COMPUTATION OF AN INTEGRAL BASIS OF QUARTIC NUMBER FIELD

L. EL FADIL

ABSTRACT. In this paper, for each prime integer p, a p-integral basis of a quartic number field K defined by an irreducible polynomial $P(X) = X^4+aX+b \in \mathbb{Z}[X]$ is given. The discriminant d_K of K and an integral basis of K are then obtained from its p-integral bases.

INTRODUCTION

Let K be a quartic number field defined by an irreducible polynomial $P(X) = X^4 + aX + b \in \mathbb{Z}[X]$, α a complex root of P, $\mathbb{Z}_K$ the ring of integers of K, d_K its discriminant and $ind(P) = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ the index of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. It is well known that: $\triangle = N_{K/\mathbb{Q}}(P')(\alpha)$ and $\triangle = (ind(P))^2 d_K$, where $\triangle$ is the discriminant of P and we can assume that for every prime p, $v_p(a) \leq 2$ or $v_p(b) \leq 3$.
Let p be a prime integer. A p-integral basis of K is a set of integral elements $\{w_1, ..., w_4\}$ such that p does not divide the index $[\mathbb{Z}_K : \Lambda]$, where $\Lambda = \sum_{i=1}^{4} \mathbb{Z}w_i$. In that case, we said that Λ is a p-maximal order of K. A triangular p-integral basis of K is a p-integral basis of K $\{1, w_2, w_3, w_4\}$ such that $w_1 = \frac{\alpha+x_1}{p^{r_1}}$, $w_2 = \frac{\alpha^2+y_2\alpha+x_2}{p^{r_2}}$ and $w_3 = \frac{\alpha^3+z_3\alpha^2+y_3\alpha+x_3}{p^{r_3}}$. In Theorem 1.1, for every prime p, a triangular p-integral basis of K is given.

For every prime p and $(x, m) \in \mathbb{Z}^2$, denote $x_p = \frac{x}{p^{v_p(x)}}$ and $x[m]$: the remainder of the Euclidean division of x by m.

In this paper, for each prime integer p, a triangular p-integral basis of a quartic number field K is given. The discriminant d_K of K and a triangular integral basis of K are then obtained from its triangular p-integral bases. These results extend those of Alaca and Williams [1], where they did not achieved the case that: ($v_2(a) = 2$ and $b = 3[4]$). However, the methods are different, ours being based on Newton's polygon techniques. The results are complete without no exception.

Key words and phrases. p-integral basis, Newton polygon.

Newton polygon

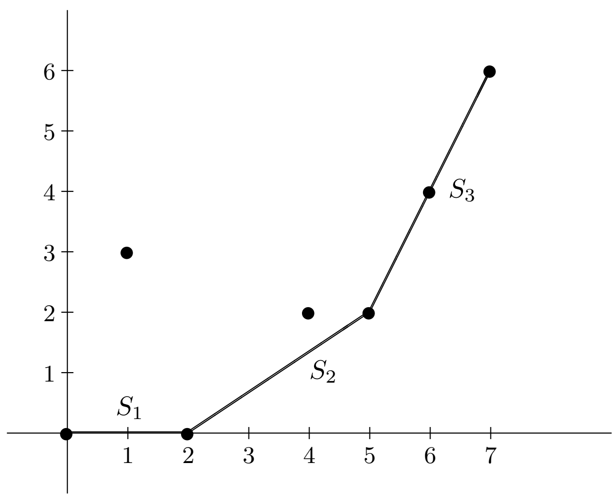
Let p be a prime integer such that p^2 divides $\triangle$ and $\phi(X)$ is an irreducible divisor of $P(X)$ modulo p. Set $m = deg\,(\phi(X))$ and let

$$P(X) = a_0(X)\phi(X)^t + a_1(X)\phi(X)^{t-1} + \cdots + a_t(X),$$

be the $\phi(X)$-adic development of $P(X)$ (every $a_i(X) \in \mathbb{Z}[X]$ and $\deg a_i(X) < m$). To any coefficient $a_i(X)$ we attach the integer $u_i = v_p(a_i(X))$ and the point of the plane $P_i = (i, u_i)$, if $u_i < \infty$.

The ϕ-Newton polygon of $P(X)$ is the lower convex envelope of the set of points $P_i = (i, u_i)$, $u_i < \infty$, in the cartesian plane. This (open) polygon is denoted by $N_\phi(P)$.

For instance, for a ϕ-development of degree 7 with $u_i = 0$, 3, 0, ∞, 2, 2, 4, 6 for $i = 0, 1, \dots, 7$, the polygon is let N be the $\phi(X)$-Newton polygon of $P(X)$.



The *length* $\ell(N_\phi(P))$ and the *height* $h(N_\phi(P))$ of the polygon are the respective lengths of the projection to the horizontal and vertical axis. Clearly, $\deg P(X) = m\ell(N_\phi(P)) + \deg a_0(X)$, where $m = deg\,\phi$.
The ϕ-Newton polygon is the union of different adjacent *sides* $S_1, \dots, S_t$ with increasing slope $\lambda_1 < \lambda_2 < \cdots < \lambda_t$. We shall write $N_\phi(P) = S_1 + \cdots + S_t$. The points joining two different sides are called the *vertexs* of the polygon. The polygon determined by the sides of positive slopes of $N_\phi(P)$ is called the *principal ϕ-polygon* of $P(X)$ and denoted by $N_\phi^+(P)$. The length and the height of $N_\phi^+(P)$ are the respective lengths of the projection to the horizontal and vertical axis.

For instance, the polygon of the figure has three sides S_1, S_2, S_3 with slopes $0 < 2/3 < 2$ and $N_\phi^+(P) = S_2 + S_3$. For every side S of the principal part $N_\phi^+(P)$, the *length* $\ell(S)$ and the *height* $h(S)$, of S, are the respective lengths of the projection to the horizontal and vertical axis. The *slope* of S is the quotient $h(S)/\ell(S)$. The positive integer $d(S) := \gcd(h(S), \ell(S))$ is called the *degree* of S. Denote $d := d(S)$ the degree of S, $h := h(S)/d$ and $e := \ell(S)/d$ positive coprime integers such that h/e is the slope of S. Let $s = \lfloor \frac{n}{m} \rfloor$ be the integral part of $\frac{n}{m}$, where $n = deg\,(P)$ and $m = deg\,(\phi)$. For every $1 \le j \le s$, let H_j be the length of the projection of $P_j(j, u_j)$ to the horizontal axis, h_j its integral part and $t_j = \text{red}\left(\dfrac{a_j(X)}{p^{h_j}}\right)$, where *red* is the canonical map defined on $\mathbb{Z}[X]$ by reduction modulo p. If $P_j \notin S$, then $t_j = 0$ and if $P_j \in S$, then $t_j \neq= 0$. If i is the abscissa of the initial point of S, let $P_S(Y)$ be the *residual polynomial* attached to S:

$$P_S(Y) := t_i Y^d + t_{i+e} Y^{d-1} + \cdots + t_{i+(d-1)e} Y + t_{i+de} \in \mathbb{F}_\phi[Y].$$

Let $ind_N(P) := \sum_{j=1}^{s} h_j$ the number of points with integer coordinates that lie below the polygon N, strictly above the horizontal axis and whose abscissas satisfy $1 \le j < l - 1$, where l is the length of N, $s = \lfloor \frac{n}{m} \rfloor$, $n = deg\,(P)$ and $m = deg\,(\phi)$.

