Bollettino Unione Matematica Italiana

Martine Picavet-L'Hermitte

When is $\mathbb{Z}[\alpha]$ seminormal or t-closed?

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **2-B** (1999), n.1, p. 189–217.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1999_8_2B_1_189_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1999.

Bollettino U. M. I.
(8) 2-B (1999), 189-217

When is $\mathbb{Z}[\alpha]$ Seminormal or t-Closed?

MARTINE PICAVET-L'HERMITTE

Sunto. – *Sia α un intero algebrico con il polinomio minimale $f(X)$. Si danno condizioni necessarie e sufficienti affinché l'anello $\mathbb{Z}[\alpha]$ sia seminormale o t-chiuso per mezzo di $f(X)$. Come applicazione, in particolare, si ottiene che se $f(X) = X^3 + aX + b$, $a, b \in \mathbb{Z}$, le condizioni sono espresse mediante il discriminante de $f(X)$.*

1. – Introduction.

Let α be an algebraic integer. Integral closedness of the ring $\mathbb{Z}[\alpha]$ was the subject of papers by T. Albu [1], G. Maury [5] and K. Uchida [12]. This last author got the following characterization [12, Theorem]:

THEOREM 1.1. – *Let R be a Dedekind domain and α an element of some integral domain which contains R. If α is integral over R, then $R[\alpha]$ is a Dedekind domain if and only if the minimal polynomial $\varphi(X)$ of α is not contained in M^2 for any maximal ideal M of the polynomial ring $R[X]$.*

Our aim is to obtain a similar characterization for seminormality or t-closedness of $\mathbb{Z}[\alpha]$. Recall some definitions:

A ring A is called *seminormal* if, for each $(x, y) \in A^2$ such that $x^3 = y^2$, there exists $a \in A$ such that $x = a^2$, $y = a^3$. When A is a reduced ring, A is seminormal if and only if the natural map $\mathrm{Pic}(A) \to \mathrm{Pic}(A[X])$ is an isomorphism [10].

A ring A is called *t-closed* if, for each $(x, y, r) \in A^3$ such that $x^3 + rxy - y^2 = 0$, there exists $a \in A$ such that $x = a^2 - ra$, $y = a^3 - ra^2$. When A is a one-dimensional Noetherian integral domain, A is t-closed if and only if the natural map $\mathrm{Pic}(A) \to \mathrm{Pic}(A[X, X^{-1}])$ is an isomorphism [7].

In section 2, we begin to recall some results about seminormality and t-closedness gotten in [6], [7], [8], and we study properties of maximal ideals in $\mathbb{Z}[\alpha]$.

In section 3, we give a necessary and sufficient condition for a ring $\mathbb{Z}[\alpha]$ to be seminormal:

Let $f(X)$ be the minimal polynomial of the algebraic integer α. Then any maximal ideal M in $\mathbb{Z}[X]$ containing $f(X)$ is of the form $M = (p, g(X))$ where p is a prime integer and $g(X)$ is a monic polynomial of $\mathbb{Z}[X]$ such that its residue class in $\mathbb{F}_p[X]$ is an irreducible polynomial dividing the residue class of $f(X)$ in $\mathbb{F}_p[X]$. Such a maximal ideal is lying over $p\mathbb{Z}$.

Consider $f(X) = q(X)\, g(X) + c(X)$, the Euclidean division of $f(X)$ by $g(X)$, and then $q(X) = a(X)\, g(X) + b(X)$, the Euclidean division of $q(X)$ by $g(X)$, so that

$$\deg b(X)\,,\ \deg \mathrm{c(X)} < \deg g(X)\,.$$

We can thus write

$$f(X) = a(X)\, g^2(X) + b(X)\, g(X) + c(X)\,.$$

Then, according to Proposition 3.1, $\mathbb{Z}[\alpha]$ is seminormal if and only if for each maximal ideal $M = (p, g(X))$ of $\mathbb{Z}[X]$ such that $f(X) \in M^2$, we have

$$b^2(X) - 4\, a(X)\, c(X) \notin p^2 M\,.$$

Section 4 is devoted to the same problem relating to t-closedness, with a more complex formulation : indeed, we have to distinguish the cases $p = 2$ and $p \neq 2$:

$\mathbb{Z}[\alpha]$ is t-closed if and only if for each maximal ideal $M = (p, g(X))$ of $\mathbb{Z}[X]$ such that $f(X) \in M^2$, we have, with the previous notations:

– if $p \neq 2$, then $[b^2(X) - 4a(X)c(X)]p^{-2}$ is not a quadratic residue mod M.

– if $p = 2$, then $b(X) \notin 4\mathbb{Z}[X]$ and $b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin 4M$ for each $h(X) \in \mathbb{Z}[X]$.

Let R be a Dedekind domain, α be an element of some integral domain which contains R and let α be integral over R. We end both sections 3 and 4 in generalizing seminormality and t-closedness criteria to the ring $R[\alpha]$.

In section 5 we give an application of sections 3 and 4 to simple cubic orders: if α is an algebraic integer with minimal polynomial $f(X) = X^3 + aX + b$, $a, b \in \mathbb{Z}$, let $\Delta = -(4a^3 + 27b^2)$ be the discriminant of $f(X)$. We obtain integral closedness, t-closedness and seminormality criteria for $\mathbb{Z}[\alpha]$; these criteria are related to arithmetical properties of Δ, when Δ is divisible by a prime integer p such that $p \neq 2, 3$ and does not divide both a and b, and to arithmetical properties of $f(a-b)$ or $f'(a-b)$, for the other prime divisors of Δ.

2. – Some generalities.

We first recall some definitions and properties of seminormality and t-closedness.

In the introduction we have just given the definitions of seminormal or t-closed rings. These notions are closely intertwined with seminormal and t-closed morphisms (see [6], [7], [10]).

DEFINITION 2.1. – *An injective ring morphism $A \to B$ is said to be* seminormal (*resp.* t-closed) *if an element b of B is in A whenever b^2, $b^3 \in A$* (*resp. whenever there exists some $r \in A$ such that $b^2 - rb$, $b^3 - rb^2 \in A$*).

PROPOSITION 2.2. – *Let A be an integral domain with integral closure $\overline{A}$. Then, A is seminormal* (*resp. t*-closed) *if and only if $A \to \overline{A}$ is seminormal* (*resp.* t-closure).

PROPOSITION 2.3. – *Let A be an integral domain with integral closure $\overline{A}$. There exist two A-subalgebras ${}^+A$ and ${}^tA$ of $\overline{A}$ such that ${}^+A$ (resp. ${}^tA$) is the smallest seminormal (resp. t-closed) A-subalgebra of $\overline{A}$; the ring ${}^+A$ (resp. ${}^tA$) is called the* seminormalization (*resp.* t-closure) *of A.*

We have the inclusion: ${}^+A \subset {}^tA$; furthermore, A is seminormal (resp. t-closed) if and only if $A = {}^+A$ (resp. $A = {}^tA$). The composite $A \to {}^+A \to {}^tA \to \overline{A}$ is called the *canonical decomposition* of $A \to \overline{A}$.

D. Ferrand and J. P. Olivier introduced in [4] the notion of minimal morphism and showed there exist three classes of minimal morphisms:

DEFINITION 2.4 [4, Définition 1.1, Proposition 4.1 and Lemme 1.2].

(1) *A ring morphism f is said to be* minimal *if*

(*a*) *f is injective and non bijective*

(*b*) *for every decomposition $f = g \circ h$ where g and h are injective ring morphisms, g or h is an isomorphism.*

(2) *Let f: $A \to B$ be a finite minimal morphism between two one-dimensional Noetherian domains with the same quotient field. Then the conductor of f is a maximal ideal P of A. Moreover, f satisfies one of the following conditions*:

(*a*) *there exists $x \in B \backslash A$ such that x^2, $x^3 \in A$ and $x^2 \in P$: we say that f is* ramified.

(*b*) *there exists $x \in B \backslash A$ such that $x^2 - x$, $x^3 - x^2 \in A$ and $x^2 - x \in P$: we say that f is* decomposed.

(*c*) *P is a maximal ideal in B and $A/P \to B/P$ is a minimal field extension: we say that f is* inert.

Then, we showed in [8] the following result:

PROPOSITION 2.5 [8, Theorem 3.4]. – *Let A be a one-dimensional Noetherian domain such that $\overline{A}$ is finite over A. Then: $A \to {}^+A$ (resp. ${}^+A \to {}^tA$, ${}^tA \to \overline{A}$) is a composite of finitely many ramified (resp. decomposed, inert) morphisms, and is not factorized by another type of minimal morphism in any decomposition into minimal morphism.*

In particular, we have $A \neq \overline{A}$ if and only if there exist some maximal ideal P in A and an element $x \in \overline{A} \setminus A$ such that $xP \subset P$.

For a Dedekind domain R (in particular if $R = \mathbb{Z}$) and an element α of some integral domain which contains R such that α is integral over R, the ring $R[\alpha]$ satisfies the assumptions of 2.5.

Next we give some results on maximal ideals in $\mathbb{Z}[\alpha]$ needed in the following.

Let α be an algebraic integer with minimal polynomial $f(X)$. Any element z of $\mathbb{Z}[\alpha]$ can be written $a(\alpha)$, where $a(X)$ is a unique polynomial in $\mathbb{Z}[X]$, such that $\deg a(X) < \deg f(X)$.

Let p be a prime integer. For a polynomial $a(X) = \sum a_i X^i \in \mathbb{Z}[X]$, we denote by $\overline{a}(X)$ the polynomial $\sum \overline{a}_i X^i \in \mathbb{F}_p[X]$, where $\overline{a}_i$ is the p-residue of a_i in $\mathbb{F}_p$.

For a given prime integer p, let $\bar{f}(X) = \prod \bar{f}_i(X)^{e_i}$ be the decomposition of $\bar{f}(X)$ into irreducible distinct polynomials $\bar{f}_i(X)$, where $f_i(X)$ is a monic polynomial and $e_i \in \mathbb{N}^*$. In particular, $f_i(X)$ and $\bar{f}_i(X)$ have the same degree.

Now we give a key lemma. As far as we know, this is a new result which looks like the results of T. Albu, G. Maury and K. Uchida (cf. 1.1). Unlike their results, we do not need any hypothesis on the ring $\mathbb{Z}[\alpha]$.

LEMMA 2.6. – *Let p be a prime integer and $M = (p, f(X))$ be an ideal of $\mathbb{Z}[X]$ such that $f(X)$ is a monic polynomial. Then p is not in M^2.*

PROOF. – We have $M^2 = (p^2, pf(X), f^2(X))$. Assume $p \in M^2$. Hence, there exist $a(X)$, $b(X)$, $c(X) \in \mathbb{Z}[X]$ such that $p = p^2 a(X) + pf(X)\, b(X) + f^2(X)\, c(X)$. As $f(X)$ is a monic polynomial, there exists α a zero of $f(X)$ in the integral closure A of some finite algebraic extension of $\mathbb{Q}$. Then we get $p = p^2 a(\alpha)$; as $p \neq 0$, we have $pa(\alpha) = 1$; thus p is a unit of A, which leads to a contradiction since there are maximal ideals in A lying over $p\mathbb{Z}$: indeed, A is integral over $\mathbb{Z}$. Therefore, we get $p \notin M^2$.

PROPOSITION 2.7. – *Let α be an algebraic integer with minimal polynomial $f(X)$. For a given prime integer p, let $\bar{f}(X) = \prod_{i=1}^{n} \bar{f}_i(X)^{e_i}$ be the decomposition of $\bar{f}(X)$ into irreducible distinct polynomials, where $f_i(X)$ is monic and $e_i \in \mathbb{N}^*$. The maximal ideals of $\mathbb{Z}[\alpha]$ lying over $p\mathbb{Z}$ are $(p, f_i(\alpha))$, for $i = 1, \ldots, n$, and $p\mathbb{Z}[\alpha]$ if $\bar{f}(X)$ is irreducible in $\mathbb{F}_p[X]$.*

PROOF. – We know that the maximal ideals of $\mathbb{Z}[\alpha]$ arise from maximal ideals of $\mathbb{Z}[X]$ containing $f(X)$, due to the isomorphism $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(f(X))$. Because $f(X)$ is a monic polynomial, a maximal ideal M' of $\mathbb{Z}[X]$ containing $f(X)$ and a prime integer p can be written $M' = (p, g(X))$, where $g(X)$ is a monic polynomial such that $\bar{g}(X)$ is irreducible in $\mathbb{F}_p[X]$. Thus $f(X) = pa(X) + g(X)\, b(X)$, where $a(X), b(X) \in \mathbb{Z}[X]$, implies $\bar{f}(X) = \bar{g}(X)\bar{b}(X)$ in $\mathbb{F}_p[X]$. Therefore $\bar{g}(X)$ is a monic irreducible polynomial dividing $\bar{f}(X)$, so that $\bar{g}(X) = \bar{f}_i(X)$, for some i. Hence $M' = (p, f_i(X))$ shows that $P_i = (p, f_i(\alpha))$ is a maximal ideal in $\mathbb{Z}[\alpha]$.

