{ 1, \alpha, \alpha^2, \frac{\alpha^3}{11}, \frac{\alpha^4}{11}, \frac{\alpha^5}{11^2}, \frac{\alpha^6}{11^2}, \frac{\alpha^7}{11^3}, \frac{\alpha^8}{11^3}, \frac{\alpha^9}{11^4}, \frac{\alpha^{10}}{11^4} \right\}$$

is an 11-integral basis of  $\mathbb{Z}_L$ , i.e., 11 does not divide the index  $[\mathbb{Z}_L : S]$ , where S is the  $\mathbb{Z}$ -order generated by E. Similarly, by using  $\theta = \frac{\alpha^2}{3}$ , we get

$$T = \left\{ 1, \alpha, \frac{\alpha^2}{3}, \frac{\alpha^3}{3}, \frac{\alpha^4}{3^2}, \frac{\alpha^5}{3^2}, \frac{\alpha^6}{3^3}, \frac{\alpha^7}{3^3}, \frac{\alpha^8}{3^4}, \frac{\alpha^9}{3^4}, \frac{\alpha^{10}}{3^5} \right\}$$

as a 3-integral basis of  $\mathbb{Z}_L$ .

Thus,

$$B = \left\{1, \alpha, \frac{\alpha^2}{3}, \frac{\alpha^3}{3.11}, \frac{\alpha^4}{3^2.11}, \frac{\alpha^5}{3^2.11^2}, \frac{\alpha^6}{3^3.11^2}, \frac{\alpha^7}{3^3.11^3}, \frac{\alpha^8}{3^4.11^3}, \frac{\alpha^9}{3^4.11^4}, \frac{\alpha^{10}}{3^5.11^4}\right\}$$

is an integral basis of  $\mathbb{Z}_L$ .

(c) Let p = 11 and  $a = 3^6$ . Then disc $(F) = \pm 11^{11}3^{60}$ . For  $q \notin \{3, 11\}, q$  does not divide ind $(\alpha)$ . Then

$$\left\{1, \alpha, \frac{\alpha^2}{3}, \frac{\alpha^3}{3}, \frac{\alpha^4}{3^2}, \frac{\alpha^5}{3^2}, \frac{\alpha^6}{3^3}, \frac{\alpha^7}{3^3}, \frac{\alpha^8}{3^4}, \frac{\alpha^9}{3^4}, \frac{(\alpha - 3^6)^{10}}{11.3^5}\right\}$$

is an integral basis of  $\mathbb{Z}_L$ .

#### REFERENCES

- AHMAD, S.—NAKAHARA, T.—HUSNINE, S. M.: Power integral bases for certain pure sextic fields, Int. J. Number Theory 10 (2014), no. 8 2257–2265.
- [2] MOTODA, Y.—NAKAHARA, T.—SHAH, S.I.A.: On a problem of Hasse, J. Number Theory 96 (2002), 326–334.
- [3] HAMEED, A.—NAKAHARA, T.—HUSNINE, S. M.—AHMAD, S.: On existence of canonical number system in certain classes of pure algebraic number fields, J. Prime Res. Math. 7 (2011), 19–24.
- [4] COHEN, D.—MOVAHHEDI, A.—SALINIER, A.: , Factorization over local fields and the irreducibility of generalized difference polynomials, Mathematika 47 (2000), no. 1–2, 173–196.
- [5] COHEN, H.: A Course in Computational Algebraic Number Theory. In: Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, Berlin, 1993.
- [6] EL FADIL, L.—BOUGHALEB, O.: p-integral bases and prime ideal factorization in quintec fields, Gulf J. Math. 4 (2016), no. 4, 140–145.
- [7] ERSHOV, YU.L.: The Dedekind criterion for arbitrary valuation rings, Dokl. Akad. Nauk 410 (2006), no. 2, 158–160. (In Russian)

### LHOUSSAIN EL FADIL

- [8] DEDEKIND, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abhandl. Kgl. Ges. Wiss. Göttingen, 23 (1878) 1–23; Gesammelte mathematische Werke, I, Vieweg, 1932, 202–232.
- [9] KHUNDUJA, S.—JHORAR, B.: When is R[θ] integrally closed?, J. Algebra Appl. 15 (2016), no. 5; https://www.worldscientific.com/doi/10.1142/S0219498816500912

Received September 8 2018

Department of Mathematics Faculty of Sciences Dhar- El Mahraz Sidi Mohamed Ben Abdellah University P.O. Box 1796 Atlas-Fez MOROCCO E-mail: lhouelfadil2@gmail.com