Mathematica Bohemica

Mohammed Sahmoudi; Mohamed E. Charkani

On relative pure cyclic fields with power integral bases

Mathematica Bohemica, Vol. 148 (2023), No. 1, 117–128

Persistent URL: http://dml.cz/dmlcz/151531

ON RELATIVE PURE CYCLIC FIELDS WITH POWER INTEGRAL BASES

Mohammed Sahmoudi, Kenitra, Mohamed E. Charkani, Fez

Received September 11, 2021. Published online April 28, 2022.
Communicated by Clemens Fuchs

Abstract. Let $L = K(\alpha)$ be an extension of a number field K, where α satisfies the monic irreducible polynomial $P(X) = X^p - \beta$ of prime degree belonging to $\mathfrak{o}_K[X]$ ($\mathfrak{o}_K$ is the ring of integers of K). The purpose of this paper is to study the monogenity of L over K by a simple and practical version of Dedekind's criterion characterizing the existence of power integral bases over an arbitrary Dedekind ring by using the Gauss valuation and the index ideal. As an illustration, we determine an integral basis of a pure nonic field L with a pure cubic subfield, which is not necessarily a composite extension of two cubic subfields. We obtain a slightly simpler computation of the discriminant $d_{L/\mathbb{Q}}$.

Keywords: discrete valuation ring; Dedekind ring; monogenity; relative integral basis; nonic field

MSC 2020: 11Rxx, 11R04, 11R21, 11Y40, 11R16

1. Introduction

Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension. It is well known that the integral closure $\mathfrak{o}_L$ of R in L is not necessarily a free R-module but a projective R-module of finite local constant rank (see [2]). We say that a field L posseses a relative integral basis (RIB for short) if $\mathfrak{o}_L$ is finite free R-module (i.e., $\mathfrak{o}_L$ admits a finite basis over R). The problem of the existence or nonexistence of RIB is a hard open problem and there are only few results for some pure cyclic extensions of small degree (of degree 2 and 3, see [19], Theorem 2; [27] and [29]). A particular case of this problem is the question of monogenity. The field L is said to be monogenic if $\mathfrak{o}_L = R[\theta]$ for some element θ in $\mathfrak{o}_L$. In this case the field L is said to possess a power integral basis (PIB for short). The problem of monogenity is a classical topic of algebraic number theory. It was

DOI: 10.21136/MB.2022.0142-21

originally examined by Dedekind (see [11]) and since then many number theorists have been attracted (cf. [3], [4], [5], [8], [9], [13], [14], [15], [18], [20], [22], [23], [24], [26], [27], [28] and others). Indeed, there are several results on the existence or nonexistence of PIB for certain Abelian extensions $L/\mathbb{Q}$, or certain relative Abelian extensions L/K where both K and L are certain ray class fields of an imaginary quadratic field (see [3], [4], [15], [20], [27]). Except for those investigations, there are few results on PIB for relative extensions of degree greater than 4 and published works deal with decomposable extensions (which are the composite of two pure subfields). There is no known work for relative Abelian indecomposable extension L/K of higher degree (i.e., which is not a composite at last of two "pure" subfields). The purpose of this paper is the study of the monogenity of pure cyclic extensions of degree equal to an arbitrary odd prime number p over a number field. Our method in this paper is, in the first step, to provide a new version of the Dedekind criterion (Theorem 4.1) that tests when a given $\alpha \in \mathfrak{o}_L$ generates a power integral basis for $\mathfrak{o}_L$ over R (i.e., it tests when $\mathfrak{o}_L = R[\alpha]$, see 4.1) and, in the second step, to apply the previous results to study the monogenity of relative pure cyclic fields of degree equal to an odd prime number. Indeed, Theorem 4.1 and Proposition 4.2 give a necessary and sufficient condition for a relative cyclic extension to admit a power integral basis (PIB). Using the previous work, we find a simpler condition for a cubic relative field to have PIB (Theorem 5.1) and we exhibit an integral basis for nonic extensions $L = K(\alpha)$, which are relative cubic over a pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$ where α is a root of a monic irreducible polynomial $P(X) = X^3 - \beta \in \mathfrak{o}_K[X]$ and m is cube-free, not equal to ± 1. As a consequence, we compute the discriminant $d_{L/\mathbb{Q}}$ given by the tower formula

$$d_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(d_{L/K}) \cdot (d_{K/\mathbb{Q}})^{[L:K]},$$

where $N_{K/\mathbb{Q}}$ denotes the norm from K to $\mathbb{Q}$ (see [21], Corollary 10.2 and [12]).

2. Preliminaries

Throughout this paper, R is a Dedekind ring of characteristic zero (i.e., containing $\mathbb{Z}$), K its fraction field. Let $\mathfrak{p}$ be a nonzero prime ideal in R and $v_\mathfrak{p}$ the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Hence, for each nonzero element $a \in R$, $v_\mathfrak{p}(a)$ is the greatest nonnegative integer l such that $\mathfrak{p}^l$ divides aR.