If $\bar{f}(X)$ is irreducible in $\mathbb{F}_p[X]$, we get $\bar{f}(X) = \bar{f}_i(X)$, whence $f(X) = f_i(X)$ and $f_i(\alpha) = 0$.

DEFINITIONS 2.8. – *From now, we denote by $M_i = (p, f_i(X))$ (resp. $P_i = (p, f_i(\alpha))$) the maximal ideals in $\mathbb{Z}[X]$ containing $f(X)$ (resp. in $\mathbb{Z}[\alpha]$).*

LEMMA 2.9. – *Let $P_i = (p, f_i(\alpha))$ be a maximal ideal in $\mathbb{Z}[\alpha]$, with $f_i(\alpha) \neq 0$.*

(1) *For $g(\alpha) \in \mathbb{Z}[\alpha]$, we get $g(\alpha) \in P_i$ if and only if $\bar{g}(X) \in (\bar{f}_i(X))$ in $\mathbb{F}_p[X]$.*

(2) *Any element $g(\alpha) \in P_i$ can be written: $g(\alpha) = a(\alpha) f_i(\alpha) + pb(\alpha)$, where $a(X), b(X) \in \mathbb{Z}[X]$, and $\deg b(X) < \deg f_i(X)$.*

(3) *If $g(\alpha) \in P_i$ and $\deg g(X) < \deg f_i(X)$, then $a(\alpha) = 0$ and $g(\alpha) \in p\mathbb{Z}[\alpha]$.*

PROOF. – First we show (1). Let $g(\alpha) \in \mathbb{Z}[\alpha]$. Then we have $g(\alpha) \in P_i$ if and only if there exist $a(\alpha), b(\alpha) \in \mathbb{Z}[\alpha]$ such that $g(\alpha) = a(\alpha) f_i(\alpha) + pb(\alpha)$, that is to say $g(X) - a(X) f_i(X) - pb(X) = f(X)\, c(X)$, with $c(X) \in \mathbb{Z}[X]$, from which it follows that $\bar{g}(X) = \bar{a}(X)\bar{f}_i(X) + \bar{f}(X)\bar{c}(X)$ in $\mathbb{F}_p[X]$. Since $\bar{f}(X)$ is divided by $\bar{f}_i(X)$, so is $\bar{g}(X)$.

Conversely, if $\bar{g}(X) \in (\bar{f}_i(X))$, we can write $\bar{g}(X) = \bar{a}(X)\bar{f}_i(X)$ in $\mathbb{F}_p[X]$. So, there is $b(X) \in \mathbb{Z}[X]$ such that $g(X) = a(X) f_i(X) + pb(X)$, whence $g(\alpha) = a(\alpha) f_i(\alpha) + pb(\alpha) \in P_i$.

(2) For $g(\alpha) \in \mathbb{Z}[\alpha]$, let $g(X) = a(X) f_i(X) + a'(X)$ be the Euclidean division of $g(X)$ by $f_i(X)$, with $\deg a'(X) < \deg f_i(X)$. This equality leads to $g(\alpha) = a(\alpha) f_i(\alpha) + a'(\alpha)$. Thus $g(\alpha) \in P_i \Leftrightarrow a'(\alpha) \in P_i \Leftrightarrow \bar{a}'(X) \in (\bar{f}_i(X))$ by (1). But, $\deg \bar{a}'(X) \leqslant \deg a'(X) < \deg f_i(X) = \deg \bar{f}_i(X)$ implies $\bar{a}'(X) = \bar{0}$ and $a'(X) =$

$pb(X)$ in $\mathbb{Z}[X]$, with $\deg b(X) = \deg a'(X) < \deg f_i(X)$. Then, $g(\alpha) = a(\alpha) f_i(\alpha) + pb(\alpha)$, with $\deg b(X) < \deg f_i(X)$.

(3) If $\deg g(X) < \deg f_i(X)$, the Euclidean division of $g(X)$ by $f_i(X)$ gives $g(X) = 0\, f_i(X) + g(X)$. With the notations of (2), we get then $a(X) = 0$, $g(X) = pb(X)$, so that $a(\alpha) = 0$ and $g(\alpha) = pb(\alpha) \in p\mathbb{Z}[\alpha]$.

Assume that the polynomial $\bar{f}(X)$ is not irreducible in $\mathbb{F}_p[X]$ for a prime $p \in \mathbb{Z}$. Let $\bar{f}_i(X)$ be an irreducible monic divisor of $\bar{f}(X)$ in $\mathbb{F}_p[X]$. If $f_i(X)$ is a monic polynomial in $\mathbb{Z}[X]$ with residue $\bar{f}_i(X)$ in $\mathbb{F}_p[X]$, consider $f(X) = q(X) f_i(X) + c(X)$ the Euclidean division of $f(X)$ by $f_i(X)$, and $q(X) = a(X) f_i(X) + b(X)$ the Euclidean division of $q(X)$ by $f_i(X)$. Thus we obtain unique polynomials $a(X)$, $b(X)$, $c(X) \in \mathbb{Z}[X]$ such that:

$$(*) \qquad f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

where $\deg b(X)$, $\deg c(X) < \deg f_i(X)$.

DEFINITION 2.10. – *Under the above conditions, we say that*

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X), \quad \textit{where} \quad \deg b(X),\ \deg c(X) < \deg f_i(X)$$

is the double *Euclidean division of* $f(X)$ by $f_i(X)$.

In $\mathbb{F}_p[X]$ we get $\bar{f}(X) = \bar{a}(X) \bar{f}_i^2(X) + \bar{b}(X)\, \bar{f}_i(X) + \bar{c}(X)$. Since $\bar{f}_i(X)$ divides $\bar{f}(X)$, it divides also $\bar{c}(X)$; inequalities between degrees give then

$$\deg \bar{c}(X) \leqslant \deg c(X) < \deg f_i(X) = \deg \bar{f}_i(X).$$

So $\bar{c}(X) = \bar{0}$ and $c(X) \in p\mathbb{Z}[X]$.

Relation $(*)$ implies the relation in $\mathbb{Z}[\alpha]$:

$$(**) \qquad a(\alpha) f_i^2(\alpha) + b(\alpha) f_i(\alpha) + c(\alpha) = 0.$$

In the next two sections, we are looking for seminormality or t-closedness criteria of $\mathbb{Z}[\alpha]$. The next result will be useful in these two sections:

PROPOSITION 2.11. – *Let $P_i = (p,\ f_i(\alpha))$ be a maximal ideal of $\mathbb{Z}[\alpha]$. There exists $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ such that $xP_i \subset P_i$ if and only if $\bar{f}_i^2(X)$ divides $\bar{f}(X)$ in $\mathbb{F}_p[X]$ and $p \notin P_i^2$.*

Under these conditions and with notation 2.10, *we have $b(X) \in p\mathbb{Z}[X]$, $c(X) \in p^2\mathbb{Z}[X]$ and $f(X) \in (p,\ f_i(X))^2$.*

PROOF. – As we have $P_i = (p,\ f_i(\alpha))$, the condition $xP_i \subset P_i$ is equivalent to px, $xf_i(\alpha) \in P_i$. Thus we can write $x = [ph(\alpha) + f_i(\alpha)\, k_1(\alpha)]p^{-1}$, where $h(X)$, $k_1(X) \in \mathbb{Z}[X]$.

We get $f_i(\alpha)\,k_1(\alpha)\,p^{-1} \notin \mathbb{Z}[\alpha]$ due to $x \notin \mathbb{Z}[\alpha]$, so that $f_i(\alpha)\,k_1(\alpha) \notin p\mathbb{Z}[\alpha]$. Furthermore, the condition $f_i(\alpha)\,x \in P_i$ gives $h(\alpha)\,f_i(\alpha) + f_i^2(\alpha)\,k_1(\alpha)\,p^{-1} \in P_i$, which is equivalent to $f_i^2(\alpha)\,k_1(\alpha) \in pP_i$. But this last condition is satisfied if and only if there exist $g_1(X)$, $h_1(X)$, $k(X) \in \mathbb{Z}[X]$ such that

$$f_i^2(X)\,k_1(X) = p^2 g_1(X) + pf_i(X)\,h_1(X) + k(X)\,f(X),$$

which gives $\bar{f}_i^2(X)\bar{k}_1(X) = \bar{k}(X)\bar{f}(X)$ in $\mathbb{F}_p[X]$. If $\bar{f}_i(X)$ divides $\bar{k}(X)$, we obtain $\bar{f}_i(X)\bar{k}_1(X) = \bar{k}_2(X)\bar{f}(X)$, with $\bar{k}_2(X) \in \mathbb{F}_p[X]$ and then we have $f_i(X)\,k_1(X) = k_2(X)\,f(X) + pk_3(X)$ in $\mathbb{Z}[X]$; so, $f_i(\alpha)\,k_1(\alpha) = pk_3(\alpha) \in p\mathbb{Z}[\alpha]$, a contradiction. Then, $\bar{f}_i(X)$ and $\bar{k}(X)$ are coprime and $\bar{f}_i^2(X)$ divides $\bar{f}(X)$. By ($*$), we get that $\bar{f}_i(X)$ divides $\bar{b}(X)$ in $\mathbb{F}_p[X]$; it follows from $\deg \bar{b}(X) < \deg \bar{f}_i(X)$ that $\bar{b}(X) = \bar{0}$, whence $b(X) \in p\mathbb{Z}[X]$. As $k(X)\,f(X) \in (p,\ f_i(X))^2$ and $k(X)$ does not belong to the maximal ideal $(p,\ f_i(X))$, we obtain in addition that $f(X)$ belongs to the primary ideal $(p,\ f_i(X))^2$.

But, we can write $c(X) = pc_2(X) = f(X) - a(X)\,f_i^2(X) - b(X)\,f_i(X)$ which implies $pc_2(X) \in (p,\ f_i(X))^2$, with $p \notin (p,\ f_i(X))^2$ by 2.6; for the same reason, we get $c_2(X) \in (p,\ f_i(X))$, and $c_2(X) \in p\mathbb{Z}[X]$, $c(X) \in p^2\mathbb{Z}[X]$, since $\deg c_2(X) = \deg c(X) < \deg f_i(X)$.

If $p \in P_i^2$, we get that $p = p^2 a'(X) + pf_i(X)\,b'(X) + f_i^2(X)\,c'(X) + f(X)\,d'(X)$ where $a'(X)$, $b'(X)$, $c'(X)$, $d'(X) \in \mathbb{Z}[X]$; as $f(X) \in (p,\ f_i(X))^2$, we should have $p \in (p,\ f_i(X))^2$, in contradiction with 2.6. Thus we get $p \notin P_i^2$.

Conversely, assume $\bar{f}_i(X)^2$ divides $\bar{f}(X)$ in $\mathbb{F}_p[X]$ and $p \notin P_i^2$. Then we have $x = f_i(\alpha)\,a(\alpha)\,p^{-1} \notin \mathbb{Z}[\alpha]$ (if not, we get $\bar{f}_i(X)\bar{a}(X) \in (\bar{f}(X))$ in $\mathbb{F}_p[X]$). Obviously, we have $px \in P_i$, as well as $f_i(\alpha)\,x$, since $f_i(\alpha)\,x = a(\alpha)\,f_i^2(\alpha)\,p^{-1} = -[b(\alpha)\,f_i(\alpha) + c(\alpha)]\,p^{-1}$ by ($**$): indeed, we have just seen that $b(X) \in p\mathbb{Z}[X]$ since $\bar{f}_i^2(X)$ divides $\bar{f}(X)$ and $c_2(\alpha) \in P_i$ since $c(\alpha) = pc_2(\alpha) = -a(\alpha)\,f_i^2(\alpha) - b(\alpha)\,f_i(\alpha) \in P_i^2$, with $p \notin P_i^2$.

REMARKS 2.12.

(1) From $xP_i \subset P_i$ where $P_i = (p,\ f_i(\alpha))$, we deduce the system:

$$\begin{cases} [A(\alpha) - x]\,p + B(\alpha)\,f_i(\alpha) = 0\,, \\ C(\alpha)p + [D(\alpha) - x]\,f_i(\alpha) = 0\,, \end{cases}$$

where $A(\alpha)$, $B(\alpha)$, $C(\alpha)$, $D(\alpha) \in \mathbb{Z}[\alpha]$.

It follows that $x^2 - [A(\alpha) + D(\alpha)]x + [A(\alpha)\,D(\alpha) - B(\alpha)\,C(\alpha)] = 0$; hence x satisfies a quadratic relation over $\mathbb{Z}[\alpha]$ and is integral over $\mathbb{Z}[\alpha]$.

(2) Under assumptions of 2.11, we can henceforth put $b(X) = pb_1(X)$ and $c(X) = p^2 c_1(X)$, with $b_1(X)$, $c_1(X) \in \mathbb{Z}[X]$. Then 2.10 gives:

$$(***) \qquad a(\alpha)\,f_i^2(\alpha) = -pb_1(\alpha)\,f_i(\alpha) - p^2 c_1(\alpha) \in pP_i$$

PROPOSITION 2.13. – *Let α be an algebraic integer with minimal polynomial $f(X)$; the following conditions are equivalent:*

(1) *$\mathbb{Z}[\alpha]$ is not integrally closed.*

(2) *There is a maximal ideal $(p, f_i(X))$ in $\mathbb{Z}[X]$ such that $f(X) \in (p, f_i(X))^2$.*

(3) *There exist a prime integer p and an irreducible monic polynomial $f_i(X) \in \mathbb{Z}[X]$ such that $\bar{f}_i^2(X)$ divides $\bar{f}(X)$ and $p \notin (p, f_i(\alpha))^2$.*

Furthermore, if one of these equivalent conditions holds, $f(X)$ belongs to the square of a maximal ideal $(p, f_i(X))$ in $\mathbb{Z}[X]$ if and only if $\bar{f}_i^2(X)$ divides $\bar{f}(X)$ and $p \notin ((p, f_i(\alpha))^2$.

