Mathematical Publications
DOI: 10.2478/tmmp-2019-0001
Tatra Mt. Math. Publ. 73 (2019), 1-8

# 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 $\left[\mathbb{Z}_{L}: R[\alpha]\right]$, 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

$$
\nu_{p}\left(\sum_{i=0}^{l} a_{i} X^{l-i}\right)=\min \left\{\nu_{p}\left(a_{i}\right), 0 \leq i \leq l\right\} \quad \text { is also denoted by } \nu_{p} .
$$

Let $L=K(\alpha)$, where $\alpha$ is a root of a monic irreducible polynomial $F(x) \in R[x]$. Let $\operatorname{disc}(F)$ be the discriminant of $F, \mathbb{Z}_{L}$ the integral closure of $R$ in $L$, and $\operatorname{ind}(\alpha)=\left[\mathbb{Z}_{L}: R[\alpha]\right]$ 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 $\bar{M}(x)$, where

$$
M(x)=\frac{F(x)-\prod_{j=1}^{r} \phi_{j}^{l_{j}}(x)}{p} \quad \text { and } \quad \bar{F}(x)=\prod_{j=1}^{r} \bar{\phi}_{j}^{l_{j}}(x)(\bmod p)
$$

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

[^0]
## 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 $\operatorname{ind}(\alpha)=\left[\mathbb{Z}_{L}: R[\alpha]\right]$. Since $R$ is a principal ideal domain, $\mathbb{Z}_{L}$ is a free $R$-module of rank $n=\operatorname{deg}(F)$. Let $\mathbf{B}=\left\{u_{1}, \ldots, u_{n}\right\}$ be an $R$-basis of $\mathbb{Z}_{L}$ and $P_{B}^{F}$ the transition matrix from $\mathbf{B}$ to the $R$-basis $\mathbf{F}=\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ of $R[\alpha]$. The index $\left[\mathbb{Z}_{L}: R[\alpha]\right]$ is the principal ideal of $R$ generated by the determinant of $P_{B}^{F}$. It is well known that this principal ideal $\left[\mathbb{Z}_{L}: R[\alpha]\right]$ 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 $\mathbf{B}=\left\{u_{1}, \ldots, u_{n}\right\}$ an $R$-basis of $\mathbb{Z}_{L}$ and $\left(q_{1}, \ldots, q_{n}\right) \in R^{n}$ such that for every $i=1, \ldots, n-1, q_{i}$ divides $q_{i+1}$, and $\mathbf{F}=\left\{q_{1} u_{1}, \ldots, q_{n} u_{n}\right\}$ 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 $\left[\mathbb{Z}_{L}: R[\alpha]\right]$ 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

$$
F(x) \equiv \prod_{i=1}^{r} \phi_{i}^{l_{i}}(x)(\bmod p)
$$

be the factorization of $\bar{F}(x)$ 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 $\left[\mathbb{Z}_{L}\right.$ : $R[\alpha]]$ if and only if for every $i:=1, \ldots, r$, either $l_{i}=1$ or $l_{i} \geq 2$ and $\nu_{p}\left(R_{i}(x)\right)=1$.

Proof. If for every $i:=1, \ldots, r, l_{i}=1$, then by the generalized Dedekind's criterion $p$ does not divide $\operatorname{ind}(\alpha)$ (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 $i=1, \ldots, r$, with $l_{i} \geq 2, \nu_{p}\left(R_{i}(x)\right)=1$ if and only if $\bar{\phi}_{i}$ does not divide $\bar{M}(x)$ in $k(p)[x]$.

Indeed, as
then $\overline{\phi_{i}}(x)$ divides

$$
F(x) \equiv \prod_{j=1}^{r} \phi_{j}^{l_{j}}(x)(\bmod p)
$$

$$
\bar{F}(x), \quad \overline{R_{i}}(x)=\overline{0}(\bmod p) \quad \text { and } \quad \overline{Q_{i}}(x)=\overline{\phi_{i}^{l_{i}-1}(x) \prod_{j \neq i} \phi_{j}^{l_{j}}}(\bmod p)
$$

Thus there exists some $H_{i}(x) \in R[x]$ such that

$$
Q_{i}(x)=\phi_{i}^{l_{i}-1}(x) \prod_{j \neq i} \phi_{j}^{l_{j}}(x)+p H_{i}(x)
$$

Therefore,

$$
F(x)=\left(\phi_{i}^{l_{i}-1}(x) \prod_{j \neq i} \phi_{j}^{l_{j}}+p H_{i}(x)\right) \phi_{i}(x)+R_{i}(x)
$$