Let $\bar{P}(X) = (\phi_1(X))^{l_1} P_2$ such that $\phi_1(X)$ does not divide $P_2(X)$ and $N_1^+ = S_1 + .. + S_s$ the principal part of $N_{\phi_1}(P)$. P is said to be ϕ_1-regular if for every $1 \le i \le s$, $P_{S_i}(Y)$ is square free. P is said to be p-regular if for every $1 \le i \le r$ and for every $1 \le j \le s_i$, $P_{S_j^i}(Y)$ is square free, where $\bar{P}(X) = \prod_{i=1}^{r} \phi_i(X))^{l_i}$ be the factorization of $\bar{P}(X)$ modulo p of irreducible polynomials and for every $1 \le i \le r$, $N_i = \oplus_j S_j^i$. The Theorem of index: $v_p(ind(P)) \ge \sum_{i=1}^{r} m_i ind_{N_i}(P)$, where $m_i = deg\,(\phi_i(X))$ for every i. With equality, if $P(X)$ is a p-regular polynomial. (cf. [4, p 326]).

1. p-integral basis of quartic number field defined by $X^4 + aX + b$

In this section, $K = \mathbb{Q}[\alpha]$, where α is a complex root of an irreducible trinomial $P(X) = X^4 + aX + b \in \mathbb{Z}[X]$ such that for every prime p, $v_p(a) \le 2$ or $v_p(b) \le 3$.

Lemma 1.1. *Let p be a prime integer and $w = \frac{t\alpha^3 + z\alpha^2 + y\alpha + x}{p^i} \in K$. Then $ch_w = X^4 + \frac{A_3}{p^i} X^3 + \frac{A_2}{p^{2i}} X^2 + \frac{A_1}{p^{3i}} X + \frac{A_0}{p^{4i}}$ is the characteristic polynomial of l_w the endomorphism of K defined by $l_w(x) = wx$, where*

$A_0 = x^4 + 3ax^2yz + 2bx^2z^2 - axy^3 - 4bxy^2z - 3ax^3t + by^4 + b^2z^4 + b^3t^4 + 3a^2x^2t^2 - 3a^2xyzt + a^2xz^3 - 5abxyt^2 + abxz^2t + 4b^2xzt^2 - a^3xt^3 + 4bx^2yt + 3aby^2zt + 2b^2y^2t^2 - abyz^3 - 4b^2yz^2t + a^2byt^3 - ab^2zt^3$,

$A_1 = -(4x^3 - 9ax^2t + 4bxz^2 + 8bxyt + 6axyz + 6a^2xt^2 - ay^3 - 4by^2z - 3a^2yzt + a^2z^3 - 5abyt^2 + abz^2t + 4b^2zt^2 - a^3t^3)$,

$A_2 = 6x^2 - 9axt + 3ayz + 4byt + 2bz^2 + 3a^2t^2$ *and* $A_3 = -4x + 3at$.

In particular, w is integral if and only if for every $1 \le j \le 3$, $\frac{A_j}{p^{ji}} \in \mathbb{Z}$.

The following theorem is an improvement and a specialization of the theorem of index on quartic number fields.

Theorem 1.2. *Let $P(X) = X^4 + mX^3 + nX^2 + aX + b \in \mathbb{Z}[X]$ be an irreducible polynomial such that for every prime p, $v_p(m) = 0$ or $v_p(n) \le 1$ or $v_p(a) \le 2$ or $v_p(b) \le 3$. Let p be a prime integer. If $P(X)$ is a p-regular polynomial, then we have the following:*

1. *If $\bar{P}(X)$ is square free, then $(1, \alpha, \alpha^2, \alpha^3)$ is a p-integral basis of $\mathbb{Z}_K$.*
2. *If $\bar{P}(X) = (\phi(X))^4$, where $\deg \phi = 1$, then $(1, \alpha, \frac{\alpha^2+a_3\alpha}{p^{h_2}}, \frac{\alpha^3+a_3\alpha^2+a_2\alpha}{p^{h_3}})$ is a p-integral basis of $\mathbb{Z}_K$, where $P(X) = \sum_{i=0}^4 a_i\phi^i$ is the ϕ_1-adic development of $P(X)$.*
3. *If $\bar{P}(X) = (\phi(X))^3 P_2$, where $\deg \phi = 1$ and $\phi(X)$ does not divide $P_2(X)$, then $(1, \alpha, \frac{\alpha^2+a_3\alpha}{p^{h_2}}, \frac{\alpha^3+a_3\alpha^2+a_2\alpha}{p^{h_3}})$ is a p-integral basis of $\mathbb{Z}_K$, where $P(X) = \sum_{i=0}^4 a_i\phi^i$ is the ϕ-adic development of $P(X)$.*
4. *If $\bar{P}(X) = (\phi(X))^2 P_2$, where $\deg \phi_1 = 1$, $\phi(X)$ does not divide $P_2(X)$ and $P_2(X)$ is square free, then $(1, \alpha, \frac{\alpha^2+a_3\alpha}{p^{h_2}}, \frac{\alpha^3+a_3\alpha^2+a_2\alpha}{p^{h_3}})$ is a p-integral basis of $\mathbb{Z}_K$, where $P(X) = \sum_{i=0}^4 a_i\phi^i$ is the ϕ-adic development of $P(X)$.*
5. *If $\bar{P}(X) = (\phi_1(X))^2(\phi_2(X))^2$, where $\deg \phi_i = 1$ and $\phi_1(X)$ does not divide $\phi_2(X)$, then for every i, let $P(X) = \sum_{j=0}^4 a_{i,j}\phi_i^j$ be the ϕ_i-adic development of $P(X)$, $w_i \frac{\alpha^3+a_{i,3}\alpha^2+a_{i,2}\alpha}{p^{h_3^i}}$ and $h_3^i \le h_3^j$. Then:*
   - (a) *If $h_3^i = 0$, then $(1, \alpha, \alpha^2, w_j)$ is a p-integral basis of $\mathbb{Z}_K$.*
   - (b) *If $h_3^i \ge 1$, then $(1, \alpha, w_i - p^{h_3^j - h_3^i} w_j, w_j)$ is a p-integral basis of $\mathbb{Z}_K$.*
6. *If $\bar{P}(X) = (\phi(X))^2$, where $\phi(X)$ is irreducible of degree 2, then $(1, \alpha, \frac{\phi(\alpha)}{p^h}, \frac{\alpha\phi(\alpha)}{p^h})$ is a p-integral basis of $\mathbb{Z}_K$, where $P(X) = \phi^2 + A(X)\phi + B(X)$ is the $\phi(X)$-adic development of $P(X)$ and h is the little of $(v_p(A(X)), \lfloor \frac{v_p(B(X))}{2} \rfloor)$.*

Proof.