PROOF. – $(1) \Leftrightarrow (2)$ is 1.1. We have $(1) \Rightarrow (3)$ by 2.11 (we cannot have $P_i = p\mathbb{Z}[\alpha]$ since $x \notin \mathbb{Z}[\alpha]$). Conversely, by 2.11, (3) yields $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ such that $xP_i \subset P_i$, for a maximal ideal P_i of $\mathbb{Z}[\alpha]$. Now 2.12 (1) shows that x is integral over $\mathbb{Z}[\alpha]$, so that $\mathbb{Z}[\alpha]$ is not integrally closed.

When $\mathbb{Z}[\alpha]$ is not integrally closed, there are maximal ideals $(p, f_i(X))$ in $\mathbb{Z}[X]$ such that $f(X) \in (p, f_i(X))^2$ (see 1.1). We can ask what is the link between α and the prime integers p. The answer is given by the following proposition:

PROPOSITION 2.14. – *Let α be an algebraic integer with minimal polynomial $f(X)$ such that $\mathbb{Z}[\alpha]$ is not integrally closed. Let $n\mathbb{Z}$ be the annihilator of the $\mathbb{Z}$-module $\overline{\mathbb{Z}[\alpha]}/\mathbb{Z}[\alpha]$, where $\overline{\mathbb{Z}[\alpha]}$ is the integral closure of $\mathbb{Z}[\alpha]$. If $(p, f_i(X))$ is a maximal ideal of $\mathbb{Z}[X]$, then $f(X) \in (p, f_i(X))^2$ if and only if p divides n and $\bar{f}_i(X)$ is a monic irreducible divisor of $\bar{f}(X)$ in $\mathbb{F}_p[X]$.*

PROOF. – Let $n\mathbb{Z}$ be the conductor in $\mathbb{Z}$ of $\mathbb{Z}[\alpha] \to \overline{\mathbb{Z}[\alpha]}$. For a prime integer p, set $S = \mathbb{Z} \setminus p\mathbb{Z}$. Obviously $\mathbb{Z}[\alpha]_S \to \overline{\mathbb{Z}[\alpha]}_S$ is an isomorphism if and only if $n \notin p\mathbb{Z}$. Then $\mathbb{Z}[\alpha]_S$ is integrally closed if and only if $n \notin p\mathbb{Z}$. But we have $\mathbb{Z}[\alpha]_S = \mathbb{Z}_S[\alpha]$ and $f(X) \in \mathbb{Z}_S[X]$ is still the minimal polynomial of α. Since $\mathbb{Z}_S$ is a Dedekind domain, $\mathbb{Z}_S[\alpha]$ is integrally closed if and only if $f(X)$ is not contained in the square of any maximal ideal of $\mathbb{Z}_S[X]$ by 1.1. But the maximal ideals of $\mathbb{Z}_S[X]$ containing $f(X)$ are of the form $(p, f_i(X))$, where $\bar{f}_i(X)$ is an irreducible factor of $\bar{f}(X)$ in $\mathbb{F}_p[X]$.

To sum up, the following statements are equivalent:

- p divides n,
- $\mathbb{Z}_S[\alpha]$ is not integrally closed,
- $f(X) \in (p, f_i(X))^2 \mathbb{Z}_S[X]$ for some $f_i(X)$ in $\mathbb{Z}_S[X]$.

This last condition is equivalent to the following:

- $f(X) \in (p, f_i(X))^2 \mathbb{Z}[X]$ for some $f_i(X)$ in $\mathbb{Z}[X]$.

One implication is obvious. Conversely, assume that $f(X) \in (p, f_i(X))^2 \mathbb{Z}_S[X]$, where $f_i(X) \in \mathbb{Z}_S[X]$. As $\mathbb{F}_p$ is the residue class field of $\mathbb{Z}$ and $\mathbb{Z}_S$, there exists $f_i'(X) \in \mathbb{Z}[X]$ such that $f_i(X) - f_i'(X) \in p\mathbb{Z}_S[X]$ so that we can choose $f_i(X) \in \mathbb{Z}[X]$. Since $f(X) \in (p, f_i(X))^2 \mathbb{Z}_S[X]$, we can write in a unique way : $f(X) = a(X) f_i^2(X) + pb(X) f_i(X) + p^2 c(X)$, with $a(X)$, $b(X)$, $c(X) \in \mathbb{Z}_S[X]$ and $\deg b(X)$, $\deg c(X) < \deg f_i(X)$. But, as $f(X)$ and $f_i(X) \in \mathbb{Z}[X]$, we can also consider the double Euclidean division of $f(X)$ by $f_i(X)$ in $\mathbb{Z}[X]$. We have then, in a unique way:

$$f(X) = a'(X) f_i^2(X) + b'(X) f_i(X) + c'(X),$$

with $a'(X)$, $b'(X)$, $c'(X) \in \mathbb{Z}[X]$ and $\deg b'(X)$, $\deg c'(X) < \deg f_i(X)$. By unicity of the division in $\mathbb{Z}_S[X]$ we have:

$$a(X) = a'(X), \quad b'(X) = pb(X) \in p\mathbb{Z}_S[X] \cap \mathbb{Z}[X].$$

If $b'(X) = \sum_{j=1}^{m} b_j' X^j$ and $b(X) = \sum_{j=1}^{m} b_j s_j^{-1} X^j$, with b_j, $b_j' \in \mathbb{Z}$ and $s_j \in S$, then $s_j b_j' = pb_j$ for each j yield $b_j' \in p\mathbb{Z}$, since $s_j \notin p\mathbb{Z}$. So $b'(X) \in p\mathbb{Z}[X]$. In the same way, we get $c'(X) = p^2 c(X) \in p^2 \mathbb{Z}_S[X] \cap \mathbb{Z}[X] = p^2 \mathbb{Z}[X]$. Thus we have $f(X) \in (p, f_i(X))^2 \mathbb{Z}[X]$ with $f_i(X) \in \mathbb{Z}[X]$.

REMARK. – We can find prime integers p such that $\mathbb{Z}_S[\alpha]$ is not integrally closed in another way : let d be the discriminant of $f(X)$; if $f(X) \in (p, f_i(X))^2$, then p divides d. So, we have only to consider the prime divisors of d.

Let R be a Dedekind domain. The double Euclidean division obtained in 2.10 is still valid for a Dedekind domain. For each maximal ideal P in R, the ring R_P is a principal domain. Let α be an element of some integral domain which contains R and such that α is integral over R and let $f(X) \in R[X]$ be the minimal polynomial of α. Then α is also integral over R_P and $f(X)$ is still its minimal polynomial in $R_P[X]$. Moreover, for a maximal ideal P in R, we can identify R/P and R_P/PR_P. So, let $f_i(X)$ be a monic polynomial in $R[X]$ such that $\bar{f}_i(X)$ is a monic irreducible divisor of $\bar{f}(X)$ in $R/P[X]$; we get then that $f_i(X)$ is also a monic polynomial in $R_P[X]$ such that $\bar{f}_i(X)$ is a monic irreducible divisor of $\bar{f}(X)$ in $R_P/PR_P[X]$. Hence it follows that the double Euclidean division of $f(X)$ by $f_i(X)$ in $R[X]$ given in 2.10 is still the double Euclidean division of $f(X)$ by $f_i(X)$ in $R_P[X]$ and, for $f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$ with $a(X)$, $b(X)$, $c(X) \in R[X]$, we also have $a(X)$, $b(X)$, $c(X) \in R_P[X]$.

Now, if P is a maximal ideal in R, there exists $p \in P$ such that $PR_P = pR_P$, where p is an irreducible element in R_P. A maximal ideal in $R[X]$ containing $f(X)$ is of the form $(P, f_i(X))$ [12, Lemma] so that $(p, f_i(X))$ is a maximal ideal in $R_P[X]$ containing $f(X)$. Conversely, a maximal ideal in $R_P[X]$ containing $f(X)$ is of the form $(p, f_i(X))$ and comes from a maximal ideal $(P, f_i(X))$ in $R[X]$. So we get:

LEMMA 2.15. – *Let R be a Dedekind domain and P be a maximal ideal in R such that $PR_P = pR_P$, with $p \in P$. For any monic polynomial $f(X) \in R[X]$ such that $(P, f(X))$ is a maximal ideal in $R[X]$, we have $(P, f(X)) = (p, f(X)) \cap R[X]$ (resp. $(P, f(X))^2 = (p, f(X))^2 \cap R[X]$), where $(p, f(X))$ is a maximal ideal in $R_P[X]$.*

PROOF. – We have obviously $(P, f(X)) \subset (p, f(X)) \cap R[X]$.

Let $g(X) \in (p, f(X)) \cap R[X]$. The Euclidean division of $g(X)$ by $f(X)$ in $R[X]$ gives $g(X) = a(X)f(X) + b(X)$, with $\deg b(X) < \deg f(X)$ and $a(X), b(X) \in R[X]$. We get then $b(X) \in pR_P[X] \cap R[X] = PR[X]$. Thanks to $p^2 R_P[X] \cap R[X] = P^2 R[X]$ we obtain the second equality by considering the double Euclidean division of a polynomial by $f(X)$.

To close the section, we have the following result:

PROPOSITION 2.16. – *Let R be a Dedekind domain and α be an element of some integral domain which contains R where α is integral over R. Then $R[\alpha]$ is seminormal (resp. t-closed) if and only if $R_P[\alpha]$ is seminormal (resp. t-closed) for each maximal ideal P in R.*

PROOF. – Consider a maximal ideal P in R. We have obviously $R_P[\alpha] = (R[\alpha])_P$. If $R[\alpha]$ is seminormal or t-closed, so is $R_P[\alpha]$ [10, Proposition 3.7] and [7, Proposition 1.15].

Conversely, as $R[\alpha]$ is an R-module, we have $R[\alpha] = \bigcap_{P \in \operatorname{Max} R} (R[\alpha])_P = \bigcap_{P \in \operatorname{Max} R} (R_P[\alpha])$. Then, if $R_P[\alpha]$ is seminormal (resp. t-closed) for each maximal ideal P in R, so is $R[\alpha]$ by [10, Corollary 3.2] and [7, Proposition 1.14].

3. – When is $\mathbb{Z}[\alpha]$ seminormal?

In view of 2.4 and 2.5, a nonseminormality condition for $\mathbb{Z}[\alpha]$ is the following : there is some $x \in \mathbb{Q}[\alpha] \backslash \mathbb{Z}[\alpha]$ such that $x^2, x^3 \in \mathbb{Z}[\alpha]$ and $xM \subset M$, for a maximal ideal M of $\mathbb{Z}[\alpha]$: indeed, $\mathbb{Z}[\alpha]$ is not seminormal if and only if $\mathbb{Z}[\alpha] \neq {}^+\mathbb{Z}[\alpha]$, or equivalently, if and only if there exists a subring B of the integral closure of $\mathbb{Z}[\alpha]$ such that $\mathbb{Z}[\alpha] \to B$ is a ramified morphism.

PROPOSITION 3.1. – *Let α be an algebraic integer with minimal polynomial $f(X)$.*

For each maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$, let

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$.

Then, $\mathbb{Z}[\alpha]$ is not seminormal if and only if there exists a maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$ such that $f(X) \in M_i^2$ and

$$b^2(X) - 4a(X)c(X) \in p^2 M_i .$$

PROOF. – As we have just seen, $\mathbb{Z}[\alpha]$ is not seminormal if and only if there exists $x \in \mathbb{Q}[\alpha] \backslash \mathbb{Z}[\alpha]$ such that $x^2, x^3 \in \mathbb{Z}[\alpha]$ and $xP_i \subset P_i$, for a maximal ideal P_i in $\mathbb{Z}[\alpha]$. Such an ideal P_i is the conductor of $\mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha, x]$ where $\mathbb{Z}[\alpha, x]$ is a $\mathbb{Z}[\alpha]$-module generated by 1 and x. Thus, $\mathbb{Z}[\alpha]$ is not seminormal if and only if there exists $x \in \mathbb{Q}[\alpha] \backslash \mathbb{Z}[\alpha]$ such that $x^2 \in P_i$ and $xP_i \subset P_i$, for a maximal ideal P_i of $\mathbb{Z}[\alpha]$. The condition $xP_i \subset P_i$ is characterized in 2.11, and we have $x = [ph(\alpha) + f_i(\alpha)\, k_1(\alpha)]p^{-1}$, under the notations of 2.11; furthermore, we got in the proof of 2.11 that $\bar{f}_i^2(X)\,\bar{k}_1(X) = \bar{f}(X)\,\bar{k}(X)$, where $\bar{k}(X)$ and $\bar{f}_i(X)$ are coprime; then we have $\bar{k}_1(X) = \bar{k}(X)\,\bar{a}(X)$ by $(*)$. We can now write, with new notations: $x = [ph(\alpha) + f_i(\alpha)\, k(\alpha)\, a(\alpha)]p^{-1}$, where $\bar{k}(X)$ and $\bar{f}_i(X)$ are coprime in $\mathbb{F}_p[X]$.