Let L be a finite separable extension of K, $\mathfrak{o}_L$ the integral closure of R in L and $\alpha \in \mathfrak{o}_L$ such that $L = K(\alpha)$. Recall that the primitive element α of L is said to be a power basis generator over K (PBG for short) if $\mathfrak{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis of $\mathfrak{o}_L$ over R (i.e., $\mathfrak{o}_L = R[\alpha]$). Then L/K is monogenic, if L admits a power basis generator over K.

The index ideal $[\mathfrak{o}_L : R[\alpha]]_R$ of R is called the index of α over R (for details on the index ideal, see [2], [6] or [12]) and may also be denoted by $\mathrm{Ind}_R(\alpha)$. It is clear that $\mathfrak{o}_L = R[\alpha]$ if and only if $\mathrm{Ind}_R(\alpha) = R$.

Let $P \in K[X]$ be the minimal monic irreducible polynomial of α over K. Since R is integrally closed, then $P \in R[X]$ (see [16], page 7). Let $\mathrm{Disc}_R(P)$ be the principal ideal of R generated by $\mathrm{Res}(P, P')$, where $\mathrm{Res}(P, P')$ denotes the resultant of the two polynomials P and its derivative P'. The index-discriminant formula

$$\mathrm{Disc}_R(P) = \mathrm{Ind}_R(\alpha)^2 D_R(\mathfrak{o}_L) \tag{2.1}$$

is well known (see [2], [6] or [12]).

In view of the index-discriminant formula (2.1), the element α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $[\mathfrak{o}_L : R[\alpha]]_R$ for any nonzero prime ideal $\mathfrak{p}$ in R such that $\mathfrak{p}^2$ divides $\mathrm{Disc}_R(P)$. This fact lead us to introduce, for any irreducible polynomial P, the set S_P of primes ideal whose square divides the ideal $\mathrm{Disc}_R(P)$. Then:

$$S_P = \{\mathfrak{p} \in \mathrm{spec}\, R\colon\ \mathfrak{p}^2 \text{ divides } \mathrm{Disc}_R(P)\}.$$

We see that the set S_P is very useful when using the Dedekind criterion (see Theorem 4.1) in order to decide if L is monogenic or not. Indeed S_P is the set of nonzero prime ideals, which may divide the ideal $\mathrm{Ind}_R(\alpha)$.

Before presenting the main results, we state some lemmas that we will use later.

3. Some lemmas

Let R be a commutative ring, let $\mathfrak{p}$ be a prime ideal in R and $S = R \setminus \mathfrak{p}$. The resulting localization $S^{-1}M$ is usually denoted by $M_\mathfrak{p}$ and called the localization of M at the prime ideal $\mathfrak{p}$ for an R-module M. Let M and N be two R-modules such that $N \subseteq M$. It is well known (by applying [1], Proposition 3.8, page 40 to the R-module quotient M/N) that $N = M$ if and only if $M_\mathfrak{p} = N_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of R. When R is a Dedekind ring and $N \subseteq M$ are two projective R-modules of the same finite constant rank, then $M_\mathfrak{p} = N_\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of R (see [2], Lemma 3, page 10). More precisely, we assert the following deep result.

Lemma 3.1. *Let R be a Dedekind ring and $N \subseteq M$ be two projective R-modules of the same finite constant rank. Then $[M_\mathfrak{p} : N_\mathfrak{p}]_{R_\mathfrak{p}} = ([M : N]_R)_\mathfrak{p}$ for any nonzero prime ideal $\mathfrak{p}$ in R. In particular, $N = M$ if and only if $M_\mathfrak{p} = N_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of R which divides the index ideal $[M : N]_R$.*

P r o o f. Indeed, by applying Proposition 3.8, page 40 in [1] to the R-module quotient M/N we see that $N = M$ if and only if $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of R. On the other hand, $[M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{R_{\mathfrak{p}}} = ([M : N]_R) \cdot R_{\mathfrak{p}}$ for any nonzero prime ideal $\mathfrak{p}$ in R (see [6] or [2], property (2), page 10). Therefore, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for any nonzero prime ideal $\mathfrak{p}$ in R which doesn't divide the index ideal $[M : N]_R$. To conclude, it suffices then to use Proposition 3.8, page 40 in [1]. □

Lemma 3.2. *Let R be an integrally closed ring and K its quotient field, L a finite separable extension of K, α a primitive element of L integral over R. Then $(R[\alpha])_{\mathfrak{p}} = R_{\mathfrak{p}}[\alpha]$ for every prime ideal $\mathfrak{p}$ of R. In particular, $\mathfrak{o}_L = R[\alpha]$ if and only if $R_{\mathfrak{p}}[\alpha]$ is integrally closed for every prime ideal $\mathfrak{p}$ of R if and only if $R[\alpha]$ is integrally closed.*

P r o o f. We obtain the result from the isomorphism $R[\alpha] = R[X]/\langle P(X)\rangle$, the properties of an integrally closed ring and its integral closure, and the properties of a multiplicatively closed subset S of a ring R, notably, $S^{-1}(R[X]) = (S^{-1}R)[X]$ (see [1]). □

R e m a r k 3.1. Let us keep the notation of Lemma 3.2. Let B be the integral closure of $R_{\mathfrak{p}}$ in L. Then $B = (\mathfrak{o}_L)_{\mathfrak{p}}$ where $(\mathfrak{o}_L)_{\mathfrak{p}}$ is the localization of $\mathfrak{o}_L$ by the prime ideal $\mathfrak{p}$ (see [1], Proposition 5.12, page 62).