1. Case 1. By Dedekind criterion, since $\bar{P}$ is square free, then $(1, \alpha, \alpha^2, \alpha^3)$ is a p-integral basis of $\mathbb{Z}_K$.
2. Cases 2, 3, 4. By theorem of index it suffices to show that every $w_i \in \mathbb{Z}_K$, where $w_2 = \frac{\alpha^2+a_3\alpha}{p^{h_2}}$ and $w_3 = \frac{\alpha^3+a_3\alpha^2+a_2\alpha}{p^{h_3}}$. Let $\phi(X) = X - x_0$. By replacing $P(X)$ by $P(X + x_0)$, we can assume that $x_0 = 0$, and then $w_2 = \frac{\alpha^2+m\theta}{p^{h_2}}$ and $w_3 = \frac{\alpha^3+m\alpha^2+n\alpha}{p^{h_3}}$. Let $Ch_{w_2}(X) = X^4 + \frac{2n}{p^{h_2}}X^3 + \frac{(n^2+2b+am)}{p^{2h_2}}X^2 + \frac{(amn+bm^2-a^2+2bn)}{p^{3h_2}}X + \frac{(bm^2n-abm+b^2)}{p^{4h_2}}$ and $Ch_{w_2}(X) = X^4 + \frac{3a}{p^{h_3}}X^3 +$

$\frac{(bn+3a^2)}{p^{2h_3}}X^2 + \frac{(a^3+2abn-b^2m)}{p^{3h_3}}X + \frac{(b^3+a^2bn-ab^2m)}{p^{4h_3}}$ be the respective characteristic polynomial of l_{w_2} and l_{w_3}, where l_w is the endomorphism of K defined by the multiplication by w. By definition of h_2, p^{h_2} divides n. Since $N_\phi(P)$ is convex, then $v_p(b) \geq 3h_2$ and $v_p(a) \geq 2h_2$. Thus, $Ch_{w_2} \in \mathbb{Z}[X]$, and then $w_2 \in \mathbb{Z}$. For w_3, by definition of h_3, p^{h_3} divides a. Since $N_\phi(P)$ is convex, then $v_p(b) \geq h_3+(h_3-h_1) \geq h_3+(h_3-h_2)$, and then $v_p(b)+v_p(n) \geq 2h_3$, $3v_p(b) \geq 4h_3$ and $2v_p(b)+v_p(m) \geq 3h_3$. Thus, $Ch_{w_3} \in \mathbb{Z}[X]$ and $w_3 \in \mathbb{Z}$.

(3) Case 5. As in the previous cases, every $w_k \in \mathbb{Z}_K$. By Hensel lemma, let $(P_1, P_2) \in \mathbb{Z}_p[X]^2$ such that $P_1P_2 = P$ and $\bar{P}_k = \phi_k^2$. Since $\bar{P}_1$ and $\bar{P}_2$ are cooprime, then $v_p(ind(P)) = v_p(ind(P_1)) + v_p(ind(P_2))$ (cf. MN). Since P is p-regular, then for every k, $v_p(ind(P_k)) = h_3^k$. Thus, If $h_3^i = 0$, then $(1, \alpha, \alpha^2, w_j)$ is a p-integral basis of $\mathbb{Z}_K$. Else, then for every k, let $\phi_k = X - x_k$. Then $a_{k,3} = 4x_k + m$. Since $x_1 \neq x_2$ modulo p, then $a_{1,3} \neq a_{2,3}$ modulo p, and then $w_i - p^{h_3^j - h_3^i}w_j = \frac{U(\alpha)}{p^{h_3^i}}$, where $U(X) \in \mathbb{Z}[X]$ of degree 2 such that the coefficient of X^2 is cooprime to p. Finally, $(1, \alpha, w_i - p^{h_3^j-h_3^i}w_j, w_j)$ is a p-integral basis of $\mathbb{Z}_K$.

(4) Case 6. By Theorem of index it suffices to show that every $\phi(\alpha) \in \mathbb{Z}_K$. Let $P(X) = \phi^2 + A(X)\phi + B(X)$ be the $\phi(X)$-adic development of $P(X)$ and $k = v_p(\phi(\alpha))$. Since $P(\alpha) = 0$, then $2v_p(\phi(\alpha)) \geq v_p(B(\alpha))$, and then $k \geq h$. Thus, $\frac{\phi(\alpha)}{p^h} \in \mathbb{Z}_K$.

The following Theorem gives us a triangular p-integral basis of K, $v_p(\triangle)$ and $v_p(d_K)$ for every prime integer p.

Theorem 1.3. *Let $p \geq 5$ be a prime integer. Under the above hypotheses, a p-integral (resp. a 2-integral, resp. a 3-integral) basis of $\mathbb{Z}_K$ is given in table A (resp. table B, B2*, B3* and B.3.2, resp. table C)*

Table A

case	$v_p(b)$	$v_p(a)$	$v_p(\triangle)$	*p-integral basis*	$v_p(d_K)$
A1	*3*	≥ 3	*9*	$(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p^2})$	*3*
A2	≥ 3	*2*	*8*	$(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p^2})$	*2*
A3	≥ 1	*0*	*0*	$(1, \alpha, \alpha^2, \alpha^3)$	*0*
A4	*2*	≥ 2	*6*	$((1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p})$	*2*
A5	*1*	≥ 1	*3*	$(1, \alpha, \alpha^2, \alpha^3)$	*3*
A6	≥ 2	*1*	*4*	$((1, \alpha, \alpha^2, \frac{\alpha^3}{p})$	*2*
A7	*0*	≥ 1	*0*	$(1, \alpha, \alpha^2, \alpha^3)$	*0*
A8	*0*	*0*	*?*	$(1, \alpha, \alpha^2, \frac{\alpha^3+t\alpha^2+t^2\alpha-3t^3}{p^m})$	$v_p(\triangle)[2]$

In case A8, $t \in \mathbb{Z}$ such that $3at + 4b = 0$ modulo p^{m+1}, $m = \lfloor \frac{v_p(\triangle}{2} \rfloor$ and $v_p(\triangle)[2]$ is the remainder of the Euclidean division of $v_p(\triangle)$ by 2.