Now consider condition (i): $x^2 \in P_i$. The following statements are equivalent to (i):

(ii) $p^2 h^2(\alpha) + 2pf_i(\alpha)\, h(\alpha)\, k(\alpha)\, a(\alpha) + f_i^2(\alpha)\, k^2(\alpha)\, a^2(\alpha) \in p^2 P_i$;

(iii) $ph^2(\alpha) + 2f_i(\alpha)\, h(\alpha)\, k(\alpha)\, a(\alpha) - k^2(\alpha) a(\alpha)[f_i(\alpha)\, b_1(\alpha) + pc_1(\alpha)] \in pP_i$;

(iv) $ph^2(X) + 2f_i(X)\, h(X)\, k(X)\, a(X) - k^2(X)\, a(X)[f_i(X)\, b_1(X) + pc_1(X)] = p^2 r(X) + pf_i(X)\, s(X) + t(X)[a(X)\, f_i^2(X) + pb_1(X)\, f_i(X) + p^2 c_1(X)]$, where $r(X), s(X), t(X) \in \mathbb{Z}[X]$.

Now, (iv) implies: $\bar{f}_i(X)\,\bar{k}(X)\,\bar{a}(X)[\bar{2}\,\bar{h}(X) - \bar{k}(X)\,\bar{b}_1(X)] = \bar{t}(X)\,\bar{a}(X)\,\bar{f}_i^2(X)$ in $\mathbb{F}_p[X]$, which is equivalent to: $\bar{k}(X)[\bar{2}\,\bar{h}(X) - \bar{k}(X)\,\bar{b}_1(X)] = \bar{t}(X)\,\bar{f}_i(X)$. As $\bar{k}(X)$ and $\bar{f}_i(X)$ are coprime, $\bar{f}_i(X)$ divides $\bar{2}\,\bar{h}(X) - \bar{k}(X)\,\bar{b}_1(X)$ whence $2h(\alpha) - k(\alpha)\, b_1(\alpha) \in P_i$. Since $f_i^2(\alpha)\, a(\alpha) \in pP_i$, we have $a(\alpha) f_i(\alpha)\, P_i \subset pP_i$ (indeed, $pa(\alpha) f_i(\alpha) \in pP_i$ and $a(\alpha) f_i^2(\alpha) \in pP_i$). So, condition $2h(\alpha) - k(\alpha)\, b_1(\alpha) \in P_i$ implies that (i) is equivalent to: $ph^2(\alpha) - pk^2(\alpha)\, a(\alpha)\, c_1(\alpha) \in pP_i$, from which it follows that $h^2(\alpha) - k^2(\alpha)\, a(\alpha)\, c_1(\alpha) \in P_i$; this last condition is equivalent to $\bar{f}_i(X)$ divides $\bar{h}^2(X) - \bar{k}^2(X)\,\bar{a}(X)\,\bar{c}_1(X)$ in $\mathbb{F}_p[X]$. Thus we get from (i) the two conditions: $\bar{f}_i(X)$ divides $\overline{2}\overline{h}(X)-\overline{k}(X)\,\overline{b}_1(X)$ and $\overline{h}^2(X)-\overline{k}^2(X)\,\overline{a}(X)\overline{c}_1(X)$ in $\mathbb{F}_p[X]$. Hence we have in $\mathbb{F}_p[X]$ congruences mod $(\bar{f}_i(X))$:

$$\begin{cases} \overline{2}\overline{h}(X) \equiv \overline{k}(X)\,\overline{b}_1(X)\,, \\ \overline{h}^2(X) \equiv \overline{k}^2(X)\,\overline{a}(X)\,\overline{c}_1(X)\,. \end{cases}$$

Eliminating $\overline{h}(X)$, these two relations combine to yield: $\bar{f}_i(X)$ divides $\overline{k}^2(X)[\overline{b}_1^2(X)-\overline{4}\overline{a}(X)\overline{c}_1(X)]$. Since $\overline{k}(X)$ and $\bar{f}_i(X)$ are coprime, $\bar{f}_i(X)$ divides $\overline{b}_1^2(X)-\overline{4}\overline{a}(X)\,\overline{c}_1(X)$. Then it follows from 2.9 that $b_1^2(X)-4a(X)\,c_1(X)\in(p,\,f_i(X))$ and $b^2(X)-4a(X)\,c(X)\in p^2(p,\,f_i(X))$, since $b(X)=pb_1(X)$ and $c(X)=p^2c_1(X)$. The direct part of the proof is done.

Conversely, assume that there exists a maximal ideal $M_i=(p_i,\,f_i(X))$ in $\mathbb{Z}[X]$ such that $f(X)\in M_i^2$ and $b^2(X)-4a(X)\,c(X)\in p^2M_i$. Thus we have by 2.11: $b_1^2(\alpha)-4a(\alpha)\,c_1(\alpha)\in P_i=(p,\,f_i(\alpha))$. Now we have to consider two cases: $p=2$ and $p\neq 2$.

- If $p=2$.

Observe that $b_1^2(\alpha)\in P_i$; it follows that $b_1(\alpha)\in P_i$, since P_i is a prime ideal. As $\deg b_1(X)<\deg f_i(X)$, we get $b_1(X)\in 2\mathbb{Z}[X]$ and $b_1(\alpha)\in 2\mathbb{Z}[\alpha]$.

Each element of the finite field $K=\mathbb{F}_2[X]/(\bar{f}_i(X))$ is a square since the characteristic of K is 2. Thus there exists $h(X)\in\mathbb{Z}[X]$ such that $\overline{h}^2(X)-\overline{c}_1(X)\overline{a}(X)\in(\bar{f}_i(X))$, or equivalently, such that $h^2(\alpha)-c_1(\alpha)\,a(\alpha)\in P_i$. Set $x=h(\alpha)+f_i(\alpha)\,a(\alpha)2^{-1}$. We have $x\notin\mathbb{Z}[\alpha]$, otherwise relation $f_i(\alpha)\,a(\alpha)\in 2\mathbb{Z}[\alpha]$ implies that $\bar{f}(X)$ divides $\bar{f}_i(X)\,\overline{a}(X)$ in $\mathbb{F}_2[X]$, a contradiction by 2.10. Such an x satisfies $xP_i\subset P_i$ since $f_i^2(\alpha)\,a(\alpha)\in 2P_i$. Furthermore, we have:

$$x^2=h^2(\alpha)+h(\alpha)f_i(\alpha)\,a(\alpha)+f_i^2(\alpha)\,a^2(\alpha)2^{-2}=$$

$$h(\alpha)f_i(\alpha)\,a(\alpha)+[h^2(\alpha)-c_1(\alpha)\,a(\alpha)]-a(\alpha)\,b_1(\alpha)f_i(\alpha)2^{-1}\in P_i\,,$$

since $h^2(\alpha)-c_1(\alpha)\,a(\alpha)\in P_i$ and $b_1(\alpha)\in 2\mathbb{Z}[\alpha]$. So, there exists $x\in\mathbb{Q}[\alpha]-\mathbb{Z}[\alpha]$ such that $xP_i\subset P_i$ and $x^2\in P_i$. Therefore $\mathbb{Z}[\alpha]$ is not seminormal.

- If $p\neq 2$.

As p is odd, we can write $p=2n-1$, where $n\in\mathbb{N}^*$. Set $x=nb_1(\alpha)+a(\alpha)f_i(\alpha)p^{-1}$. We obtain $x\notin\mathbb{Z}[\alpha]$ as above, since $a(\alpha)f_i(\alpha)\notin p\mathbb{Z}[\alpha]$; furthermore $xP_i\subset P_i$ because $f_i^2(\alpha)\,a(\alpha)\in pP_i$. Thus we get $x^2=n^2b_1^2(\alpha)+2nb_1(\alpha)f_i(\alpha)\,a(\alpha)p^{-1}+f_i^2(\alpha)\,a^2(\alpha)\,p^{-2}$. But $b_1^2(\alpha)-4a(\alpha)\,c_1(\alpha)=b_2(\alpha)\in$

P_i implies

$$x^2 = n^2 b_2(\alpha) + 4n^2 a(\alpha)\, c_1(\alpha) + $$
$$2nb_1(\alpha) f_i(\alpha)\, a(\alpha)\, p^{-1} + a(\alpha)\, p^{-2}[-pb_1(\alpha) f_i(\alpha) - p^2 c_1(\alpha)] =$$
$$n^2 b_2(\alpha) + (4n^2 - 1)\, a(\alpha)\, c_1(\alpha) + (2n-1)\, p^{-1} b_1(\alpha) f_i(\alpha)\, a(\alpha)\,.$$

Thus $p = 2n - 1$ implies $x^2 \in P_i$ and $\mathbb{Z}[\alpha]$ is not seminormal.

Next, we give one of our main results, a seminormality criterion for an order $\mathbb{Z}[\alpha]$.

THEOREM 3.2. – *Let α be an algebraic integer with minimal polynomial $f(X)$.*

For each maximal ideal $M_i = (p,\, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$, let

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$.

Then $\mathbb{Z}[\alpha]$ is seminormal if and only if $b^2(X) - 4a(X)\, c(X) \notin p^2 M_i$ for each prime $p \in \mathbb{Z}$ and $f_i(X)$ for which $f(X) \in M_i^2$.

PROOF. – We know that integral closedness implies seminormality. $\mathbb{Z}[\alpha]$ is seminormal if and only if the conditions of 3.1 are not fulfilled, that is to say, for each maximal ideal $(p,\, f_i(X))$ in $\mathbb{Z}[X]$, either $f(X) \notin (p,\, f_i(X))^2$ or $f(X) \in (p,\, f_i(X))^2$ and $b^2(X) - 4a(X)\, c(X) \notin p^2 (p,\, f_i(X))$. If we have $f(X) \notin (p,\, f_i(X))^2$ for each maximal ideal $(p,\, f_i(X))$ in $\mathbb{Z}[X]$, apply 1.1 to get that $\mathbb{Z}[\alpha]$ is integrally closed.

COROLLARY 3.3. – *Let R be a Dedekind domain and α be an element of some integral domain which contains R where α is integral over R. Let $f(X) \in R[X]$ be the minimal polynomial of α. For each maximal ideal $M_i = (P,\, f_i(X))$ in $R[X]$ containing $f(X)$, let*

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$ in $R[X]$ and let $p \in P$ be such that $PR_P = pR_P$. Then $R[\alpha]$ is seminormal if and only if, for each maximal ideal $M_i = (P,\, f_i(X))$ in $R[X]$ such that $f(X) \in M_i^2$, we have:

- *$2 \notin P$ implies $b^2(X) - 4a(X)\, c(X) \notin P^2 M_i$,*
- *$2 \in P$ implies $b(X) \notin P^2 R[X]$ or $p^{-2} a(X) c(X)$ is not a quadratic residue mod $(M_i)_P$.*

PROOF. – By 2.16, $R[\alpha]$ is not seminormal if and only if there exists a maximal ideal P in R such that $R_P[\alpha]$ is not seminormal. As far as the PID property of the ring $\mathbb{Z}$ is used we can go back to the proof of 3.1 since R_P is a principal domain. If $R_P[\alpha]$ is not seminormal, by the first part of the proof of 3.1, there exists a maximal ideal $(M_i)_P = (p, f_i(X))$ in $R_P[X]$, where $M_i = (P, f_i(X))$ is a maximal ideal in $R[X]$, such that $f(X) \in (M_i)_P^2$ and $b^2(X) - 4a(X)\,c(X) \in p^2(M_i)_P \cap R[X] = P^2 M_i$. Moreover, we have $b(X) = pb_1(X)$ and $c(X) = p^2 c_1(X)$, with $b_1(X), c_1(X) \in R_P[X]$. So we get $b_1^2(X) - 4a(X)\,c_1(X) \in (M_i)_P$. Following the notations of the proof of 3.1, we still have in $R_P/PR_P[X]$ the congruence $\bar{h}^2(X) \equiv \bar{k}^2(X)\,\bar{a}(X)\,\bar{c}_1(X) \bmod (\bar{f}_i(X))$.

If $2 \in P$, condition $b^2(X) - 4a(X)\,c(X) \in P^2 M_i$ implies $b^2(X) \in P^2 M_i$, since $c(X) \in M_i$. Because we can write $b(X) = pb_1(X)$ in $R_P[X]$, we get $b_1^2(X) \in (M_i)_P$. As in the proof of 3.1, we get then $b_1(X) \in pR_P[X]$, which implies $b(X) \in p^2 R_P[X] \cap R[X] = P^2 R[X]$.