Lemma 3.3. *Let R be a Dedekind ring, K its fraction field, L a finite separable extension over K and $\mathfrak{o}_L$ the integral closure of R in L. Let $\alpha \in \mathfrak{o}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $\mathfrak{p}$ be a nonzero prime ideal in R and B the integral closure of $R_{\mathfrak{p}}$ in L. Then $\mathrm{Ind}_{R_{\mathfrak{p}}}(\alpha) = (\mathrm{Ind}_R(\alpha))_{\mathfrak{p}}$. In particular $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $B = R_{\mathfrak{p}}[\alpha]$.*

P r o o f. We obtain the result from Lemma 3.1 and Lemma 3.2, and the fact that any multiplicatively closed subset S of a ring R permutes with the integral closure (see [1], Proposition 5.12, page 62), notably, $S^{-1}(\mathfrak{o}_L)$ is equal to the integral closure of $(S^{-1}R)$ in L like in Remark 3.1. □

The spectrum of a commutative ring R, denoted by $\mathrm{Spec}(R)$, is the set of prime ideals of R.

Lemma 3.4. *Let R be a Dedekind ring, K its fraction field, L a finite separable extension over K and $\mathfrak{o}_L$ the integral closure of R in L. Let $\alpha \in \mathfrak{o}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $P \in R[X]$ be the monic minimal polynomial of α and $S_P = \{\mathfrak{p} \in \mathrm{Spec}(R) \colon \mathfrak{p}^2$ divides $\mathrm{Disc}_R(P)\}$. Then α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P.*

P r o o f. Indeed, we see that if $\mathfrak{p}$ is a nonzero prime ideal in R and $\mathfrak{p} \notin S_P$ then—by the index-discriminant formula—$\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$. We obtain the result from Lemmas 3.1–3.3, and the fact that α is a PBG of L over K if and only if $(\mathfrak{o}_L)_\mathfrak{p} = R_\mathfrak{p}[\alpha]$, for all nonzero prime ideals $\mathfrak{p}$ in R if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for all nonzero prime ideals $\mathfrak{p}$ in S_P. □

$\mathrm{Spec}(R)$ is equipped with the Zariski topology, for which the closed sets are the sets

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R)\colon\ I \subseteq \mathfrak{p}\}$$

where I is an ideal in R. Note also that for any ideal I in R and $n \in \mathbb{N}$ we have $V(I^n) = V(I)$. So, from a suitable condition we have the following basic result.

Lemma 3.5. *Let R be a Dedekind ring, K its fraction field and $\mathfrak{o}_K$ be the integral closure of R in K. Given any $(s, m) \in \mathbb{N}^* \times \mathbb{N}$, we put $\theta = \sqrt[s]{m}$ and assume that $\theta \in \mathfrak{o}_K$. Then $V(\theta\mathfrak{o}_K) = V(m\mathfrak{o}_K)$.*

Lemma 3.6. *Let $(R, \mathfrak{p} = \pi R, k)$ be a discrete valuation ring with a finite residue field k. Suppose that the characteristic of R is zero and $pR = \mathfrak{p}^e$ where p is a prime number. Let $\beta \in R - \mathfrak{p}$ and $t = |k|$ the cardinality of k. Let s be a positive integer less than or equal to $\min(p, e+1)$. Then β is a p-power modulo $\mathfrak{p}^s$ if and only if $v_\pi(\beta^{t-1} - 1) \geqslant s$.*

P r o o f. Let $a \in R$ be such that $\beta \equiv a^p \bmod \mathfrak{p}^s$, then $\beta^{t-1} \equiv a^{p(t-1)} \bmod \mathfrak{p}^s$. But $a^{(t-1)} \equiv 1 \bmod \mathfrak{p}$ (since $a \notin \mathfrak{p}$), then $a^{t-1} = 1 + \pi u$ $(u \in R)$ and hence $a^{p(t-1)} = 1 + \pi^p u^p + \pi^{e+1} v$. As $s \leqslant \min(p, e+1)$, then $a^{p(t-1)} \equiv 1 \bmod \mathfrak{p}^s$. From this we conclude $\beta^{t-1} \equiv 1 \bmod \mathfrak{p}^s$. Conversely, suppose that $v_\mathfrak{p}(\beta^{t-1} - 1) \geqslant s$, then $\beta^{t-1} = 1 + \pi^s b$ $(b \in R)$ and like $p \nmid t-1$ there exists $(u, v) \in \mathbb{Z}^2$ such that $up + v(t-1) = 1$, therefore $\beta = \beta^{up} + c\pi^s\beta^{up}$ with $c \in R$ since $\beta^{v(t-1)} \equiv 1 \bmod \mathfrak{p}^s$. It follows that $\beta = a^p + z\pi^s$ where $a = \beta^u$, $z = c\beta^{up}$. Consequently, $\beta \equiv a^p \bmod \mathfrak{p}^s$. □

4. Monogenity of relative cyclic extensions

4.1. Dedekind criterion for relative extensions using Gaussian valuation. Let K be a nonzero commutative field and v be a valuation on K. Let $P = a_0 + a_1X + \ldots + a_nX^n \in K[X]$. We put $v_G(P) = \inf\{v(a_i)\colon\ 0 \leqslant i \leqslant n\}$. Then v_G is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to v. First we present a new simple version of the Dedekind criterion in global case.