Table B

case	*conditions*	$v_2(\triangle)$	*2-integral basis*	$v_2(d_K)$
B1	$v_2(b) \geq 3,\ v_2(a) = 2$	*8*	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2})$	*2*
B2	$v_2(b) = 3, v_2(a) \geq 5$	*17*	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2})$	*11*
B3	$v_2(b) = 3,\ v_2(a) = 4$	*16*	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2})$	*10*
B4	$v_2(b) = 3,\ v_2(a) = 3$	*12*	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2})$	*6*
B5	$b = 4 + 16B,\ a = 16A, A = B[2]$	*14*	$(1, \alpha, \frac{\alpha^2+2\alpha+2}{2^2}, \frac{\alpha^3+2\alpha^2+(2+4B)\alpha}{2^3})$	*4*
B6	$b = 4 + 16B,\ a = 16A, A \neq B[2]$	*14*	$(1, \alpha, \frac{\alpha^2+2\alpha+2}{2^2}, \frac{\alpha^3+2\alpha^2+2\alpha}{2^2})$	*6*
B7	$v_2(b) = 2,\ v_2(a) = 3$	*12*	$(1, \alpha, \frac{\alpha^2+2}{4}, \frac{\alpha^3+2\alpha}{4})$	*6*
B8	$v_2(b) = 2,\ v_2(a) = 2$	*8*	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2})$	*4*
B9	$v_2(b) \geq 2,\ v_2(a) = 1$	*4*	$(1, \alpha, \alpha^2, \frac{\alpha^3}{2})$	*2*
B10	$v_2(b) = 1,\ v_2(a) \geq 3$	*11*	$(1, \alpha, \alpha^2, \alpha^3)$	*11*
B11	$v_2(b) = 1,\ v_2(a) = 2$	*8*	$(1, \alpha, \alpha^2, \alpha^3)$	*8*
B12	$v_2(b) = 1,\ v_2(a) = 1$	*4*	$(1, \alpha, \alpha^2, \alpha^3)$	*4*
B13	$v_2(a) = 0$	*0*	$(1, \alpha, \alpha^2, \alpha^3)$	*0*
B14	$v_2(a) \geq 3, b = 1\,[4]$	*8*	$(1, \alpha, \alpha^2, \alpha^3)$	*8*
B15	$v_2(a) \geq 3, b = 3\,[4]$	*8*	$(1, \alpha, \frac{\alpha^2+1}{2}, \frac{\alpha^3-\alpha^2+\alpha-1}{2})$	*4*
B16	$v_2(a) = 2, b = 1\,[4]$	*9*	$(1, \alpha, \alpha^2, \alpha^3)$	*9*
B17	$v_2(a) = 2, b = 7\,[8]$	*10*	$(1, \alpha, \frac{\alpha^2+1}{2}, \frac{\alpha^3-\alpha^2+\alpha-1}{2})$	*6*
B18	$v_2(a) = 1, b = 3\,[4]$	*4*	$(1, \alpha, \alpha^2, \alpha^3)$	*4*
B19	$v_2(a) = 1, b = 1\,[4]$	*4*	$(1, \alpha, \alpha^2, \frac{\alpha^3-\alpha^2+\alpha-1}{2})$	*2*
*B2**	$b = 3[4],\ v_2(a) = 2$	*	*cf table B2**	*

If $b = 3[4]$ and $v_2(a) = 2$, then let $A = 4 + a$, $B = 1 + a + b$. Consider $F(X) = P(X + 1) = X^4 + 4X^3 + 6X^2 + AX + B$ and $\theta = \alpha - 1$. Then

*Table B2**

conditions	$v_2(\triangle)$	*2-integral basis*	$v_2(d_K)$
$v_2(B)+1 \geq 2v_2(A)$	$5+2v_2(A)$	$(1, \alpha, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^m}),\ m=v_2(A)$	3
$v_2(B)+1 < 2v_2(A),\ v_2(\triangle)=0[2]$ $v_2(B)=2m$	$8+v_2(B)$	$(1, \alpha, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^m})$	6
$v_2(B)+1 < 2v_2(A),\ v_2(\triangle)=1[2]$ $v_2(B)=2m$	$5+2v_2(A)$	$(1, \alpha, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^m})$	5
$v_2(B)+1 < 2v_2(A),\ v_2(B)=1[2]$	*	*cf Table B3**	*

Table B3:* $v_2(B)+1 < 2v_2(A),\ v_2(B)=2k+1$

conditions	*2-integral basis*
$2v_2(A) > v_2(B)+1, v_2(d)=1$	$(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^{k+1}})$
$2v_2(A) > v_2(B)+1, v_2(d)\geq 2$	*go to* $B.3.2$

B.3.2: Assume that $v_2(d) \geq 2$*. Let* $t \in \mathbb{Z}$ *such that* $v_2(n_2t+A_2)=s$, $s_1 = L(\lfloor\frac{v_2(d)-1}{2}\rfloor, \lfloor\frac{k+2}{2}\rfloor)$ *and* $H(X)=F(X+2^kt)=X^4+m'X^3+n'X^2+A'X+B'$.

conditions	*2-integral basis*
$v_2(A)\geq k+3$	$s=1$, $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(-3.2^kt+4)\theta^2+6\theta-6.2^kt}{2^{k+1}})$
$v_2(A)=k+2, v_2(d)\geq 3$	$s=s_1$ $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(4-3.2^kt)\theta^2+(6-4.2^{k+1}t)\theta-6.2^kt}{2^{k+s_1+2}})$
$v_2(A)=k+2, v_2(d)=2, v_2(B')=2k+4$	$s=1$ $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(4-3.2^kt)\theta^2+6\theta-6.2^kt}{2^{k+2}})$
$v_2(A)=k+2, v_2(d)=2, v_2(B')=2k+3$	*Replace* F *and* θ *by* H *and* $\theta-2^kt$

Table C

case	*conditions*	$v_3(\triangle)$	*3-integral basis*	$v_p(d_K)$
C1	$v_3(b)\ge 4,\ v_3(a)=2$	*11*	$(1,\alpha,\frac{\alpha^2}{3},\frac{\alpha^3}{3^2})$	*5*
C2	$v_3(b)\ge 4,\ v_3(a)=1$	*7*	$(1,\alpha,\alpha^2,\frac{\alpha^3}{3})$	*5*
C3	$v_3(b)\ge 4, v_3(a)=0, a^2\ne 1[9]$	*3*	$(1,\alpha,\alpha^2,\alpha^3)$	*3*
C4	$v_3(b)\ge 4, v_3(a)=0, a^2=1[9]$	*3*	$(1,\alpha,\alpha^2,\frac{\alpha^3-a\alpha^2+\alpha}{3})$	*1*
C5	$v_3(b)=3,\ v_3(a)\ge 2,$	*9*	$(1,\alpha,\frac{\alpha^2}{3},\frac{\alpha^3}{3^2})$	*3*
C6	$v_3(b)=3,\ v_3(a)=1$	*7*	$(1,\alpha,\alpha^2,\frac{\alpha^3}{3})$	*5*
C7	$v_3(b)=3,\ a^2=1[9]$	*3*	$(1,\alpha,\alpha^2,\frac{\alpha^3-a\alpha^2+\alpha}{3})$	*1*
C8	$v_3(b)=3,\ v_3(a)=0, a^2\ne 1[9]$	*3*	$(1,\alpha,\alpha^2,\alpha^3)$	*3*
C9	$v_3(b)=2,\ v_3(a)\ge 2,$	*6*	$((1,\alpha,\frac{\alpha^2}{3},\frac{\alpha^3}{3})$	*2*
C10	$v_3(b)=2,\ v_3(a)=1$	*6*	$(1,\alpha,\alpha^2,\frac{\alpha^3}{3})$	*4*
C11	$v_3(b)=2,\ a^2=1[9]$	*3*	$(1,\alpha,\alpha^2,\frac{\alpha^3-a\alpha^2+\alpha}{3})$	*1*
C12	$v_3(b)=2,\ v_3(a)=0,\ a^2\ne 1[9]$	*3*	$(1,\alpha,\alpha^2,\alpha^3)$	*3*
C13	$v_3(b)=1,\ v_3(a)\ge 1,$	*3*	$(1,\alpha,\alpha^2,\alpha^3)$	*3*
C14	$b=6[9],\ v_3(a)=0,\ a^2\ne 4[9],$	*3*	$(1,\alpha,\alpha^2,\alpha^3)$	*3*
C15	$b=6[9],\ a^2=4[9],$	*3*	$(1,\alpha,\alpha^2,\frac{\alpha^3-a\alpha^2+\alpha+a}{3})$	*1*
C16	$b=3[9],\ v_3(a)=0,\ a^2\ne 7[9],$	*4*	$(1,\alpha,\alpha^2,\alpha^3)$	*4*
C17	$b=3[9], a^2=7[9],\ a^4-a^2+b=0[27]$	≥ 6	$(1,\alpha,\frac{\alpha^2-1}{3},\frac{\alpha^3+z\alpha^2+y\alpha+x}{3^m})$	$v_3(\triangle)[2]$
C18	$b=3[9], a^2=7[9],\ v_3(a^4-a^2+b)=2$	5	$(1,\alpha,\alpha^2,\frac{\alpha^3-a\alpha^2+\alpha+a}{3})$	3
C19	$v_3(b)=0$	0	$(1,\alpha,\alpha^2,\alpha^3)$	0