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 $\bar{\phi}_{i}$ does not divide $\bar{M}(x)$ in $k(p)[x]$ if and only if $\frac{R_{i}(x)}{p} \not \equiv 0(\bmod p)$. That is $\nu_{p}\left(R_{i}(x)\right)=1$.
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 $\nu_{p}\left(R_{i}(x)\right)=1$.
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 $\left[\mathbb{Z}_{L}: R[\alpha]\right]$ 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 $\left\{\alpha^{i} \theta^{j}, 0 \leq i<m-1\right.$ and $\left.0 \leq j<n-1\right\}$ is a p-integral basis of $\mathbb{Z}_{L}$, where $m=\operatorname{deg}(\phi), \theta=\frac{\phi(\alpha)^{u}}{p^{v}}, u$ and $v$ are nonnegative integers satisfying $\nu_{p}(a) u-n v=1$ such that $0 \leq u<n$.
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 $\nu_{p}(a) u-n v=1$

## LHOUSSAIN EL FADIL

such that $0 \leq u<n$. Consider $g_{1}(x)=x^{n}-\frac{a^{u}}{p^{n v}}$. Then $g_{1}(x) \in R[x]$ and $g_{1}(\theta)=0$. Since $\nu_{p}\left(\frac{a^{u}}{p^{n v}}\right)=\nu_{p}(a) u-n v=1$, by Eisenstein's criterion $g_{1}(x)$ is irreducible in $R[x]$. By Theorem [2.1, $p$ does not divide the index $\left[\mathbb{Z}_{F}=R[\theta]\right] ;\left\{\theta^{j}, 0 \leq\right.$ $j<n-1\}$ 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 $\bar{h}(x)=\bar{\phi}(x)(\bmod \mathfrak{p}), \bar{\phi}(x)$ is irreducible over $k(p)$, and $f(\mathfrak{p} / p)=1 ; k(\mathfrak{p})=k(p)$, we have $\bar{h}(x)=\bar{\phi}(x)$ is irreducible over $k(\mathfrak{p})$. Again by Theorem 2.1,

$$
\left[\mathbb{Z}_{L}=\mathbb{Z}_{F}[\alpha]\right] \not \subset \mathfrak{p} ; \quad\left\{\alpha^{i}, 0 \leq i<m-1\right\}
$$

is a $\mathfrak{p}$-integral basis of $\mathbb{Z}_{L}$ over $\mathbb{Z}_{F}$, where $m=\operatorname{deg}(\phi)$. Finally,

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

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 $\nu_{p}(a$ and $n$ are coprime. Let $\theta=\frac{\alpha^{u}}{p^{v}}$, where $u$ and $v$ are the unique non-negative integers satisfying $\nu_{p}(a) u-n v=1$ and $0 \leq u<n$. Then $p$ does not divide the index $\left[\mathbb{Z}_{L}: R[\theta]\right]$.

For any element $\theta \in \mathbb{Z}_{L}$, we say that $\theta$ generates a power integral basis of $\mathbb{Z}_{L}$ over $R$ if $\left(1, \theta, \ldots, \theta^{n-1}\right)$ 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 $0 \leq u<n$. Then we have the following:
(1) If $p$ divides $m$ or $p$ does not divide $m$ and $\nu_{p}\left(m^{p-1}-1\right)=1$, then $\mathbb{Z}_{L}$ is monogenic. Especially $\mathbb{Z}_{L}=\mathbb{Z}[\theta]$.
(2) If $p$ does not divide $m$ and $\nu_{p}\left(m^{p-1}-1\right) \geq 2$, then $\left(1, \theta, \ldots, \theta^{p-2}, \frac{\theta^{p-1}}{p}\right)$ is an integral basis of $\mathbb{Z}_{L}$.

## DEDEKIND'S CRITERION AND INTEGRAL BASES

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 $\nu_{p}\left(a^{p-1}-1\right)=1$, then

$$
\left(\frac{\alpha^{k}}{\prod_{i=1}^{r} p_{i}^{\left\lfloor\frac{k e_{i}}{p}\right\rfloor}}, 0 \leq k<p\right) \quad \text { is a } \mathbb{Z} \text {-integral basis of } \mathbb{Z}_{L}
$$

(2) If $p$ does not divide $a$ and $\nu_{p}\left(a^{p-1}-1\right) \geq 2$, then

$$
\left\{\frac{\alpha^{k}}{\prod_{i=1}^{r} p_{i}^{\left\lfloor\frac{k e_{i}}{p}\right\rfloor}}, 0 \leq k<p-1\right\} \cup\left\{\frac{\alpha^{p-1}}{p \prod_{i=1}^{r} p_{i}^{\left\lfloor\frac{(p-1) e_{i}}{p}\right\rfloor}}\right\}
$$