Theorem 4.1 (Dedekind criterion)**.** *Let R be a Dedekind ring, K its fraction field, L be a finite separable extension over K and $\mathfrak{o}_L$ be the integral closure of R in L. Let $\alpha \in \mathfrak{o}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let*

$P = \mathrm{Irrd}(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a nonzero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\overline{P}$ be the image in $k[X]$ of P and assume that $\overline{P} = \prod_{i=1}^{r} \overline{P_i}^{l_i}$ is the prime decomposition of $\overline{P}$ in $k[X]$ with $P_i \in R[X]$ being a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \leqslant i \leqslant r$. Let $V_i \in R[X]$ be the remainder of the Euclidean division of P by P_i. Let $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let υ_G be the Gauss valuation on $K[X]$ associated to $\upsilon_{\mathfrak{p}}$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geqslant 2$.

P r o o f. In view of Proposition 3.2, it suffices to show the result in the local case. Then we can assume that $(R, \mathfrak{p}, k)$ is a discrete valuation ring, K its quotient field, $\mathfrak{p} = \pi R$ its maximal ideal and $k = R/\mathfrak{p}$ its residual field. Let α be an algebraic integer over R, $A = R[\alpha]$ and $L = K(\alpha)$ a finite separable extension over K.

Let $T \in R[X]$ satisfying $P = \prod_{i=1}^{r} P_i^{l_i} + \pi T$ where π is a uniformizer of R. Let $U_i \in R[X]$ be the remainder of the Euclidean division of T by P_i and $V_i \in R[X]$ the remainder of the Euclidean division of P by P_i. The uniqueness of the remainder shows that $V_i = \pi U_i$. As $\overline{P}_i$ is irreducible then $\gcd(\overline{P}_i, \overline{T}) = 1$ if and only if $\overline{U}_i \neq \overline{0}$, which is equivalent to $\upsilon_G(U_i) = 0$ and therefore to $\upsilon_G(V_i) = 1$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if the element α is a PBG of L over $R_{\mathfrak{p}}$ (see [17] and Lemma 3.3).

Finally, by the Dedekind criterion (see [5], Theorem 3.1, [17] or [25]), the element α is PBG of L over $R_{\mathfrak{p}}$ if and only if $\gcd(\overline{P}_i, \overline{T}) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geqslant 2$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geqslant 2$. □

4.2. Monogenity of relative pure cyclic extension: Local case. Let R be a Dedekind ring containing $\mathbb{Z}$ and $\mathfrak{p}$ be a nonzero prime ideal in R. It is clear that $\mathrm{char}(R/\mathfrak{p}) = p$ if and only $\mathfrak{p} \in V(pR)$. Let $P = X^p - \beta$ be a monic irreducible polynomial in $R[X]$ (p is an odd prime number). Then the discriminant of P is equal to $\mathrm{Disc}_R(P) = p^p \beta^{(p-1)} R$. As $p \geqslant 3$, then the set $S_P = V(pR) \cup V(\beta R)$. Now it is time to give our first main result.

Theorem 4.2. *Let $(R, \mathfrak{p} = \pi R, k)$ be a discrete valuation ring with a finite residual field. Let K be the quotient field of R, L a finite separable extension of K, α a primitive element of L which is integral over R, and $P = X^p - \beta$ its monic irreducible polynomial in $R[X]$, where p is an odd prime number. Let $\upsilon_\pi = \upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Suppose that the characteristic of the residual field k is a prime number q. Let $t = |k|$ be the cardinality of k (i.e., the number of elements in k). If $\beta \in \mathfrak{p}$ then α is a PBG of L/K if and only if $\upsilon_\pi(\beta) = 1$. Suppose that $\beta \in R - \mathfrak{p}$. Then the following properties hold:*

(1) *If $q = p$, then the following assumptions are equivalent:*
   (a) *α is a PBG of L/K,*
   (b) *$\upsilon_\pi(\beta^{t-1} - 1) = 1$,*
   (c) *β is not a p-power modulo π^2.*

(2) *If $q \neq p$ then α is a PBG of L/K.*

We summarize our results in Table 1.

$\upsilon_{\mathfrak{p}}(b) \geqslant 1$	α is a PBG $\Leftrightarrow \upsilon_\pi(b) = 1$	
	$q \neq p$	$q = p$
$\upsilon_{\mathfrak{p}}(b) = 0$	α is a PBG	α is a PBG $\Leftrightarrow \upsilon_\pi(\beta^{t-1} - 1) = 1$

Table 1. Monogenity in the local case.