Conversely, let us assume that there exists a maximal ideal $M_{iP} = (p, f_i(X))$ in $R_P[X]$ such that $f(X) \in (M_i)_P^2$ and such that:

– if $2 \notin P$, then $b^2(X) - 4a(X)\,c(X) \in P^2 M_i$,

– if $2 \in P$, then $b(X) \in P^2 R[X]$ and $p^{-2}a(X)\,c(X)$ is a quadratic residue mod $(M_i)_P$.

• If $2 \notin P$, we get that 2 and p are coprime in R_P. Hence we can write $2n + mp = 1$, with $n, m \in R_P$ and the proof of 3.1 is again valid with $x = nb_1(\alpha) + a(\alpha) f_i(\alpha) p^{-1}$.

• If $2 \in P$, as R/P is not necessarily a finite field with characteristic 2, any element may not be a quadratic residue mod $(M_i)_P$. Anyway, we can set $2 = pn$, $n \in R_P$. If $a(X)\,c_1(X) = a(X)\,c(X)p^{-2}$ is a quadratic residue mod $(M_i)_P$, there exists $h(X) \in R_P[X]$ such that $\bar{h}^2(X) - \bar{c}_1(X)\,\bar{a}(X) \in (\bar{f}_i(X))$ in $R_P/PR_P[X]$. Moreover, we have $b_1(X) \in pR_P[X]$ since $b(X) \in P^2 R[X]$. We take then $x = h(\alpha) + f_i(\alpha)\,a(\alpha)\,p^{-1}$ and we end the proof as in 3.1.

So we get the following result:

$R[\alpha]$ is not seminormal if and only if there exists a maximal ideal $M_i = (P, f_i(X))$ in $R[X]$ such that $f(X) \in M_i^2$ and such that:

– if $2 \notin P$, then $b^2(X) - 4a(X)\,c(X) \in P^2 M_i$

– if $2 \in P$, then $b(X) \in P^2 R[X]$ and $p^{-2}a(X)\,c(X)$ is a quadratic residue mod $(M_i)_P$.

Then the seminormality criteria follows immediately.

REMARK. – If 2 is a unit in R or if R/P is a finite field for each maximal ideal P in R containing 2, we recover the condition of 2.2.

4. – When is $\mathbb{Z}[\alpha]$ t-closed?

As in the previous section, we begin to give conditions for $\mathbb{Z}[\alpha]$ not to be t-closed. By 2.3, $\mathbb{Z}[\alpha]$ is not t-closed if and only if $\mathbb{Z}[\alpha] \neq {}^t\mathbb{Z}[\alpha]$, or equivalently, $\mathbb{Z}[\alpha] \to {}^t\mathbb{Z}[\alpha]$ is composed only of ramified or decomposed minimal morphisms (by 2.5). So, it follows from 2.4 that $\mathbb{Z}[\alpha]$ is not t-closed if and only if there exists a subring B of the integral closure of $\mathbb{Z}[\alpha]$ such that $\mathbb{Z}[\alpha] \to B$ is a ramified or a decomposed morphism. Hence, we deduce from 2.4 that $\mathbb{Z}[\alpha]$ is not t-closed if and only if there is some $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ and a maximal ideal P of $\mathbb{Z}[\alpha]$ with $xP \subset P$, where P is the conductor of $\mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha, x]$, such that:

(1) either $x^2, x^3 \in \mathbb{Z}[\alpha]$,

(2) or $x^2 - x,\ x^3 - x^2 \in \mathbb{Z}[\alpha]$.

Condition (1) means that $\mathbb{Z}[\alpha]$ is not seminormal and is 3.1.

Thus we are aiming to give a necessary and sufficient condition for the existence of $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ and a maximal ideal P of $\mathbb{Z}[\alpha]$ such that $xP \subset P$ and x satisfies (2).

LEMMA 4.1. – *Let α be an algebraic integer with minimal polynomial $f(X)$. For each maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$, let*

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$.

Then, there exist $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ and a maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$ such that $x(p, f_i(\alpha)) \subset (p, f_i(\alpha))$ and $x^2 - x \in (p, f_i(\alpha))$ if and only if $f(X) \in M_i^2$ and:

– *if $p \neq 2$, $[b^2(X) - 4a(X)\,c(X)]p^{-2}$ is a nonzero quadratic residue mod M_i.*

– *if $p = 2$, $b(X) \notin 4\mathbb{Z}[X]$ and there exists $h(X) \in \mathbb{Z}[X]$ such that*

$$b^2(X)[h^2(X) + h(X)] - a(X)\,c(X) \in 4M_i\,.$$

PROOF. – For a maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$, let P_i be the maximal ideal $(p, f_i(\alpha))$ of $\mathbb{Z}[\alpha]$. As in 3.1, the condition $xP_i \subset P_i$, for $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ gives $x = [ph(\alpha) + f_i(\alpha)\,k(\alpha)\,a(\alpha)]p^{-1}$, where $\bar{k}(X)$ and $\bar{f}_i(X)$ are coprime in $\mathbb{F}_p[X]$, so that $f_i(\alpha)\,k(\alpha)\,a(\alpha) \notin p\mathbb{Z}[\alpha]$. The following statements are equivalent:

(i) $x^2 - x \in P_i$,

(ii) $p[h^2(\alpha) - h(\alpha)] + f_i(\alpha) k(\alpha) a(\alpha)[2h(\alpha) - 1] - k^2(\alpha) a(\alpha)[b_1(\alpha) f_i(\alpha) + pc_1(\alpha)] \in pP_i$,

(iii) $p[h^2(X) - h(X)] + f_i(X)\, k(X)\, a(X)[2h(X) - 1] - k^2(X)\, a(X)[b_1(X) f_i(X) + pc_1(X)] = p^2 a_2(X) + pf_i(X)\, b_2(X) + c_2(X)\, f(X)$, with $a_2(X),\ b_2(X),\ c_2(X) \in \mathrm{Z}[X]$.

Then (iii) implies in $\mathbb{F}_p[X]$ the relation:

$$\bar{f}_i(X)\, \overline{k}(X)\, \overline{a}(X)[\overline{2}\,\overline{h}(X) - \overline{1} - \overline{k}(X)\, \overline{b}_1(X)] = \overline{c}_2(X) \bar{f}_i^{\,2}(X)\, \overline{a}(X)$$

so that: $\overline{k}(X)[\overline{2}\,\overline{h}(X) - \overline{1} - \overline{k}(X)\, \overline{b}_1(X)] = \overline{c}_2(X)\, \bar{f}_i(X)$. But, as $\overline{k}(X)$ and $\bar{f}_i(X)$ are coprime, we get the following condition

$$\bar{f}_i(X) \text{ divides } \overline{2}\,\overline{h}(X) - \overline{1} - \overline{k}(X)\, \overline{b}_1(X) \ (\dagger)$$

Thus, $2h(\alpha) - 1 - k(\alpha)\, b_1(\alpha) \in P_i$ allows us to write:

$$2h(\alpha) - 1 - k(\alpha)\, b_1(\alpha) = pa_3(\alpha) + f_i(\alpha)\, b_3(\alpha), \quad \text{with } a_3(X),\ b_3(X) \in \mathbb{Z}[X].$$

So (ii) implies $p[h^2(\alpha) - h(\alpha)] + f_i(\alpha)\, k(\alpha)\, a(\alpha)[pa_3(\alpha) + f_i(\alpha)\, b_3(\alpha)] - pk^2(\alpha)\, a(\alpha)\, c_1(\alpha) \in pP_i$ which gives $h^2(\alpha) - h(\alpha) - k^2(\alpha)\, a(\alpha)\, c_1(\alpha) \in P_i$ and then

$$\bar{f}_i(X) \text{ divides } \overline{h}^2(X) - \overline{h}(X) - \overline{k}^2(X)\, \overline{a}(X)\, \overline{c}_1(X) \ (\dagger\dagger).$$

To sum up, (i) implies ($\dagger$) and ($\dagger\dagger$). To carry on the direct part of the proof we have to consider two cases.

– If $p = 2$, condition ($\dagger$) becomes : $\bar{f}_i(X)$ divides $\overline{1} + \overline{k}(X)\, \overline{b}_1(X)$. So, $\bar{f}_i(X)$ and $\overline{b}_1(X)$ are coprime, $b(X) \notin 4\mathbb{Z}[X]$ and we get:

$$(\dagger\dagger) \Rightarrow \bar{f}_i(X) \text{ divides } \overline{b}_1^2(X)[\overline{h}^2(X) + \overline{h}(X)] - \overline{a}(X)\, \overline{c}_1(X)$$

$$\Rightarrow \text{there exists } h(X) \in \mathbb{Z}[X] \text{ such that } b_1^2(X)[h^2(X) + h(X)] - a(X)\, c_1(X) \in (2,\ f_i(X))$$

$$\Rightarrow \text{there exists } h(X) \in \mathbb{Z}[X] \text{ such that } b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \in 4(2,\ f_i(X)).$$

– If $p \neq 2$, as in 3.1, set $p = 2n - 1$. Eliminating $\overline{h}(X)$ between ($\dagger$) and ($\dagger\dagger$), we get that ($\dagger$) $\Leftrightarrow$ $\bar{f}_i(X)$ divides $\overline{h}(X) - \overline{n}[\overline{1} + \overline{k}(X)\overline{b}_1(X)]$ and this last condition combines with ($\dagger\dagger$) to give the following equivalent conditions to ($\dagger\dagger$):

- $\bar{f}_i(X)$ divides $\overline{n}^2[\overline{1} + \overline{2}\,\overline{k}(X)\, \overline{b}_1(X) + \overline{k}^2(X)\, \overline{b}_1^2(X)] - \overline{n}[\overline{1} + \overline{k}(X)\, \overline{b}_1(X)] - \overline{k}^2(X)\, \overline{a}(X)\, \overline{c}_1(X)$
- $\bar{f}_i(X)$ divides $\overline{n}^2 - \overline{n} + (\overline{2n} - \overline{1})\, \overline{n}\,\overline{k}(X)\, \overline{b}_1(X) + \overline{k}^2(X)[\overline{n}^2 \overline{b}_1^2(X) - \overline{a}(X)\, \overline{c}_1(X)]$.
- $\bar{f}_i(X)$ divides $\overline{4}(\overline{n}^2 - \overline{n}) + \overline{4}\,\overline{k}^2(X)[\overline{n}^2 \overline{b}_1^2(X) - \overline{a}(X)\, \overline{c}_1(X)]$,
- $\bar{f}_i(X)$ divides $\overline{k}^2(X)[\overline{b}_1^2(X) - \overline{4}\,\overline{a}(X)\, \overline{c}_1(X)] - \overline{1}$.

Now, bearing in mind that $\bar{k}(X)$ and $\bar{f}_i(X)$ are coprime, we observe that there exists $\bar{k}_1(X)$ such that $\bar{f}_i(X)$ divides $\bar{k}(X)\bar{k}_1(X)-\bar{1}$. Therefore, we get that (††) is equivalent to

$$\bar{f}_i(X) \text{ divides } \bar{b}_1^2(X)-\bar{4}\bar{a}(X)\,\bar{c}_1(X)-\bar{k}_1^2(X),$$

which implies $b_1^2(X)-4a(X)\,c_1(X)=[b^2(X)-4a(X)\,c(X)]\,p^{-2}$ is a nonzero quadratic residue mod $(p,\ f_i(X))$.

Conversely, let us assume that the conditions of 4.1 are fulfilled.

If $p\neq 2$ and if there exists $k_1(X)\in\mathbb{Z}[X]\backslash(p,\ f_i(X))$ such that

$$[b^2(X)-4a(X)\,c(X)]p^{-2}-k_1^2(X)\in(p,\ f_i(X))$$

we have $b_1^2(\alpha)-4a(\alpha)\,c_1(\alpha)-k_1^2(\alpha)\in P_i$.

Consider $h(X)=n[1+k(X)\,b_1(X)]$, with $k(X)\,k_1(X)-1\in(p,\ f_i(X))$, since $\bar{k}_1(X)$ and $\bar{f}_i(X)$ are coprime. By the direct part of the proof, we get:

$$h^2(X)-h(X)-k^2(X)\,a(X)\,c_1(X)\in(p,\ f_i(X));$$

setting $x=h(\alpha)+f_i(\alpha)\,k(\alpha)\,a(\alpha)\,p^{-1}$, we have: $x\notin\mathbb{Z}[\alpha]$, $x^2-x\in P_i$ and $xP_i\subset P_i$, since $2h(X)-1-k(X)\,b_1(X)\in(p,\ f_i(X))$.

If $p=2$, assume that $b(X)\notin 4\mathbb{Z}[X]$ and that there exist $h(X)\in\mathbb{Z}[X]$ such that $b^2(X)[h^2(X)+h(X)]-a(X)\,c(X)\in 4(2,\ f_i(X))$ and $k(X)\in\mathbb{Z}[X]$ such that $k(X)\,b_1(X)-1\in(2,\ f_i(X))$. Then, for $x=h(\alpha)+f_i(\alpha)\,k(\alpha)\,a(\alpha)2^{-1}$, we still have $x\in\mathbb{Q}[\alpha]\backslash\mathbb{Z}[\alpha]$ such that $xP_i\subset P_i$ and $x^2-x\in P_i$ and we are done.