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 $\left[\mathbb{Z}_{L}: \mathbb{Z}[\theta]\right]$. Let $p_{i}$ be a prime integer dividing $a$. Then $\bar{F}(x)=x^{p}\left(\bmod p_{i}\right)$, 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],

$$
\left(\left\{\frac{\alpha^{k}}{p_{i}^{\left\lfloor\frac{k e_{i}}{p}\right\rfloor}}\right\}, 0 \leq k<p\right) \quad \text { is a } p_{i} \text {-integral basis of } \mathbb{Z}_{L}
$$

If $p$ does not divide $a$ and $\nu_{p}\left(a^{p-1}-1\right)=1$, then $\bar{F}(x)=(x-a)^{p}(\bmod p)$. Let

$$
H(x)=F(x+a)=x^{p}+\cdots+p a^{p-1} x+a^{p}-a .
$$

Then

$$
\bar{H}(x)=x^{p}(\bmod p)
$$

As $a^{p}-a$ is the remainder of $H(x)$ by $x$ and $\nu_{p}\left(a^{p-1}-1\right)=1$, by Theorem 2.1, $q$ does not divide the index $\left[\mathbb{Z}_{L}: \mathbb{Z}[\alpha]\right]$.
(2) If $p$ does not divide $a$ and $\nu_{p}\left(a^{p-1}-1\right) \geq 2$, then $\bar{H}(x)=x^{p}(\bmod p)$ 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],

$$
\left(1, \alpha, \ldots, \alpha^{p-2}, \frac{\alpha^{p-1}}{p}\right) \quad \text { is a } p \text {-integral basis of } \mathbb{Z}_{L} .
$$

## 3. Examples

(1) Let

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

Since

$$
F(x)=\left(x^{2}+x-1\right)^{8}-8, \quad \bar{\phi}(x)=\overline{x^{2}+x-1}(\bmod 2)
$$

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
$\operatorname{disc}(F(x))=\mp 2^{90} .73 .1831, \quad$ for every prime integer $p \neq 2$, $p$ does not divide $\operatorname{ind}(\alpha)$. For $p=2$, let $\theta=\frac{\alpha^{3}}{2}$. Then

$$
\left(1, \theta, \ldots, \theta^{7}, \alpha, \alpha \theta, \ldots, \alpha \theta^{7}\right) \quad \text { is an integral basis of } \mathbb{Z}_{L}
$$

(2) Let
$F(x)=x^{16}+8 x^{15}+20 x^{14}-70 x^{12}-56 x^{11}+112 x^{10}+120 x^{9}$

$$
-125 x^{8}-120 x^{7}+112 x^{6}+56 x^{5}-70 x^{4}+20 x^{2}-8 x-23
$$

Since

$$
F(x)=\left(x^{2}+x-1\right)^{8}-24
$$

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 ind $(\alpha)$. For $p=2$, let $\theta=\frac{\alpha^{3}}{2}$. Then 2 does not divide $\left[\mathbb{Z}_{L}: \mathbb{Z}[\theta]\right]$. For $p=3$, since $\nu_{3}(24)=1$, 3 does not divide $\left[\mathbb{Z}_{L}: \mathbb{Z}[\alpha]\right]$.
(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 $v_{5}\left(22^{4}-1\right)=1, v_{5}(\operatorname{ind}(\theta))=0$. Thus $\mathbb{Z}_{L}$ is monogenic, with $\theta=\frac{\alpha^{4}}{22^{3}}$ generating a power integral basis.
(b) Let $p=11$ and $a=23^{6} .11^{5}$. Since $\operatorname{disc}(F)= \pm 11^{11} a^{10}$, for every prime $q \notin\{2,3,11\}, p$ does not divide $\operatorname{disc}(F)$.

## 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 $\left[\mathbb{Z}_{L}: S\right]$, 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 $\operatorname{disc}(F)= \pm 11^{11} 3^{60}$. For $q \notin\{3,11\}, q$ does not divide ind $(\alpha)$. Then

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

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

## REFERENCES

[1] 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 $R[\theta]$ integrally closed?, J. Algebra Appl. 15 (2016), no. 5; https://www.worldscientific.com/doi/10.1142/S0219498816500912

Received September 82018
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


[^0]:    (c) 2019 Mathematical Institute, Slovak Academy of Sciences.

    2010 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.