P r o o f. For simplicity of notations, write s instead of $\upsilon_\pi(\beta)$. If $\beta \in \mathfrak{p}$, then the remainder of the Euclidean division of P by X is $r(X) = \beta$. Hence, from Theorem 4.1, α is a PBG if and only if $\upsilon_\pi(\beta) = 1$. We now turn to the case $\beta \in R - \mathfrak{p}$.

(1) Assume that $q = p$.

(a) $\Leftrightarrow$ (b): As $s = 0$, then $S_P = \{\pi R\}$. Reducing P modulo the prime ideal πR of R which lies above pR yields

$$\begin{aligned}\overline{P(X)} &\equiv \overline{X}^p - \overline{\beta} \bmod \pi R \\ &\equiv \overline{X}^p - \overline{\beta}^t \bmod \pi R \quad (\text{since } \beta^t \equiv \beta \bmod \pi) \\ &\equiv (\overline{X} - \overline{\beta}^{p^{f-1}})^p \bmod \pi R.\end{aligned}$$

Moreover, let $r(X)$ be the remainder of the Euclidean division of P by $X - \beta^{p^{f-1}}$. It is clear that $r(X) = P(\beta^{p^{f-1}})$ and then $r(X) = \beta^{p^f} - \beta$. Hence α is a PBG if and only if $\upsilon_\pi(\beta^t - \beta) = 1$.

(b) $\Leftrightarrow$ (c): We apply Lemma 3.6 above for $s = 2$.

(2) Assume that $q \neq p$. Since $\beta \in R - \mathfrak{p}$, it follows that P is a separable polynomial. Otherwise, if P has α as a double root, then from $P'(X) = pX^{p-1}$ we get $\alpha = 0$ which means that $\beta \in \mathfrak{p}$ and completes the proof in this case. □

R e m a r k 4.1. Let us keep all the notations of Proposition 4.2. We can resume the above result as follows.

(1) If $\mathrm{char}(k) = p$ then α is a PBG of L/K if and only if $\upsilon_{\mathfrak{p}}(\beta^t - \beta) = 1$.
(2) If $\mathrm{char}(k) \neq p$ then α is a PBG of L/K if and only if $\upsilon_{\mathfrak{p}}(\beta) \leqslant 1$.

4.3. Monogenity of relative pure cyclic extension: the Dedekind case. Let R be a commutative ring containing $\mathbb{Z}$, K its fraction field and p a prime number. We denote by $\mathrm{Fib}_K(p)$ or $\mathrm{Fib}_R(p)$ the set all nonzero prime ideals in R which lie above p. It is clear that if R is a Dedekind ring then $\mathrm{Fib}_R(p) = V(\mathfrak{p}R)$.

Let R be a Dedekind ring containing $\mathbb{Z}$ and $P = X^p - \beta$ a monic irreducible polynomial in $R[X]$. Recall that the discriminant of P is equal to $\mathrm{Disc}_R(P) = p^p\beta^{(p-1)}R$. As $p \geqslant 3$, then the set $S_P = \mathrm{Fib}_R(p) \cup V(\beta R)$. Note also that if $\mathfrak{p}$ is a nonzero prime ideal in R then $\mathrm{char}(R/\mathfrak{p}) = p$ if and only $\mathfrak{p} \in \mathrm{Fib}_R(p)$.

Theorem 4.3. *Let R be a Dedekind ring with a finite residual field and K its fraction field. Assume that* $\mathrm{char}\, K = 0$ *and $L = K(\alpha)$ is a finite separable extension of K. Let $P = X^p - \beta \in R[X]$ be the monic minimal polynomial of α, where p is an odd prime number. Then*

(1) *If $\mathrm{Fib}_R(p) \subseteq V(\beta R)$, then α is a PBG of L over K if and only if β is square free.*
(2) *Assume that $\mathrm{Fib}_R(p) \nsubseteq V(\beta R)$. Let $\mathrm{Fib}_R(p) - V(\beta R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. For all $i \in \{1, \ldots, s\}$, let us denote by v_i the $\mathfrak{p}_i$-adic valuation associated to $\mathfrak{p}_i$ and $t_i = |R/\mathfrak{p}_i|$ the cardinality of the residual field $R/\mathfrak{p}_i$. Then α is a PBG of L over K if and only if "β is square free" and $v_i(\beta^{t_i} - \beta) = 1$ for all $i \in \{1, \ldots, s\}$.*

P r o o f. Indeed, the discriminant of P is equal to $\mathrm{Disc}_R(P) = p^p\beta^{(p-1)}R$. As $p \geqslant 3$, then the set $S_P = V(\beta R) \cup (\mathrm{Fib}_R(p) - V(\beta R))$ is the disjoint union. By Lemma 3.4, α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P. Let $\mathfrak{p}$ be a prime in S_P by localization at $\mathfrak{p}$, the ring $R_\mathfrak{p}$ is a discrete valuation ring. We may then apply Proposition 4.2 to $R_\mathfrak{p}$.

It is clear that if $\mathfrak{p}$ in $V(\beta R)$ then $\beta \in \mathfrak{p}$. Then by Proposition 4.2, the ideal $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $v_\mathfrak{p}(\beta) = 1$. Then there are two cases:

(1) If $\mathrm{Fib}_R(p) \subseteq V(\beta R)$ then $S_P = V(\beta R)$. Hence α is a PBG of L over K if and only if, for any prime $\mathfrak{p}$ in $V(\beta R)$, the ideal $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$. Therefore by Proposition 4.2, α is a PBG of L over K if and only if β is square free.