In case C17, x,y,z are defined as follows: $4x=3a\,[3^m]$, $a^2y=16b^2\,[3^m]$, $az+4b_3=0[3^m]$ and $m=\lfloor\frac{v_2(\triangle)-2}{2}\rfloor$.

Proof. First, $\triangle=2^8b^3-3^3a^4$ and the proof is based on the Newton polygon. For every prime p, let $u_3=v_p(a)$, $u_4=v_p(b)$, $\bar{P}(X)$ the reduction of P modulo p, N the X-Newton polygon of P and N^+ its principal part.

(1) Case 1: $(v_p(b)=3$ and $v_p(a)\ge 2)$: A1, B2, B3, B4, C5.

$$\bar{P}(X)=X^4 \text{ and } ind_N(P)=3.$$

1) If $u_3\ge 3$, then $N=S$ is one side and $P_S(Y)=Y+\overline{b_p}$ is square free and $(1,\alpha,\frac{\alpha^2}{p},\frac{\alpha^3}{p^2})$ is a p-integral basis of $\mathbb{Z}_K$.

2) If $u_3 = 2$, then $N = S_1 + S_2$ with slopes respectively $1/3$ and 1. $P_{S_1}(Y) = Y + \overline{a_p}$ and $P_{S_2}(Y) = \overline{a_p}Y + \overline{b_p}$ are square free. Thus, $(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p^2})$ is a p-integral basis of $\mathbb{Z}_K$.

(2) Case 2: ($v_p(b) \geq 2$ and $v_3(a) = 1$) : A6, B9, C2, C6, C10.

$N = S_1 + S_2$ with slopes respectively $1/3$ and 1. $P_{S_1}(Y)$ and $P_{S_2}(Y)$ are of degree 1. So, Thus, $(1, \alpha, \alpha^2, \frac{\alpha^3}{p})$ is a p-integral basis of $\mathbb{Z}_K$.

(3) Case 3: ($v_p(b) \geq 1$ and $v_3(a) = 0$): A3, B3, C3, C4, C7, C8, C11, C12, C14, C15, C16, C17,C18.
If $p \neq 3$, then $\bar{P}(X)$ is square free and then $v_p(ind(P)) = 0$.

For $p = 3$, let $F(X) = P(X - a) = X^4 - 4aX^3 + 6a^2X^2 + AX + B$, where $A = -a(4a^2 - 1)$ and $B = (a^4 - a^2 + b)$. Then $v_3(A) \geq 1$ and $v_3(B) \geq 1$. It follows that $v_3(ind(P)) = 0$ if and only if $v_3(B) = 1$, i.e., if ($a^2 = 1$ modulo 9 and $v_3(b) = 1$) or ($a^2 \neq 1$ modulo 9 and $v_3(b) \geq 2$, then $v_3(ind(P)) = 0$. Else, then $u_1 = 0$, $u_2 = 1$, $u_3 = v_3(A) \geq 1$ and $u_4 = v_3(B) \geq 2$.

(a) If $u_3 = 1$ or $u_4 = 2$, then $v_3(ind(P)) = 1$ and $(1, \alpha, \alpha^2, \frac{\alpha^3 - a\alpha^2 + \alpha + a}{3})$ is a 3-integral basis of $\mathbb{Z}_K$: ($b = 6$ and $a^2 = 4$ modulo 9) or ($b = 3$, $a^2 = 7$ modulo 9 and $v_3(a^4 - a^2 + b) = 2$).

(b) If $u_3 \geq 2$ and $u_4 \geq 3$:($b = 3$, $a^2 = 7$ modulo 9 and $a^4 - a^2 + b = 0$ modulo 27), then let $m = \lfloor \frac{v_2(\triangle)-2}{2} \rfloor$ and $(x, y, z) \in \mathbb{Z}_K$ defined by $4x = 3a\,[3^m]$, $a^2y = 16b_3^2\,[3^m]$, $az + 4b_3 = 0[3^m]$ as defined in Proof of B19 in [1]. Let $w = \frac{\alpha^3 + z\alpha^2 + y\alpha + x}{3^m}$; replacing the A_i as defined in Lemma 1.1, we have $A_3 = 0$ modulo 3^m, $A_2 = 0$ modulo 3^{2m}, $A_1 = 0$ modulo 3^{3m} and $A_0 = 0$ modulo 3^{4m}, and then $w \in \mathbb{Z}_K$. Finally, $(1, \alpha, \frac{\alpha^2 - 1}{3}, \frac{\alpha^3 + z\alpha^2 + y\alpha + x}{3^m})$ is a 3-integral basis of $\mathbb{Z}_K$.

(4) Case 4: ($v_p(b) = 2$ and $v_3(a) \geq 2$): A4, C9, B5, B6, B7, B8:

For $p \neq 2$, $N = S$ is one side and $P_S(Y) = Y^2 + \bar{b_p}$ is square free. Hence $v_p(ind(P)) = 2$
For $p = 2$, $N = S$ is one side and $P_S(Y) = (Y+1)^2$. Since $P(X)$ is not 2-regular, we will use a higher order. Let $t_1 = (X, 1/2, Y+1)$ and $\phi_2(X) = X^2+2$ as defined in[3], page 16 and let V_2 be the 2-adic valuation of 2^d-order as defined in[3], page 17. Then $V_2(\phi_2) = 2$, $V_2(X) = 1$ and for every $x \in \mathbb{Z}$, $V_2(x) = 2v_2(x)$. Let $P(X) = \phi_2^2(X) - 4\phi_2(X) + (4AX + 4b_2 + 4)$, $R_0 = V_2(\phi_2^2(X)) = 4$, $R_1 = V_2(4\phi_2(X)) = 6$ and $R_2 = V_2(4AX + 4b_2 + 4)$. From [3, Th 4.18, p:48], it follows that:

(a) If $v_2(a)=2$, then $R_2=5$ and $(1,\alpha,\frac{\alpha^2}{2},\frac{\alpha^3}{2})$ is a 2-integral basis of $\mathbb{Z}_K$.