PROPOSITION 4.2. – *Let α be an algebraic integer with minimal polynomial $f(X)$.*

For each maximal ideal $M_i=(p,\ f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$, let

$$f(X)=a(X)\,f_i^2(X)+b(X)\,f_i(X)+c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$.

Then, $\mathbb{Z}[\alpha]$ is not t-closed if and only if there exists a maximal ideal $M_i=(p,\ f_i(X))$ of $\mathbb{Z}[X]$ such that $f(X)\in M_i^2$ and:

(*a*) *if $p\neq 2$, $[b^2(X)-4a(X)\,c(X)]p^{-2}$ is a quadratic residue mod M_i.*

(*b*) *if $p=2$, $b(X)\in 4\mathbb{Z}[X]$, or there exists $h(X)\in\mathbb{Z}[X]$ such that*

$$b^2(X)[h^2(X)+h(X)]-a(X)\,c(X)\in 4M_i\,.$$

PROOF. – Come back to the beginning of this section. We have seen that $\mathbb{Z}[\alpha]$ is not t-closed if and only if there exist some $x \in \mathbb{Q}[\alpha]\backslash\mathbb{Z}[\alpha]$ and a maximal ideal P of $\mathbb{Z}[\alpha]$ with $xP \subset P$ such that:

(1) either $x^2, x^3 \in \mathbb{Z}[\alpha]$,

(2) or $x^2 - x, x^3 - x^2 \in \mathbb{Z}[\alpha]$.

If (1) is satisfied, $\mathbb{Z}[\alpha]$ is not seminormal and there exists, by 3.1, a maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ such that $f(X) \in M_i^2$ and $b^2(X) - 4a(X)\,c(X) \in p^2 M_i$, that is to say, $[b^2(X) - 4a(X)\,c(X)]p^{-2} \in M_i$.

If (2) is satisfied, P is the conductor of $\mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha, x]$ and $x^3 - x^2 \in \mathbb{Z}[\alpha]$ implies $x^2 - x \in P$; we are then under the assumption of 4.1 and we get $f(X) \in M_i^2$.

If $p \neq 2$, with the notations of 4.1, we get that $[b^2(X) - 4a(X)\,c(X)]\,p^{-2}$ is a nonzero quadratic residue mod M_i. But, $[b^2(X) - 4a(X)\,c(X)]\,p^{-2} \in M_i$ implies $[b^2(X) - 4a(X)\,c(X)]\,p^{-2}$ is a zero quadratic residue mod M_i.

Hence in any case $[b^2(X) - 4a(X)\,c(X)]p^{-2}$ is a quadratic residue mod M_i.

If $p = 2$, and if (1) is satisfied, we still have $[b^2(X) - 4a(X)\,c(X)]2^{-2} \in M_i = (2, f_i(X))$, with $f(X) \in M_i^2$. Remember that this last condition implies $b_1^2(X) - 4a(X)\,c_1(X) \in M_i$, where $b(X) = 2b_1(X)$ and $c(X) = 4c_1(X)$; this implies that $b_1(X) \in 2\mathbb{Z}[X]$.

If (2) is satisfied, we have seen in 4.1 that $b(X) \notin 4\mathbb{Z}[X]$ and that there exists $h(X) \in \mathbb{Z}[X]$ such that $b^2(X)[h^2(X) + h(X)] - a(X)\,c(X) \in 4M_i$.

Conversely, let us assume the conditions of 4.2 are fulfilled. Let $M_i = (p, f_i(X))$ be a maximal ideal of $\mathbb{Z}[X]$ such that $f(X) \in M_i^2$ and satisfying (a) or (b):

(a) If $p \neq 2$ then $[b^2(X) - 4a(X)\,c(X)]p^{-2}$ is a quadratic residue mod M_i. If this quadratic residue is nonzero, by 4.1, there exists $x \in \mathbb{Q}[\alpha]\backslash\mathbb{Z}[\alpha]$ such that $x^2 - x \in P_i = (p, f_i(\alpha))$, with $xP_i \subset P_i$. This implies $x^3 - x^2 \in \mathbb{Z}[\alpha]$ and $\mathbb{Z}[\alpha]$ is not t-closed.

If $[b^2(X) - 4a(X)\,c(X)]p^{-2} \in M_i$, then $\mathbb{Z}[\alpha]$ is not seminormal in view of 3.1, whence is not t-closed.

(b) If $p = 2$ and $b(X) \in 4\mathbb{Z}[X]$, then $b^2(X) - 4a(X)\,c(X) \in 4M_i$ and $\mathbb{Z}[\alpha]$ is still not t-closed.

If $p = 2$ and $b(X) \notin 4\mathbb{Z}[X]$, there exists $h(X) \in \mathbb{Z}[X]$ such that

$$b^2(X)[h^2(X) + h(X)] - a(X)\,c(X) \in 4M_i$$

then it follows again that $\mathbb{Z}[\alpha]$ is not t-closed by 4.1.

REMARKS.

(1) If $f(X) \in (p, f_i(X))^2$ is such that $\bar{f}_i^3(X)$ divides $\bar{f}(X)$ in $\mathbb{F}_p[X]$, we can observe that for any prime integer p, the conditions of 4.2 are fulfilled:

Indeed $\bar{f}_i(X)$ divides $\bar{a}(X)$ whence $a(X) \in (p, f_i(X))$.

If $p \neq 2$, the condition «$b_1^2(X) - 4a(X)\, c_1(X)$ is a quadratic residue mod $(p, f_i(X))$» is always satisfied.

If $p = 2$, the condition « $b(X) \in 4\mathbb{Z}[X]$ or there exists $h(X) \in \mathbb{Z}[X]$ such that $b_1^2(X)[h^2(X) + h(X)] - a(X)\, c_1(X) \in (2, f_i(X))$» is satisfied, since we can choose $h(X) = 0$ if $b(X) \notin 4\mathbb{Z}[X]$.

(2) The map $z \mapsto z^2 + z$ is an additive group endomorphism of $\mathbb{F}_2[X]/(\bar{f}_i(X))$, the kernel of which is $\{0, 1\}$. Since this map is not surjective, for a given $\bar{k}^2(X)\, \bar{a}(X)\, \bar{c}_1(X) \in \mathbb{F}_2[X]$, there is not always $\bar{h}(X) \in \mathbb{F}_2[X]$ such that (††) is satisfied; nevertheless half of the elements of $\mathbb{F}_2[X]/(\bar{f}_i(X))$ can be written $z^2 + z$, with $z \in \mathbb{F}_2[X]/(\bar{f}_i(X))$.

We are now able to give a characterization for $\mathbb{Z}[\alpha]$ to be t-closed.

THEOREM 4.3. – *Let α be an algebraic integer with minimal polynomial $f(X)$.*

For each maximal ideal $M_i = (p, f_i(X))$ of $\mathbb{Z}[X]$ containing $f(X)$, let

$$f(X) = a(X) f_i^2(X) + b(X) f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$.

Then $\mathbb{Z}[\alpha]$ is t-closed if and only if, for each maximal ideal $M_i = (p, f_i(X))$ for which $f(X) \in M_i^2$, we have:

– if $p \neq 2$, $[b^2(X) - 4a(X)\, c(X)]\, p^{-2}$ is not a quadratic residue mod M_i (‡).

– if $p = 2$, $b(X) \notin 4\mathbb{Z}[X]$ and, for each $h(X) \in \mathbb{Z}[X]$, we have:

$$b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin 4M_i \ (‡‡).$$

Moreover, if $\mathbb{Z}[\alpha]$ is t-closed, for each maximal ideal $M_i = (p, f_i(X))$ for which $f(X) \in M_i^2$, we have $\bar{f}(X) \notin (\bar{f}_i^3(X))$ in $\mathbb{F}_p[X]$.

PROOF. – The proof is similar to the proof of 3.2.

REMARK. – Set $K = \mathbb{F}_p[X]/(\bar{f}_i(X))$ and denote by $\pi(x)$ the residue class of $x \in \mathbb{Z}[X]$. Then:

If $p \neq 2$, condition (‡) is equivalent to: $Y^2 - \pi[(b^2(X) - 4a(X)\, c(X))p^{-2}]$ is irreducible in $K[Y]$.

If $p = 2$, condition (‡‡) is equivalent to: $(Y^2 + Y)\,\pi(b^2(X)2^{-2}) - \pi(a(X)\,c(X)2^{-2})$ is irreducible in $K[Y]$.

PROPOSITION 4.4. – *Let $\mathbb{Z}[\alpha]$ be a t-closed, non integrally closed ring, with integral closure $\overline{\mathbb{Z}[\alpha]}$. There exist $P \in \operatorname{Spec}(\mathbb{Z}[\alpha])$ and $Q \in \operatorname{Spec}(\overline{\mathbb{Z}[\alpha]})$ lying over P, such that $[\overline{\mathbb{Z}[\alpha]}/Q : \mathbb{Z}[\alpha]/P]$ is even.*

PROOF. – Remark 2.12 (1) shows that there is some $x \in \overline{\mathbb{Z}[\alpha]} \setminus \mathbb{Z}[\alpha]$ satisfying a quadratic relation over $\mathbb{Z}[\alpha]$. Denote by A (resp. B) the ring $\mathbb{Z}[\alpha]$ (resp. $\mathbb{Z}[\alpha, x]$). We have seen that there exists a maximal ideal P in A such that $xP \subset P$: in fact, P is the conductor of t-closed minimal morphism $A \to B$ since A is a t-closed ring [6, Remark 2 of Definition 3.1]. Thus, P is a maximal ideal in B by [6, Theorem 3.15] and $B/P = (A/P)[\overline{x}]$ is a two-dimensional vector space over A/P. As $A \to \overline{\mathbb{Z}[\alpha]}$ is a finite (order) morphism, we get the result.

REMARK. – Assume that $A = \mathbb{Z}[\alpha]$ is not integrally closed, with integral closure $\overline{A}$. Then there exists an element $x \in \overline{A} \setminus A$ which is a zero of a monic polynomial $f(X) \in A[X]$ with degree 2:

- if $\mathbb{Z}[\alpha]$ is t-closed, the result is given by 4.4,
- if $\mathbb{Z}[\alpha]$ is not t-closed, the result is given by 2.5.

We recall that an integral domain A is quadratically integrally closed if $x^2 + ax + b = 0$, for x in the quotient field of A and $a, b \in A$, implies $x \in A$ [2].

This implies the following result:

PROPOSITION 4.5. – *Let α be an algebraic integer. Then, $\mathbb{Z}[\alpha]$ is quadratically integrally closed if and only if it is integrally closed.*

PROOF. – Obviously, an integrally closed ring is quadratically integrally closed. Conversely, assume that $\mathbb{Z}[\alpha]$ is quadratically integrally closed and not integrally closed. By 2.11 and Remark 2.12 (1), there exists $x \in \mathbb{Q}[\alpha] \setminus \mathbb{Z}[\alpha]$ satisfying a quadratic (integral) relation over $\mathbb{Z}[\alpha]$, *i.e.*, there exist $a(\alpha), b(\alpha) \in \mathbb{Z}[\alpha]$ such that $x^2 + a(\alpha)\,x + b(\alpha) = 0$. Then, the assumption on $\mathbb{Z}[\alpha]$ implies $x \in \mathbb{Z}[\alpha]$, a contradiction. Therefore, $\mathbb{Z}[\alpha]$ is integrally closed.

COROLLARY 4.6. – *Let R be a Dedekind domain and α be an element of some integral domain which contains R where α is integral over R. Let $f(X) \in R[X]$ be the minimal polynomial of α. For each maximal ideal $M_i = (P, f_i(X))$ in $R[X]$ containing $f(X)$, let*

$$f(X) = a(X)\,f_i^2(X) + b(X)\,f_i(X) + c(X)$$

be the double Euclidean division of $f(X)$ by $f_i(X)$ in $R[X]$ and let $p \in P$ be such that $PR_P = pR_P$. Then $R[\alpha]$ is t-closed if and only if, for each maximal ideal $M_i = (P, f_i(X))$ in $R[X]$ such that $f(X) \in M_i^2$, we have:

- *$2 \notin P$ implies $[b^2(X) - 4a(X)c(X)]p^{-2}$ is not a quadratic residue mod $(M_i)_P$*

- *$2 \in P$ implies:*

– if $b(X) \notin P^2R[X]$, then $b^2(X)[h^2(X) + h(X)] - a(X)c(X) \notin P^2M_i$ for each $h(X) \in R[X]$

– if $b(X) \in P^2R[X]$, then, $p^{-2}a(X)c(X)$ is not a quadratic residue mod $(M_i)_P$.

PROOF. – By 2.16, $R[\alpha]$ is not t-closed if and only if there exists a maximal ideal P in R such that $R_P[\alpha]$ is not t-closed. Then, there exists a maximal ideal in $R_P[X]$, of the form $(M_i)_P$, where $M_i = (P, f_i(X))$ is a maximal ideal in $R[X]$ such that $f(X) \in (M_i^2)_P$.

Following the proof of 4.3, we begin to give conditions for the existence of an element x in the integral closure of $R_P[\alpha]$ such that $x^2 - x$ or $x^2 \in (P_i)_P$ and $x(P_i)_P \subset (P_i)_P$, where $P_i = (P, f_i(\alpha))$ is a maximal ideal in $R[\alpha]$. We get then $(P_i)_P = (p, f_i(\alpha))$ in $R_P[\alpha]$, where $p \in P$ is such that $PR_P = pR_P$.