(2) If $\mathrm{Fib}_R(p) \nsubseteq V(\beta R)$ then $S_P = V(\beta R) \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are in $\mathrm{Fib}_R(p) - V(\beta R)$. It is clear that $\mathrm{char}\, R/\mathfrak{p}_i = p$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to p since $pR \subset \mathfrak{p}_i$). According to Proposition 4.2, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $v_i(\beta^{t_i} - \beta) = 1$, where t_i is the cardinality of the residual field $R/\mathfrak{p}_i$. □

R e m a r k 4.2. Note that if $R = \mathbb{Z}$, Theorem 4.3 coincides with the result obtained in [7], Proposition 4.2 and [5], Proposition 5.2).

5. Illustration: Pure nonic field

Using what we have proved in Section 4, we can now give in complete detail an integral basis for certain extensions of degree 9. We first need to compute an integral basis for relative cubic extension by giving the necessary and sufficient conditions, which implies its monogenity.

Theorem 5.1. *Let $K = \mathbb{Q}(\theta)$ be a cubic number field, where $\theta = \sqrt[3]{m}$, m is a cube-free integer not equal to ± 1 and $m \equiv 1 \bmod 3$. Let $\beta = \theta + 1$ and $L = K(\alpha)$ be a cubic extension where α is a root of the monic irreducible polynomial $P = X^3 - \beta \in R[X]$, then α is a PBG of L over $\mathbb{Q}$ if and only if $v_3(m-1) = 1$ and $m+1$ is square free. Furthermore the discriminant of L/K is $d_{L/K} = 27(\theta+1)^2$.*

Proof. From [10], Proposition 6.4.14 and [16] there exists a unique prime ideal $\mathfrak{b}$ in R such that $3\mathfrak{o}_K = \mathfrak{b}^3$. By Lemma 3.5, we have $v_{\mathfrak{b}}(\theta) = 0$ since $3 \nmid m$. Now we claim that $v_{\mathfrak{b}}(\beta) = 0$. So, as $m \equiv 1 \bmod 3$, then $v_{\mathfrak{b}}(m+1) = 0$ and by the formula $(\theta+1)(\theta^2 - \theta + 1) = m + 1$, one checks that $v_{\mathfrak{b}}(\beta) = 0$. Furthermore, $\mathrm{Fib}_K(3) \nsubseteq V(\beta\mathfrak{o}_K)$. Hence, by Theorem 4.3, α is a PBG of L over K if and only if $\nu_{\mathfrak{b}}(\beta^3 - \beta) = 1$ and β is square free. Let us first assume that $\nu_{\mathfrak{b}}(\beta^3 - \beta) = 1$. As $\beta^3 - \beta = \theta(\theta+1)(\theta+2)$, then

$$\nu_{\mathfrak{b}}(\theta) + \nu_{\mathfrak{b}}(\theta+1) + \nu_{\mathfrak{b}}(\theta+2) = 1. \tag{5.1}$$

On the other hand,

$$\nu_{\mathfrak{b}}(\theta-1) + \nu_{\mathfrak{b}}(\theta^2+\theta+1) = \nu_{\mathfrak{b}}(m-1). \tag{5.2}$$

Then, $\nu_{\mathfrak{b}}(\theta-1) = \nu_{\mathfrak{b}}(\theta+2) = 1$ and $\nu_{\mathfrak{b}}(\theta^2+\theta+1) = \nu_{\mathfrak{b}}((\theta-1)^2+3\theta) = 2$ by property of the dominance principle. So, we can deduce that $\nu_{\mathfrak{b}}(m-1) = 3$ which implies $\nu_3(m-1) = 1$. Conversely, if $\nu_3(m-1) = 1$, then $\nu_{\mathfrak{b}}(m-1) = 3$ which gives $\nu_{\mathfrak{b}}(\theta-1) + \nu_{\mathfrak{b}}(\theta^2+\theta+1) = 1$. So, we have 3 cases to study:

- ▷ If $\nu_{\mathfrak{b}}(\theta-1) = 0$, then using the dominance principle, we have $\nu_{\mathfrak{b}}(\theta^2+\theta+1) = \nu_{\mathfrak{b}}((\theta-1)^2+3\theta) = 0$ which is a contradiction.
- ▷ If $\nu_{\mathfrak{b}}(\theta-1) = 3$, then using the dominance principle, we have $\nu_{\mathfrak{b}}(\theta^2+\theta+1) = \nu_{\mathfrak{b}}((\theta-1)^2+3\theta) = 3$ which is a contradiction.
- ▷ If $\nu_{\mathfrak{b}}(\theta-1) = 1$, then using the dominance principle, we have $\nu_{\mathfrak{b}}(\theta^2+\theta+1) = \nu_{\mathfrak{b}}((\theta-1)^2+3\theta) = 2$, hence grouping and using (5.1), we get $\nu_{\mathfrak{b}}(\beta^3-\beta) = 1$.