(b) If $v_2(a)=3$, then $R_2=7$ and $(1,\alpha,\frac{\alpha^2}{2},\frac{\alpha^3+2\alpha}{4})$ is a 2-integral basis of $\mathbb{Z}_K$.

(c) If $b_2+1=0$ modulo 4 and $v_2(a)\geq 4$, then $R_2\geq 8$ and $(1,\alpha,\frac{\alpha^2+2}{4},\frac{\alpha^3+2\alpha}{4})$ is a 2-integral basis of $\mathbb{Z}_K$.

(d) If $b_2+1=2$ modulo 4 and $v_2(a)\geq 4$, then let $b=4+16B$, $a=16A$, $\phi_2(X)=X^2+2X+2t$ and $P(X)=\phi_2^2(X)-4(X+t-1)\phi_2(X)+8(t-1+2A)X+4(1+t^2+4B-2t)$. Then $R_0=4$ $R_1=7$. Since $1+t^2+4B-2t=2(1-t+2B)$ modulo 8, let $t\in\mathbb{Z}$ such that $1-t+2B=0$ modulo 4. It follows that: if $B=A$ modulo 2, then $R_2\geq 10$, $v_2(ind(P))=5$ and $(1,\alpha,\frac{\alpha^2+2\alpha+2}{4},\frac{\alpha^3+2\alpha^2+2(1+2B)\alpha}{2^3})$ is a 2-integral basis of $\mathbb{Z}_K$.

If $B\neq A$ modulo 2, then $R_2=9$, $v_2(ind(P))=4$ and $(1,\alpha,\frac{\alpha^2+2\alpha+2}{4},\frac{\alpha^3+2\alpha^2+2\alpha}{2^2})$ is a 2-integral basis of $\mathbb{Z}_K$.

(5) Case 5: $(v_p(b)=1$ and $v_3(a)\geq 1)$: A5, C13, B10,B11, B12.

$N=S$ is one side and $P_S(Y)=Y+\overline{b_p}$ is square free. Hence $v_p(ind(P))=0$. v

(6) Case 6: $v_p(b)\geq 3$ and $v_3(a)=2$: A2, C1, B1:

$N=S_1+S_2$ with slopes respectively $2/3$ and u_4-2. Since every $P_{S_i}(Y)$ is square free, then $v_p(ind(P))=3$.

(7) Case 7: $v_p(b)=0$ and $v_3(a)\geq 1$: A7, B14, B15,..., B19, B2*, B3* and C19.
If $p\neq 2$, then $\bar{P}(X)$ is square free.

For $p=2$, according to the Dedekind criterion, let $f(X)=\frac{P(X)-(X+1)^4}{2}=-2X^3-3X^2+\frac{a-4}{2}X+\frac{b-1}{2}$ and $f(-1)=1+\frac{a}{2}+\frac{b-1}{2}$. Thus,

If $(v_2(a)\geq 2$ and $b=1$ modulo 4) or $(v_2(a)=1$ and $b=3$ modulo 4), then $(1,\alpha,\alpha^2,\alpha^3)$ is a 2-integral basis of $\mathbb{Z}_K$.
Else, let $P(X+1)=X^4+4bX^3+6X^2+(4+a)X+(1+a+b)$. Then $u_1=2$, $u_2=1$ and

(a) If $v_2(a)=1$ and $b=1$ modulo 4, then $u_3=1$, $u_4\geq 2$ and $(1,\alpha,\alpha^2,\frac{\alpha^3-\alpha^2-\alpha-1}{2})$ is a 2-integral basis of $\mathbb{Z}_K$.

(b) If $(v_2(a)\geq 3$ and $b=3$ modulo 8) or $(v_2(a)=2$ and $b=7$ modulo 8), then $u_3=u_4=2$ and $N=S$ is one side such that $P_S(Y) = Y^2 + Y + 1$ is irreducible. Hence, $(1, \alpha, \frac{\alpha^2+1}{2}, \frac{\alpha^3-\alpha^2-\alpha-1}{2})$ is a 2-integral basis of $\mathbb{Z}_K$.

(c) If $v_2(a) = 2$ and $b = 3$ modulo 4, let $F(X) = P(X + 1) = X^4 + 4X^3 + 6X^2 + (4 + a)X + (1 + b + a) = X^4 + 4X^3 + 6X^2 + AX + B$, where $A = 4 + a$, $B = 1 + b + a$, $v_2(A) \geq 3$ and $v_2(B) \geq 3$. First, we have $\triangle = disc(F) = 256B^3 - 768B^2A + 768BA^2 + 176A^3 + 2304B^2 - 4608BA - 288A^2 - 27A^4 + 6912B$. Consequently,

(i) If $v_2(B) + 1 \geq 2v_2(A)$, then $v_2(\triangle) = 5 + 2v_2(A)$, $v_2(ind(P)) = 1 + v_2(A)$, $v_2(d_K) = 3$ and $(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3+4\alpha^2+6\alpha}{2^m})$ is a 2-integral basis of $\mathbb{Z}_K$, where $m = v_2(A)$.

(ii) If $v_2(B)$ is even and $v_2(B) + 1 < 2v_2(A)$, then

if $v_2(\triangle)$ is even, then $v_2(\triangle) = 8 + v_2(B)$, $v_2(ind(P)) = 1 + \lfloor \frac{v_2(B)}{2} \rfloor$, $v_2(d_K) = 6$ and $(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3+4\alpha^2+6\alpha)}{2^m})$ is a 2-integral basis of $\mathbb{Z}_K$, where $m = \lfloor \frac{v_2(B)}{2} \rfloor$.
If $v_2(\triangle)$ is odd, then $v_2(\triangle) = 5 + 2v_2(A)$, $v_2(ind(P)) = 1 + \lfloor \frac{v_2(B)}{2} \rfloor$, $(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3+4\alpha^2+6\alpha}{2^m})$ is a 2-integral basis of $\mathbb{Z}_K$, where $m = \lfloor \frac{v_2(B)}{2} \rfloor$. Since $v_2(\triangle) = 5 + 2v_2(A)$ and $v_2(B) + 1 < 2v_2(A)$, then $v_2(B) = 2v_2(A) - 2$. Thus, $v_2(d_K) = 3$.