Condition $x^2 - x \in (P_i)_P$ is the same as the one get in 4.1, considering the cases $2 \in P$ and $2 \notin P$ instead of $p = 2$ and $p \neq 2$. Now, we have seen in 3.3 that, if $2 \in P$, there exists x in the integral closure of $R_P[\alpha]$ such that $x^2 \in (P_i)_P$ and $x(P_i)_P \subset (P_i)_P$ if and only if $b(X) \in P^2R[X]$ and $a(X)c(X)p^{-2}$ is a quadratic residue mod $(M_i)_P$. When $2 \in P$, the condition of non t-closedness of $R_P[\alpha]$ gotten in 4.2 for $p = 2$ is changed into one of the two following conditions:

«$b(X) \notin P^2R_P[X]$ and there exists $h(X) \in R_P[X]$ such that

$$b^2(X)[h^2(X) + h(X)] - a(X)c(X) \in p^2(M_i)_P»$$

or

«$b(X) \in P^2R_P[X]$ and $p^{-2}a(X)c(X)$ is a quadratic residue mod $(M_i)_P$» .

We get then the two following conditions for t-closedness of $R_P[\alpha]$, when $2 \in P$:

«$b(X) \in P^2R_P[X]$ or $b^2(X)[h^2(X) + h(X)] - a(X)c(X) \notin p^2(M_i)_P$

for each $h(X) \in R_P[X]$»

and

$$«b(X) \notin P^2 R_P[X] \text{ or } p^{-2} a(X)\, c(X) \text{ is not a quadratic residue mod} (M_i)_P» .$$

Hence it results that $R_P[\alpha]$ is t-closed, when $2 \in P$, if and only if the two following conditions are satisfied:

«$b(X) \notin P^2 R_P[X]$ implies that for each $h(X) \in R_P[X]$ we have

$$b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin p^2 (M_i)_P»$$

and

«$b(X) \in P^2 R_P[X]$ implies that $p^{-2} a(X)\, c(X)$

is not a quadratic residue mod $(M_i)_P$».

In fact, the condition

$$\text{for each } h(X) \in R_P[X] \text{ we have } b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin p^2 (M_i)_P$$

is equivalent to:

$$\text{for each } h(X) \in R[X] \text{ we have } b^2(X)[h^2(X) + h(X)] - a(X) c(X) \notin P^2 M_i.$$

Indeed, we have seen in 3.3 that $p^2 (M_i)_P \cap R[X] = P^2 M_i$. So, if $h(X) \in R[X]$ is such that

$$b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin p^2 (M_i)_P$$

we get then $b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin P^2 M_i$. Conversely, assume that for each $h(X) \in R[X]$, we have $b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) \notin P^2 M_i$ and let $g(X) \in R_P[X]$. Thanks to the isomorphism $R/P \simeq R_P/PR_P$, there exists $h(X) \in R[X]$ such that $g(X) = h(X) + pk(X)$, where $k(X) \in R_P[X]$. Now

$$b^2(X)[h^2(X) + h(X)] - a(X)\, c(X) = p^2[b_1^2(X)[g^2(X) + g(X)] - a(X)\, c_1(X)] +$$

$$p^2 b_1^2(X)[p^2 k^2(X) - 2pg(X)\, k(X) - pk(X)] \notin p^2 (M_i)_P.$$

But $p^2 b_1^2(X)[p^2 k^2(X) - 2pg(X)\, k(X) - pk(X)] \in p^2 (M_i)_P$ implies

$$b_1^2(X)[g^2(X) + g(X)] - a(X)\, c_1(X) \notin (M_i)_P$$

and then $b^2(X)[g^2(X) + g(X)] - a(X)\, c(X) \notin p^2 (M_i)_P$.

5. – Application to simple cubic orders.

H. Tanimoto [11, Theorem 2.3, Theorem 4.4 and Theorem 5.1], D. Dobbs and M. Fontana [3, Theorem 2.5 and Corollary 4.5] obtained characterizations for a quadratic order to be integrally closed, quasinormal or GPVD (which is equivalent to be t-closed in our situation) or seminormal. Their results can be deduced from 2.12, 3.2 and 4.3. Now we study the situation for another special class of algebraic orders : a cubic order $\mathbb{Z}[\alpha]$, where α is a zero of the irreducible polynomial $f(X) = X^3 + aX + b$ (in $\mathbb{Z}[X]$).

Let p be a prime integer. The decomposition in $\mathbb{F}_p[X]$ of $\bar{f}(X)$ into monic irreducible polynomials $\bar{f}_i(X)$ give $\bar{f}(X) = \prod \bar{f}_i^{e_i}(X)$, with an index e_i such that $e_i \geq 2$ if and only if $\bar{f}(X)$ has a multiple zero, that is to say if and only if p divides the discriminant $\Delta = -(4a^3 + 27b^2)$ of $f(X)$.

PROPOSITION 5.1. – *Let α be an algebraic integer with minimal polynomial*

$$f(X) = X^3 + aX + b \in \mathbb{Z}[X].$$

Then, $\mathbb{Z}[\alpha]$ is integrally closed if and only if, for each prime integer p dividing the discriminant $\Delta = -(4a^3 + 27b^2)$ of $f(X)$, we have:

– *if $p = 2, 3$ or divides both a and b, then p^2 does not divide $f(a - b)$,*

– *for all other p dividing Δ, then p^2 does not divide Δ.*

PROOF. – We know by 2.13 that $\mathbb{Z}[\alpha]$ is integrally closed if and only if, for each prime integer p and each monic irreducible divisor $\bar{f}_i(X)$ of $X^3 + \bar{a}X + \bar{b}$ in $\mathbb{F}_p[X]$, we have $X^3 + aX + b \notin (p, f_i(X))^2$, where $f_i(X)$ is a monic polynomial in $\mathbb{Z}[X]$ with residue $\bar{f}_i(X)$ in $\mathbb{F}_p[X]$.

If $\deg \bar{f}_i(X) \geq 2$, we get $X^3 + aX + b \notin (p, f_i(X))^2$, since $\bar{f}_i^2(X)$ cannot divide $\bar{f}(X)$.

Hence it is enough to consider the case $\deg \bar{f}_i(X) = 1$, *i.e.*, $\bar{f}_i(X) = X - \bar{a}_1$. Then $a_1 \in \mathbb{Z}$, with residue $\bar{a}_1 \in \mathbb{F}_p$, satisfies the relation $f(a_1) = a_1^3 + aa_1 + b \in p\mathbb{Z}$. With definition 2.10, we obtain $f(X) = (X - a_1)^2(X + 2a_1) + (X - a_1)k + f(a_1)$, where $k = f'(a_1) = 3a_1^2 + a$, that is:

$$f(X) = (X - a_1)^2(X + 2a_1) + (X - a_1)(3a_1^2 + a) + f(a_1)\ (*).$$

Consider the relation $f(X) \in (p, X - a_1)^2$, which is equivalent to

$$(X - a_1)f'(a_1) + f(a_1) \in (p, X - a_1)^2,$$

and also, after an easy calculation, to $f'(a_1) \in p\mathbb{Z}\ (**)$ and $f(a_1) \in p^2\mathbb{Z}\ (***)$.

Then, for such an $a_1 \in \mathbb{Z}$, we have in $\mathbb{F}_p$:

$$\text{(S)} \qquad \begin{cases} \overline{a}_1^3 + \overline{a}\,\overline{a}_1 + \overline{b} = \overline{0} \\ \overline{3}\,\overline{a}_1^2 + \overline{a} = \overline{0} \end{cases},$$

where the last condition is equivalent to $(**)$, which implies $\overline{\Delta} = \overline{-4a^3 + 27b^2} = \overline{0}$ in $\mathbb{F}_p$. Conversely, if $\overline{\Delta} = \overline{0}$ in $\mathbb{F}_p$, there exists $a_1 \in \mathbb{Z}$ satisfying (S).

Now, if p is a prime integer such that p divides Δ, there exists $a_1 \in \mathbb{Z}$ satisfying (S).

– If $p = 2, 3$ or divides both a and b, relation (S) is fulfilled by $a_1 = a - b$. So, $f(X) \in (p, X - a_1)^2$ if and only if p^2 divides $(a-b)^3 + a(a-b) + b$.

– If $p \neq 2, 3$ and does not divide both a and b, relation (S) yields $\overline{2aa_1 + 3b} = \overline{0}$ in $\mathbb{F}_p$; thus we get $\overline{a}_1 = -(\overline{3b})(\overline{2a})^{-1}$. Furthermore, we can write $a_1^3 + aa_1 + b = np$ and $3a_1^2 + a = mp$, with $n, m \in \mathbb{Z}$. Thus, we observe that:

$$-\Delta = 4a^3 + 27b^2 = 4m^3p^3 + 9p^2(3n^2 - 6nma_1 - a_1^2m^2) + 108a_1^3pn\,.$$

As $\overline{3}\,\overline{a}_1^2 = -\overline{a}$ in $\mathbb{F}_p$, we get that p does not divide a_1. So, $f(a_1) \in p^2\mathbb{Z}$ if and only if p divides n, or also, if and only if p^2 divides Δ.

To sum up, for $a_1 \in \mathbb{Z}$ such that $f(a_1) \in p\mathbb{Z}$, the following conditions are equivalent:

- $f(X) \notin (p, X - a_1)^2$,
- $f(a_1) \notin p^2\mathbb{Z}$ or $f'(a_1) \notin p\mathbb{Z}$,
- either $\overline{a}_1$ is not a multiple zero of $\bar{f}(X)$ in $\mathbb{F}_p[X]$ or $\overline{a}_1$ is a multiple zero of $\bar{f}(X)$ in $\mathbb{F}_p[X]$ (and, in this case, p divides Δ) and $f(a_1) \notin p^2\mathbb{Z}$,
- either $\overline{a}_1$ is not a multiple zero of $\bar{f}(X)$ in $\mathbb{F}_p[X]$ or p divides Δ and

  – if $p = 2, 3$ or divides both a and b, then p^2 does not divide $(a-b)^3 + a(a-b) + b$,

  – for all other p dividing Δ, then p^2 does not divide Δ.

Thus the result is gotten.

REMARK. – We have shown, under suitable assumptions (Δ is coprime to 2, 3, a and b), a noteworthy converse to the well known result: if the discriminant of an integral ring extension A of $\mathbb{Z}$ is square-free, then A is integrally closed (see for instance [9, 5.3, Proposition 1]). Let α be an algebraic integer with minimal polynomial $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$.

If the discriminant Δ of $f(X)$ is coprime to 2, 3, a and b and $\mathbb{Z}[\alpha]$ is integrally closed, then Δ is square-free.

EXAMPLE. – Let α be an algebraic integer with minimal polynomial $X^3 + 2X + 2$ (an irreducible polynomial by Eisenstein's criterion). Here $a = b = 2$, so $\Delta = -140 = -7 \times 5 \times 4$. Then, 25 and 49 does not divide Δ, 2 divides Δ, but 4 does not divide $(a-b)^3 + a(a-b) + b = 2$. So, $\mathbb{Z}[\alpha]$ is integrally closed although 4 divides Δ.

PROPOSITION 5.2. – *Let α be an algebraic integer with minimal polynomial*

$$f(X) = X^3 + aX + b \in \mathbb{Z}[X].$$

Then, $\mathbb{Z}[\alpha]$ is t-closed if and only if for each prime integer p dividing the discriminant $\Delta = -(4a^3 + 27b^2)$ of $f(X)$, conditions (1) *and* (2) *are verified:*

(1) *if $p \neq 2, 3$, does not divide both a and b and if p^2 divides Δ, we have Δp^{-2} is not a quadratic residue mod* (p).

(2) *if $p = 2, 3$ or divides both a and b and if p^2 divides $f(a-b)$, then $p = 2$ and 8 divides neither $f(a-b)$ nor $2f'(a-b)$* (*or, equivalently* 4 *divides* $a+1$).

PROOF. – Let us assume that $\mathbb{Z}[\alpha]$ is not integrally closed. So, with the notations of 4.3, there must be a prime p and $f_i(X) \in \mathbb{Z}[X]$ such that $f(X) \in (p, f_i(X))^2$. According to the proof of 5.1, we must have $\deg \bar{f}_i(X) = 1$, so that $f_i(X) = X - a_1$ and $\bar{a}_1$ is a multiple root of $\bar{f}(X)$ in $\mathbb{F}_p[X]$.