Secondly, let $\mathfrak{p}$ be a prime ideal in $V(\beta)$. We can see from this that β is square free if and only if $\nu_{\mathfrak{p}}(\beta) = 1$ ($\mathrm{Fib}_K(3) \nsubseteq V(\beta\mathfrak{o}_K)$). Let us write

$$\beta(\beta^2 - 3\beta + 3) = m + 1. \tag{5.3}$$

Then, $\nu_{\mathfrak{p}}(\beta) + \nu_{\mathfrak{p}}(\beta^2 - 3\beta + 3) = \nu_{\mathfrak{p}}(m+1)$. Now, using the dominance principle, $\nu_{\mathfrak{p}}(\beta^2 - 3\beta + 3) = 0$. So, $\nu_{\mathfrak{p}}(\beta) = \nu_{\mathfrak{p}}(m+1)$. Putting all this together we have proved β is square free if and only if $m+1$ is square free, since $\nu_{\mathfrak{p}}(m+1) \geqslant 1$.

That proves the first part of the theorem. For the remainder, we have

$$d_{L/K} = N_{L/K}(P'(\alpha)) = N_{L/K}(3\beta^2) = 27(\theta+1)^2.$$

□

Corollary 5.1. *Under the conditions of Theorem* 5.1, *let* $L = \mathbb{Q}(\alpha, \theta)$ *and write* $m = ab^2$ *with* a *and* b *squarefree and coprime. We set*

$$t = \begin{cases} \dfrac{\theta^2}{b} & \text{if } a^2 \not\equiv b^2 \bmod 9, \\ \dfrac{\theta^2 - a \cdot b^2\theta + b^2}{3b} & \text{if } a^2 \equiv b^2 \bmod 9. \end{cases}$$

Then

$$\mathfrak{B} = \{1, \theta, t, \alpha, \alpha\cdot\theta, \alpha\cdot t, \alpha^2, \alpha^2\cdot\theta, \alpha^2\cdot t\}$$

is an integral basis of L. *Furthermore, the discriminant of* L *is given by*

$$d_{L/\mathbb{Q}} = \begin{cases} -27^4 \cdot (m+1)^2 \cdot a^6 \cdot b^6 & \text{if } a^2 \equiv b^2 \bmod 9, \\ -27^6 \cdot (m+1)^2 \cdot a^6 \cdot b^6 & \text{if } a^2 \not\equiv b^2 \bmod 9. \end{cases}$$

P r o o f. The proof is presented for the first case, the second one is similar. By [10], Theorem 6.4.13, page 346, if $a^2 \not\equiv b^2 \bmod 9$, we have that $\{1, \beta, \beta^2/b\}$ is an integral basis of K over $\mathbb{Q}$ according to Theorem 5.1 and [8], Lemma 2.1. It is easily seen that $\mathfrak{B} = \{1, \theta, t, \alpha, \alpha\cdot\theta, \alpha\cdot t, \alpha^2, \alpha^2\cdot\theta, \alpha^2\cdot t\}$ is an integral basis of L. Indeed, $d_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(d_{L/K}) \cdot (d_{K/\mathbb{Q}})^{[L:K]}$, so

$$d_{L/\mathbb{Q}} = \begin{cases} N_{K/\mathbb{Q}}(27\cdot(\theta+1)^2)\cdot(-3\cdot a^2\cdot b^2)^3 & \text{if } a^2 \equiv b^2 \bmod 9, \\ N_{K/\mathbb{Q}}(27\cdot(\theta+1)^2)\cdot(-27\cdot a^2\cdot b^2)^3 & \text{if } a^2 \not\equiv b^2 \bmod 9. \end{cases}$$

The minimal monic polynomial of $\theta+1$ is given by $T(X) = X^3 - 3X^2 + 3X - (m+1)$, then

$$d_{L/\mathbb{Q}} = \begin{cases} -27^4 \cdot (m+1)^2 \cdot a^6 \cdot b^6 & \text{if } a^2 \equiv b^2 \bmod 9, \\ -27^6 \cdot (m+1)^2 \cdot a^6 \cdot b^6 & \text{if } a^2 \not\equiv b^2 \bmod 9. \end{cases}$$

□

R e m a r k 5.1. Let us keep all the notations of Theorem 5.1. We know that

$$\mathrm{Disc}_R(P) = I_\alpha^2 \cdot d_{L/K},$$

where the first factor is the square of the relative index of α over K, and P the minimal monic polynomial of α. We can check that

$$I_\alpha^2 = \begin{cases} 27^2 \cdot b^6 & \text{if } a^2 \equiv b^2 \bmod 9, \\ b^6 & \text{if } a^2 \not\equiv b^2 \bmod 9. \end{cases}$$

In the first case, one can say that $\theta + 1$ is not a PBG of $L/\mathbb{Q}$ if $a^2 \equiv b^2 \bmod 9$.