(iii) $v_2(B)$ is odd and $v_2(B) + 1 < 2v_2(A)$. By the Theorem of the polygon $F(X) = H(X)G(X)$ in $\mathbb{Z}_2[X]$, where $H(X) = X^2 + rX + s$, $G(X) = X^2 + RX + S$,

$$\begin{cases} v_2(s) = 1, & v_2(S) = v_2(B) - 1, \\ v_2(r) \geq 1, & v_2(R) > \frac{v_2(B)-1}{2} \\ B = sR + rS, & A = Sr + Rs, \qquad 4 = r + R. \end{cases}$$

Since $4 = r + R$, $v_2(r) \geq 3$ and $v_2(r) = 2$. So, $v_2(disc(H)) = v_2(r^2 - 4s) = 3$, $v_2(Res(H, G)) = 2v_2(H(\theta)) = 2$, where θ is a root of $G(X)$. As $v_2(r) \geq 1$ and $v_2(s) = 1$, we have $H(X)$ is irreducible in $\mathbb{Z}_2[X]$. On the other hand, as $disc(F) = disc(H)\, disc(G)\, (Res(H, G))^2$,
$v_2(disc(F)) = v_2(disc(H)) + 2v_2(Res(H, G)) + v_2(disc(G)) = 7 + v_2(disc(G))$. Thus,

(A) If $G(X)$ is irreducible in $\mathbb{Z}_2[X]$, then from [4], $v_2(ind(F)) = 0 + 2 + v_2(ind(G))$. Let θ be a root of $G(X)$ and $u = \frac{\theta+x}{2^k} \in \mathbb{Q}_2[\theta]$. Since the characteristic polynomial of u is $Ch_u = X^2 - (\frac{2x-R}{2^k}X + \frac{(2x-R)^2+(disc(G))}{2^{2k+2}}$, where $disc(G) = 4S-$

R^2, then u is integral if and only if 2^{2k+2} divides $disc(G)$. Therefore, $v_2(ind(G)) = \lfloor \frac{v_2(disc(G))}{2} \rfloor - 1$. Thus, $v_2(ind(F)) = 2 + \lfloor \frac{v_2(disc(G))}{2} \rfloor - 1$, and then if $v_2(\triangle)$ is even, then $v_2(ind(F)) = \frac{v_2(disc(F))-6}{2}$ and $v_2(d_K)$=6. Else, then $v_2(ind(F)) = \frac{v_2(disc(F))-5}{2}$ and $v_2(d_K) = 5$.

(B) $G(X) = (X-\theta_1)(X-\theta_2)$ in $\mathbb{Z}_2[X]$, then $v_2(disc(G)) = 2v_2(\theta_1-\theta_2))$ and $v_2(disc(F)) = 7+2v_2((\theta_1-\theta_2))$. On the other hand, $v_2(ind(F)) = 2+v_2(Res(G_1,G_2) = 2+v_2((\theta_1-\theta_2))$. Hence $v_2(d_K) = 3$.

In these cases, $(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3+z\alpha^2+y\alpha^2+x}{2^m})$ is a 2-integral basis of $\mathbb{Z}_K$, where $m = \lfloor \frac{v_2(disc)-v_2(d_K)}{2} \rfloor - 1$, x, y and z are integers.

Since we can not compute the coefficients of $G(X)$ in $\mathbb{Q}_p$ neither to test if $G(X)$ is irreducible in $\mathbb{Q}_p[X]$, we must give, in $C.1$, a method which allows to compute the integers x, y and z independently of the knowledge of the irreducibility of $G(X)$.

(8) $C.1$: Let $F(X) = X^4+4X^3+6X^2+AX+B \in \mathbb{Z}[X]$, where $v_2(A) \geq 2$ and $v_2(B) \geq 3$. Let θ be a complex root of $F(X)$ and $d = A_2^2 - 3B_2$. It follows that:

(a) If $v_2(B)+1 \geq 2v_2(A)$, then $v_2(ind(F)) = r+1$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^r})$ is a 2-integral basis of $\mathbb{Z}_K$, where $r = v_2(B)$.

(b) If $v_2(B) \leq 2v_2(A)$ and $v_2(B)$ is even, then $v_2(ind(F)) = r+1$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^r})$ is a 2-integral basis of $\mathbb{Z}_K$, where $r = \lfloor \frac{v_2(B)}{2} \rfloor$.

(c) If $v_2(B) \leq 2v_2(A)$ and $v_2(B) = 2k+1$ is odd, then let $t \in \mathbb{Z}$ such that $v_2(3t+A_2) = s$, $H(X) = F(X+2^kt) = X^4+m_1X^3+n_1X^2+A_1X+B_1$, where $m_1 = 4+2^{k+2}t$, $n_1 = 6+3.2^{k+2}t+3.2^{2k+1}t^2$, $A_1 = A+3.2^{k+2}t+3.2^{2k+2}t^2+2^{3k+2}t^3$ and $B_1 = B+2^kAt+3.2^{2k+1}t^2+2^{3k+2}t^3+2^{4k}t^4$. Then $3^4B_1 = 2^{2k+1}(3^4B - 3^3A_2A + 3^3A_2^2 + 3^42^{3k+2}t^3 + 3^42^{4k}t^4 + 2^{2s}L) = -2^{2k+1}3^3d + 2^{3k+2}t^3 + 2^{4k}t^4 + 2^{2(s+k)+1}L$, where $L \in \mathbb{Z}$ is odd. Then $v_2(m_1) \geq 2$, $v_2(n_1) = 1$ and

(i) If $v_2(d) = 1$ or $k = 1$, then $v_2(B_1) = 2k+2$, $v_2(ind(F)) = k+2$, and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6\theta}{2^{k+1}})$ is a 2-integral basis of $\mathbb{Z}_K$.

(ii) If $v_2(d) \geq 2$, $k \geq 2$ and $v_2(A) > k+2$, then $v_2(A_1) = k+2$ and $v_2(B_1) \geq 2k+3$. Hence $v_2(ind(F)) = k+3$

and $(1, \theta, \frac{\theta^2}{2}, w_3)$ is a 2-integral basis of $\mathbb{Z}_K$, where $w_3 = \frac{\theta^3+(4-3.2^k t)\theta^2+6\theta-3.2^{k+1}t}{2^{k+2}}$.

(iii) If $v_2(A) = k+2$, $k \geq 2$ and $v_2(d) \geq 3$, then for $s = L(\lfloor \frac{v_2(d)-1}{2} \rfloor, \lfloor \frac{k}{2} \rfloor)$, $v_2(A_1) = k+2+s$, $v_2(B_1) \geq 2(k+s+1)+1$. Hence $v_2(ind(F)) = k+2+s$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(4-3.2^k t)\theta^2+6\theta-3.2^{k+1}t}{2^{k+1+s}})$ is a 2-integral basis of $\mathbb{Z}_K$.

(iv) If $v_2(A) = k+2$ and $v_2(d) = 2$, then for $s = 1$, $v_2(A_1) = k+3$ and $v_2(B_1) \geq 2(k+1)+1$. Thus,

If $v_2(B_1) = 2(k+1)+1$, then replace F and θ by H and $\theta - 2^k t$ and resume with $C.1$.

If $v_2(B_1) = 2(k+2)$, then $v_2(ind(F)) = k+3$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(4-3.2^k t)\theta^2+6\theta-3.2^{k+1}t}{2^{k+2}})$ is a 2-integral basis of $\mathbb{Z}_K$.

If $v_2(B_1) \geq 2(k+2)+1$, then $v_2(ind(F)) = k+3$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+4\theta^2+6t\theta}{2^{k+1}})$ is a 2-integral basis of $\mathbb{Z}_K$.

If $v_2(B_1) \geq 2(k+2)+1$, then $v_2(ind(F)) = k+4$ and $(1, \theta, \frac{\theta^2}{2}, \frac{\theta^3+(4-3.2^k t)\theta^2+6\theta-3.2^{k+1}t}{2^{k+3}})$ is a 2-integral basis of $\mathbb{Z}_K$.