As we get $f(X) = (X-a_1)^2(X + 2a_1) + (X - a_1)(3a_1^2 + a) + f(a_1)$, it follows from 4.3 that $\mathbb{Z}[\alpha]$ is t-closed if and only if, for each prime $p \in \mathbb{Z}$ and $f_i(X)$ for which $f(X) \in (p, f_i(X))^2$, we have:

– if $p \neq 2$, $[(a + 3a_1^2)^2 - 4(X + 2a_1)f(a_1)]p^{-2}$ is not a quadratic residue mod $(p, X - a_1)$ (‡),

– if $p = 2$, $a + 3a_1^2 \notin 4\mathbb{Z}$ and, for each $h(X) \in \mathbb{Z}[X]$, we get:

$$(a + 3a_1^2)^2[h^2(X) + h(X)] - (X + 2a_1)f(a_1) \notin 4(2, X - a_1) \text{ (‡‡)}.$$

For $p \neq 2$, condition (‡) is equivalent to:

$$\forall h(X) \in \mathbb{Z}[X], \quad (a + 3a_1^2)^2 - 12a_1 f(a_1) - p^2 h^2(X) \notin p^2(p, X - a_1).$$

But, we can write $h(X) = (X - a_1)\, g(X) + k,\ k \in \mathbb{Z}$. So, we have

$$(\ddagger) \Leftrightarrow \forall k \in \mathbb{Z}, (a + 3a_1^2)^2 - 12a_1(a_1^3 + aa_1 + b) - k^2p^2 \notin p^3\mathbb{Z}$$

$$\Leftrightarrow \forall k \in \mathbb{Z},\ a^2 - 3a_1^4 - 6aa_1^2 - 12a_1 b - k^2p^2 \notin p^3\mathbb{Z}\,.$$

As p^2 divides Δ, we can write $\Delta = -(4a^3 + 27b^2) = -rp^2$, with $r \in \mathbb{Z}$, and $2aa_1 + 3b = sp$, with $s \in \mathbb{Z}$, since a_1 is such that $\overline{2aa_1 + 3b} = \overline{0}$ in $\mathbb{F}_p$.

Moreover, if $p \neq 3$ and does not divide a and b, we get then:

$$(\ddagger) \Leftrightarrow \forall k \in \mathbb{Z},\ 16a^4(a^2 - 3a_1^4 - 6aa_1^2 - 12a_1 b - k^2p^2) \notin p^3\mathbb{Z}$$

$$\Leftrightarrow \forall k \in \mathbb{Z},\ 16a^6 - 3(sp - 3b)^4 - 24a^3(sp - 3b)^2 - 96a^3b(sp - 3b) - 16a^4k^2p^2 \notin p^3\mathbb{Z}$$

$$\Leftrightarrow \forall k \in \mathbb{Z}, (4a^3 + 27b^2)(-6s^2p^2 + 12spb + 4a^3 - 9b^2) - 16a^4k^2p^2 \notin p^3\mathbb{Z}$$

$$\Leftrightarrow \forall k \in \mathbb{Z},\ r(4a^3 - 9b^2) - k^2 \notin p\mathbb{Z}, \quad \text{since } \overline{4a^2} \text{ is invertible in } \mathbb{F}_p$$

$$\Leftrightarrow \forall k \in \mathbb{Z},\ -36b^2r - k^2 \notin p\mathbb{Z} \text{ since } 4a^3 + 27b^2 \in p\mathbb{Z}$$

$$\Leftrightarrow \forall k \in \mathbb{Z},\ -r - k^2 \notin p\mathbb{Z} \text{ since } \overline{6b} \text{ is invertible in } \mathbb{F}_p\,.$$

So $(\ddagger)$ is equivalent to $-(4a^3 + 27b^2)p^{-2} = \Delta p^{-2}$ is not a quadratic residue modulo p.

If $p = 3$, we know that 9 divides $f(a_1)$ so that $12a_1(a_1^3 + aa_1 + b) \in 27\mathbb{Z}$.

In the same way, if p divides both a and b, we obtain that p^2 divides $f(a_1)$ and we have seen in 5.1 that we can choose $a_1 = 0$.

In these two cases, $(\ddagger)$ is equivalent to $(a + 3a_1^2)^2p^{-2}$ is not a quadratic residue mod (p), a contradiction. So, we cannot have $p = 3$ or p divides both a and b.

If $p = 2$, the same argumentation for $h(X)$ shows that condition $(\ddagger\ddagger)$ is equivalent to: for each $k \in \mathbb{Z}$, $(a + 3a_1^2)^2(k^2 + k) - 3a_1 f(a_1) \notin 8\mathbb{Z}$ and $a + 3a_1^2 \notin 4\mathbb{Z}$. But, since 2 divides $a + 3a_1^2$ and $k^2 + k$ for each $k \in \mathbb{Z}$, condition $(\ddagger\ddagger)$ is equivalent to $a_1 f(a_1)$ and $2f'(a_1) \notin 8\mathbb{Z}$. Furthermore, we have only to consider the case where $f(X) \in (2, X - a_1)^2$, which, by the proof of 5.1, is equivalent to 2 divides Δ and 4 divides $f(a_1)$. So, it implies that a is odd, 4 divides $a + 1$, and $a_1 f(a_1) \notin 8\mathbb{Z}$ is then equivalent to $(a - b)^3 + a(a - b) + b \notin 8\mathbb{Z}$. Conversely, this last condition, combined with 4 divides $a + 1$ implies $(\ddagger\ddagger)$ and the proof of the proposition is done.

Example. – Consider $f(X) = X^3 + 8X + 1$. Since $\bar{f}(X)$ has no zero in $\mathbb{F}_3$, we get that $f(X)$ is irreducible in $\mathbb{Z}[X]$. Let α be a zero of $f(X)$ and consider $\mathbb{Z}[\alpha]$. The discriminant of $f(X)$ is $\Delta = -(2048 + 27) = -2075 = -25 \times 83$. By 5.1, we get that $\mathbb{Z}[\alpha]$ is not integrally closed. The only prime p such that p^2 divides Δ

is 5, and $5 \neq 3, 2$, divides neither 8 nor 1. As we have $-(4a^3+27b^2)5^{-2} = -83 \equiv 2 \bmod (5)$ and as 2 is not a quadratic residue modulo 5, then $\mathbb{Z}[\alpha]$ is t-closed.

PROPOSITION 5.3. – *Let α be an algebraic integer with minimal polynomial*

$$f(X) = X^3 + aX + b \in \mathbb{Z}[X].$$

Then, $\mathbb{Z}[\alpha]$ is seminormal if and only if for each prime integer p dividing the discriminant $\Delta = -(4a^3+27b^2)$ of $f(X)$, conditions (1) *and* (2) *are verified*:

(1) *if $p \neq 2, 3$, does not divide both a and b and if p^2 divides the discriminant Δ, we have that p^3 does not divide Δ.*

(2) *if $p = 2, 3$ or divides both a and b and if p^2 divides $f(a-b)$, then $f'(a-b) \notin p^2\mathbb{Z}$.*

PROOF. – Let us assume that $\mathbb{Z}[\alpha]$ is not integrally closed. So, with the notations of 3.2, there must be a prime $p \in \mathbb{Z}$ and $f_i(X) \in \mathbb{Z}[X]$ such that $f(X) \in (p, f_i(X))^2$. According to the proof of 5.1, we must have $\deg \bar{f}_i(X) = 1$, so that $f_i(X) = X - a_1$ and $\bar{a}_1$ is a multiple root of $\bar{f}(X)$ in $\mathbb{F}_p[X]$.

As we get $f(X) = (X-a_1)^2(X+2a_1) + (X-a_1)(3a_1^2+a) + f(a_1)$, the following conditions are equivalent:

- $\mathbb{Z}[\alpha]$ is seminormal,

- according to 3.2, for each prime integer p and each $f_i(X) \in \mathbb{Z}[X]$ for which $f(X) \in (p, f_i(X))^2$, we have $b^2(X) - 4a(X)\,c(X) \notin p^2(p, f_i(X))$,

- for each prime integer p and $a_1 \in \mathbb{Z}$ for which $f(X) \in (p, X-a_1)^2$, we have $(a+3a_1^2)^2 - 4(X+2a_1)f(a_1) \notin p^2(p, X-a_1)$,

- p^3 does not divide $(a+3a_1^2)^2 - 12a_1(a_1^3+aa_1+b)$ for each prime integer p and $a_1 \in \mathbb{Z}$ for which $f(X) \in (p, X-a_1)^2$, that is such that p divides Δ.

Consider a prime integer p dividing Δ.

– if $p \neq 2, 3$, does not divide both a and b and is such that p^2 divides Δ, we get: p^3 does not divide $(a+3a_1^2)^2 - 12a_1(a_1^3+aa_1+b)$ if and only if p^3 does not divide $16a^4[(a+3a_1^2)^2 - 12a_1(a_1^3+aa_1+b)]$ if and only if $(4a^3 - 9b^2)(4a^3+27b^2) \notin p^3\mathbb{Z}$ by using notation and calculation of 5.2.

But $4a^3 - 9b^2 = (4a^3 + 27b^2) - 36b^2$ and $4a^3 + 27b^2 \in p^2\mathbb{Z}$. So, the following conditions are equivalent:

- $(4a^3 - 9b^2)(4a^3 + 27b^2) \notin p^3\mathbb{Z}$,
- $-36b^2(4a^3 + 27b^2) \notin p^3\mathbb{Z}$,
- $4a^3 + 27b^2 \notin p^3\mathbb{Z}$, since $p \neq 2, 3$ and does not divide b.

Thus we obtain (1).

– if $p = 2, 3$ or divides both a and b, we have seen in 5.1 that we can choose $a_1 = a - b$. In any case, p^2 divides $f(a_1)$, and, if $p = 2, 3$ or divides both a and b, then p^3 divides $12a_1 f(a_1)$; then p^3 does not divide $(a + 3a_1^2)^2 - 12a_1(a_1^3 + aa_1 + b)$ is equivalent to p^3 does not divide $(a + 3a_1^2)^2$, which is equivalent to p^2 does not divide $a + 3a_1^2 = a + 3(a - b)^2$.

EXAMPLE. – Consider $f(X) = X^3 + 2X + 4$. As $\bar{f}(X)$ has no zero in $\mathbb{F}_5$, $f(X)$ is irreducible in $\mathbb{Z}[X]$. Let α be a zero of $f(X)$ and consider $\mathbb{Z}[\alpha]$. The discriminant of $f(X)$ is $\Delta = -(32 + 27 \times 16) = -16 \times 29$. So, $p = 2$ is the only prime such that p^2 divides Δ. Here, 8 divides $f(a - b) = -8$; thus $\mathbb{Z}[\alpha]$ is not t-closed by 5.2 . But, $f'(a - b) = 14 \notin 4\mathbb{Z}$, so $\mathbb{Z}[\alpha]$ is seminormal.

REMARKS. – (1) When $a = 0$, we recover the results obtained by H. Tanimoto for $\mathbb{Z}[\sqrt[n]{m}]$ to be normal, seminormal and quasinormal when $n = 3$ [11].

(2) In this section, we did not study the situation for a ring $R[\alpha]$, where R is a Dedekind domain and α is an element of some integral domain which contains R where α is integral over R. Indeed, for $R = \mathbb{Z}$, special cases where p is a prime integer dividing the discriminant such that $p = 2, 3$ or divides both a and b imply: $\overline{a_1} = \overline{a - b}$ is a common zero of $\bar{f}(X)$ and $\bar{f}'(X)$ in $\mathbb{F}_p[X]$, which may no longer be verified when taking another Dedekind domain R. Hence we cannot give an explicit expression of a_1 when $R \neq \mathbb{Z}$.

REFERENCES

[1] T. ALBU, *On a paper of Uchida concerning simple finite extensions of Dedekind domains*, Osaka J. Math., **16** (1979), 65-69.
[2] D. F. ANDERSON - D. E. DOBBS - J. A. HUCKABA, *On seminormal overrings*, Comm. Algebra, **10** (1982), 1421-1448.
[3] D. E. DOBBS - M. FONTANA, *Seminormal rings generated by algebraic integers*, Matematika, **34** (1987), 141-154.
[4] D. FERRAND - J. P. OLIVIER, *Homomorphismes minimaux d'anneaux*, J. Algebra, **16** (1970), 461-471.

[5] G. MAURY, *La condition «intégralement clos» dans quelques structures algébriques*, Ann. Sci. Ecole Norm. Sup., **78** (1961), 31-100.
[6] G. PICAVET - M. PICAVET-L'HERMITTE, *Morphismes t-clos*, Comm. Algebra, **21** (1993), 179-219.
[7] G. PICAVET - M. PICAVET-L'HERMITTE, *Anneaux t-clos*, Comm. Algebra, **23** (1995), 2643-2677.
[8] M. PICAVET-L'HERMITTE, *Decomposition of order morphisms into minimal morphisms*, Math. J. Toyama Univ., **19** (1996), 17-45.
[9] P. SAMUEL, *Théorie Algébrique des Nombres* (Hermann, Paris) 1967.
[10] R. G. SWAN, *On seminormality*, J. Algebra, **67** (1980), 210-229.
[11] H. TANIMOTO, *Normality, seminormality and quasinormality of* $\mathbb{Z}[\sqrt[n]{m}]$, Hiroshima Math. J., **17** (1987), 29-40.
[12] K. UCHIDA, *When is* $\mathbb{Z}[\alpha]$ *the ring of the integers?*, Osaka J. Math., **14** (1977), 155-157.

Laboratoire de Mathématiques Pures, Université Blaise Pascal (Clermont II)
63177 Aubière Cedex, France
e-mail: picavet@ucfma.univ-bpclermont.fr

Pervenuta in Redazione
il 6 maggio 1997