References

[1] *M. F. Atiyah, I. G. Macdonald*: Introduction to Commutative Algebra. Addison-Wesley, Massachusetts, 1969. zbl MR doi

[2] *J. W. S. Cassels, A. Fröhlich* (eds.): Algebraic Number Theory. Academic Press, London, 1967. zbl MR

[3] *P. Cassou-Noguès, M. J. Taylor*: A note on elliptic curves and the monogeneity of rings of integers. J. Lond. Math. Soc., II. Ser. *37* (1988), 63–72. zbl MR doi

[4] *P. Cassou-Noguès, M. J. Taylor*: Unités modulaires et monogénéité d'anneaux d'entiers. Séminaire de théorie des nombres, Paris 1986–87. Progress in Mathematics 75. Birkhäuser, Boston, 1988, pp. 35–64. (In French.) zbl MR

[5] *M. E. Charkani, A. Deajim*: Generating a power basis over a Dedekind ring. J. Number Theory *132* (2012), 2267–2276. zbl MR doi

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

[7] *M. E. Charkani, O. Lahlou*: On Dedekind's criterion and monogenicity over Dedekind rings. Int. J. Math. Math. Sci. *2003* (2003), 4455–4464. zbl MR doi

[8] *M. E. Charkani, M. Sahmoudi*: Sextic extension with cubic subfield. JP J. Algebra Number Theory Appl. *34* (2014), 139–150. zbl

[9] *M. E. Charkani, M. Sahmoudi, A. Soullami*: Tower index formula and monogenecity. Commun. Algebra *49* (2021), 2469–2475. zbl MR doi

[10] *H. Cohen*: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138. Springer, Berlin, 1993. zbl MR doi

[11] *R. Dedekind*: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen. Abh. Akad. Wiss. Gött., Math-Phys. Kl., 3. Folge *23* (1878), 3–38. (In German.)

[12] *A. Fröhlich, M. J. Taylor*: Algebraic Number Theory. Cambridge Studies in Advanced Mathematics 27. Cambridge University Press, Cambridge, 1993. zbl MR doi

[13] *I. Gaál, L. Remete*: Power integral bases in cubic and quartic extensions of real quadratic fields. Acta Sci. Math. *85* (2019), 413–429. zbl MR doi

[14] *A. Hameed, T. Nakahara*: Integral bases and relative monogenity of pure octic fields. Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér. *58* (2015), 419–433. zbl MR

[15] *H. Ichimura*: On power integral bases of unramified cyclic extensions of prime degree. J. Algebra *235* (2001), 104–112. zbl MR doi

[16] *G. J. Janusz*: Algebraic Number Fields. Graduate Studies in Mathematics 7. AMS, Providence, 1996. zbl MR doi

[17] *M. Kumar, S. K. Khanduja*: A generalization of Dedekind criterion. Commun. Algebra *35* (2007), 1479–1486. zbl MR doi
[18] *M. J. Lavallee, B. K. Spearman, K. S. Williams*: Lifting monogenic cubic fields to monogenic sextic fields. Kodai Math. J. *34* (2011), 410–425. zbl MR doi
[19] *H. B. Mann*: On integral bases. Proc. Am. Math. Soc. *9* (1958), 167–172. zbl MR doi
[20] *W. Narkiewicz*: Elementary and Analytic Theory of Algebraic Numbers. Springer, Berlin, 1990. zbl MR doi
[21] *J. Neukirch*: Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften 322. Springer, Berlin, 1999. zbl MR doi
[22] *M. Sahmoudi*: Explicit integral basis for a family of sextic field. Gulf J. Math. *4* (2016), 217–222. zbl MR
[23] *M. Sahmoudi, A. Soullami*: On monogenicity of relative cubic-power extensions. Adv. Math., Sci. J. *9* (2020), 6817–6827. doi
[24] *M. Sahmoudi, A. Soullami*: On sextic integral bases using relative quadratic extention. Bol. Soc. Parana. Mat. (3) *38* (2020), 175–180. zbl MR doi
[25] *P. Schmid*: On criteria by Dedekind and Ore for integral ring extensions. Arch. Math. *84* (2005), 304–310. zbl MR doi
[26] *A. Soullami, M. Sahmoudi, O. Boughaleb*: On relative power integral basis of a family of numbers fields. Rocky Mt. J. Math. *51* (2021), 1443–1452. zbl MR doi
[27] *B. K. Spearman, K. S. Williams*: Relative integral bases for quartic fields over quadratic subfields. Acta Math. Hung. *70* (1996), 185–192. zbl MR doi
[28] *B. K. Spearman, K. S. Williams*: A relative integral basis over $\mathbb{Q}(\sqrt{-3})$ for the normal closure of a pure cubic field. Int. J. Math. Math. Sci. *25* (2003), 1623–1626. zbl MR doi
[29] *L. C. Washington*: Relative integral bases. Proc. Am. Math. Soc. *56* (1976), 93–94. zbl MR doi

Authors' addresses: *Mohammed Sahmoudi*, Ibn Tofail University, Laboratory of Engineering Sciences, National School of Applied Sciences, P. B. 242, Av. of the University, Kenitra 14000, Morocco, e-mail: mohammed.sahmoudi@uit.ac.ma; *Mohamed E. Charkani*, Sidi Mohamed Ben Abdellah University, Laboratory of Engineering Sciences, Faculty of Sciences, B. P. 1796, Fez, 30003, Morocco, e-mail: mcharkani@gmail.com.