(9) Case 8: $v_p(ab) = 0$: A8.

If $p \in \{2, 3\}$, then $v_p(\triangle) = 0$, $(1, \alpha, \alpha^2, \alpha^3)$ is a p-integral basis of $\mathbb{Z}_K$ and $v_p(d_K) = 0$.
Let $p \geq 5$. If $v_p(disc(2^8 b^3 - 3^3 a^4)) \leq 1$, then $(1, \alpha, \alpha^2, \alpha^3)$ is a p-integral basis of $\mathbb{Z}_K$ and $v_p(d_K) = 0$.

Else, since $3a \neq 0$ modulo p, let $t \in \mathbb{Z}$ such that $3at + 4b = 0$ modulo p^s, where $s = m+1$ and $m = \lfloor \frac{v_p(\triangle)}{2} \rfloor$ ($3at + 4b = p^s L$). Then $(3a)^3 P'(t) = -\triangle + 3.4^3 b^2 p^s L$ modulo p^{2s}. Thus, $v_p(P'(t)) \geq s$. Moreover, $(3a)^4 P(t) = b\triangle - p^s \triangle$ modulo p^{2s}. Thus, $v_p(P(t)) = v_p(\triangle)$. Let $P(X+t) = X^4 + 4tX^3 + 6t^2 X^2 + P'(t)X + P(t)$. Since $6t^2 \neq 0$ modulo p, then $N = S_0 + S_1$ with slopes respectively 0 and $\frac{v_p(\triangle)}{2}$ and $P_{S_1}(Y)$ is square free. Hence, $v_p(ind(P)) = \lfloor \frac{v_p(\triangle)}{2} \rfloor$, $\frac{\theta^3+4t\theta^2+6t^2\theta}{p^m} \in \mathbb{Z}_K$, where $\theta = \alpha - t$. Thus, $(1, \alpha, \alpha^2, \frac{\alpha^3+t\alpha^2+t^2\alpha-3t^3}{p^m})$ is a p-integral basis of z_K and $v_p(d_K) = v_p(\triangle)$ modulo 2.

(10) Case 9: B13, C19. Since $v_p(\triangle) = 0$, $(1, \alpha, \alpha^2, \alpha^3)$ is a p-integral basis of $\mathbb{Z}_K$ and $v_p(d_K) = 0$.

2. An integral basis of a quartic number field defined by $X^4 + aX + b$

Remarks 2.1. (1) *Let p be a prime integer such that p^2 divides $\triangle$. For every $1 \le i \le 3$, let $w_{i,p} = \frac{L_i^p(\alpha)}{p^{r_{i,p}}}$, where $L_i^p(X) \in \mathbb{Z}[X]$ is a monic polynomial of degree i such that $\mathcal{F} = (1, w_{1,p}, w_{2,p}, w_{3,p})$ is a triangular p-integral basis of K. Ten $r_{1,p} \le r_{2,p} \le r_{3,p}$, $v_p(\triangle) = r_1 + r_2 + r_3$ and $v_p(d_K) = v_p(\triangle) - 2(r_1 + r_2 + r_3)$.*

(2) *Let $p_1, \cdots, p_r$ be the primes such that every p_i^2 divides $\triangle$. For every $1 \le i \le 3$, denote $d_i = \prod_{j=1}^{r} p_j^{r_{ij}}$, where for every j, $w_{i,j} = \frac{L_i^{p_j}(\alpha)}{p^{r_{ij}}}$ and $(1, w_{1,j}, w_{2,j}, w_{3,j})$ is a p_j-integral basis of K. Then $1 \mid d_1 \mid d_2 \mid d_3$ are the elementary divisors of $\mathbb{Z}_K/\mathbb{Z}[\alpha]$. In particular, d_3 is the conductor of the order $\mathbb{Z}[\alpha]$ and $d_1 d_2 d_3 = \mp \operatorname{ind}(P)$.*

(3) *We can always assume that a triangular p-integral basis has the property: if $r_i = r_{i+1}$, then we can take $w_{i+1} = \alpha w_i$.*

One can recover a triangular integral basis from different triangular p-integral basis for all p as follows:

Proposition 2.2. *Let $p_1,\ldots,p_s$ the prime integers such that p^2 divides $\triangle$ and 1, d_1, d_2 and d_3 the elementary divisors of the abelian group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$. For every j, let $\mathcal{F}_j = (1, w_{1,j}, w_{2,j}, w_{3,j})$ be a triangular p_j-integral basis of K, i.e., $w_{i,j} = \frac{L_i^j(\alpha)}{p_j^{r_{ij}}}$ such that every $L_i^j(X)$ is a monic polynomial of $\mathbb{Z}[X]$ of degree i. Then $\mathcal{B} = (1, w_1, w_2, w_3)$ is a triangular integral basis of K, where every $w_i = \frac{L_i(\alpha)}{d_i}$, $L_i(X) = L_i^j(X)$ modulo $p_j^{r_{ij}}$.*

Proof. Since $ind(P) = d_1 d_2 d_3$, we need only to check that every $w_i \in \mathbb{Z}_K$. Let $1 \le i \le 3$. Since for every i the integers $(\frac{d_i}{p_j^{r_{ij}}})_{1 \le j \le s}$ are pairwise coprime, there exist integers $t_1, \ldots, t_s$ such that $\sum_{j=1}^{s} t_j \frac{d_i}{p_j^{r_{ij}}} = 1$. Hence, $\frac{L_i(\alpha)}{d_i} = \sum_{j=1}^{s} t_j \dfrac{L_i(\alpha)}{p_j^{r_{ij}}} \in \mathbb{Z}_K$, because all $\frac{L_i(\alpha)}{p_j^{r_{ij}}} \in \mathbb{Z}_K$.

Acknowledgments

This work is supported by the Spanish ministry (Ref: SB 2006-0128) at "CRM" of Barcelona, I would like to thanks the "CRM" of Barcelona for their extraordinary hospitality and facilities for doing this work.

As well as the Professor E. Nart, who communicated me the Newton polygon technical and for his valuable comments and suggestions.

References

[1] S. Alaca and K. S. Williams, *p-integral basis of a quartic field defined by a trinomial $X^4 + aX + b$*, Far East J. Math. Sci. **12** (2004), 137–168.

[2] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer-Verlag Berlin Heidelberg, New York, Paris, Tokyo, second correction (1995).
[3] J. Guardia, J. Montes and E. Nart, *Newton Polygons of Higher Order in Algebraic Number Theory*, arxiv.org/abs/0807.2620v2 [Math.NT] 31 October 2008.
[4] J. Montes and E. Nart, *On a Theorem of Ore*, J. of Alg. **146** (1992) 318–334.
[5] J. Montes, *Poligons de Newton de orden superior y aplicaciones aritméticas*, Ph.D Thesis at "UAB", Barcelona-Spain (1999).
[6] P. Llorente, E. Nart and N. Vila, J. Théorie des nombres de Bordeaux, T3, n 1 (1991) 27–41.

L. Houssain El Fadil
CRM, App 50, Faculty of Sciences, Campus UAB
Bellatera E-08193, Barcelona-Spain
E-mail address: lhouelfadil@hotmail.com