ฐานเชิงพี-อินทิกรัลของบางควินติกฟีลด์

นาย ยศนันต์ มีมาก

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2542
ISBN 974-334-415-2

p-INTEGRAL BASES OF SOME QUINTIC FIELDS

Mr. Yotsanan Meemark

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Mathematics
Department of Mathematics
Faculty of Science
Chulalongkorn University
Academic Year 1999
ISBN 974-334-415-2

Thesis Title	p-Integral Bases of Some Quintic Fields
By	Mr. Yotsanan Meemark
Department	Mathematics
Thesis Advisor	Assistant Professor Ajchara Harnchoowong, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master's Degree.

....Dean of Faculty of Science
(Associate Professor Wanchai Phothiphichitr, Ph.D.)

Thesis Committee

....Chairman
(Assistant Professor Patanee Udomkavanich, Ph.D.)

....Thesis Advisor
(Assistant Professor Ajchara Harnchoowong, Ph.D.)

...........Amorn...Wasanawichit.........Member
(Assistant Professor Amorn Wasanawichit, Ph.D.)

ยศนันต์ มีมาก : ฐานเชิงพี-อินทิกรัลของบางควินติกฟิลด์. (p-INTEGRAL BASES OF SOME QUINTIC FIELDS) อ. ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร. อัจฉรา หาญชูวงศ์, 30 หน้า. ISBN 974-334-415-2.

ในฟิลด์ $K = \mathbf{Q}(\theta)$ โดยที่ θ เป็นรากตัวหนึ่งของพหุนามลดทอนไม่ได้ $x^5 + a$ ใน $\mathbf{Z}[x]$ ฐานเชิงพี-อินทิกรัลถูกคำนวณขึ้นสำหรับทุก ๆ จำนวนเฉพาะพี และ ฐานเชิงจำนวนเต็ม และ ดิสคริมิแนนต์ของ K สามารถหาได้จากฐานเชิงพี-อินทิกรัลที่คำนวณได้นี้

ภาควิชา **คณิตศาสตร์** ลายมือชื่อนิสิต ....
สาขาวิชา **คณิตศาสตร์** ลายมือชื่ออาจารย์ที่ปรึกษา ....
ปีการศึกษา **2542** ลายมือชื่ออาจารย์ที่ปรึกษาร่วม -

##4172398923 MAJOR: MATHEMATICS
KEYWORD: QUINTIC FIELD / p-INTEGRAL BASIS / INTEGRAL BASIS

YOTSANAN MEEMARK : p-INTEGRAL BASES OF SOME QUINTIC FIELDS. THESIS ADVISOR: ASSISTANT PROFESSOR AJCHARA HARNCHOOWONG, Ph.D. 30 pp. ISBN 974-334-415-2.

In the number field $K = \mathbf{Q}(\theta)$, where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbf{Z}[x]$, p-integral bases are computed, for all rational primes p and from these an integral basis of K and its discriminant $d(K)$ are obtained.

ภาควิชา คณิตศาสตร์ ลายมือชื่อนิสิต ....
สาขาวิชา คณิตศาสตร์ ลายมือชื่ออาจารย์ที่ปรึกษา ....
ปีการศึกษา **2542** ลายมือชื่ออาจารย์ที่ปรึกษาร่วม -

ACKNOWLEDGEMENT

I am greatly indebted to Assistant Professor Ajchara HarnChoowong, Ph.D., my advisor, for all her help during preparation and writing this thesis. I would like to thank Assistant Professor Pattanee Udomkavanich, Ph.D. and Assistant Professor Amorn Wasanawichit, Ph.D., my thesis committee, for their suggestions to this thesis. I would like to thank Saban Alaca, Ph.D. who sent his paper directly to me and this paper became the main thing to develop my theorems in this thesis. I would also like to thank all teachers, who have taught me, for my knowledge and skills. Finally, I would like to express my gratitude to my friends in this department. I really enjoy studying with them.

CONTENTS

Chapter I

Introduction

In order to study the structure of the ring of integers of a number field K, an integral basis of K and its discriminant play an important role. Although they are difficult to compute, some kind of number fields, e.g., the quadratic field $\mathbb{Q}[\sqrt{m}]$ where m is a square free integer, the set of algebraic integers is

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m \equiv 2 \text{ or } 3 \pmod 4$$

and

$$\left\{ \frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} \text{ if } m \equiv 1 \pmod 4.$$

We know that if the degree of a number field K is greater than 2, it is difficult to determine the structure of the ring of integers. There are several methods to compute an integral basis of a number field. Most of them are difficult to calculate and apply for every number field.

In [1], Saban Alaca developed theorems about p-integral bases of a number field K and used them to obtain an integral basis of K and its discriminant. The procedure used here is to find a p-integral basis, for every rational prime p, of the number field K, and then an integral basis of K and its discriminant are obtained from its p-integral bases. He applied these results to cubic fields in [2]. Like other methods, p-integral basis, for every rational prime p, of K cannot be found easily if K is a complicated number field.

In this research, we wish to use the results in [1] to find an integral basis of the number field $K = \mathbb{Q}(\theta)$ where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbb{Z}[x]$. Therefore, the main work is to compute a p-integral basis, for every rational prime p, of our number field K. After that we consider only p-integral bases of K for each rational prime p dividing $\mathrm{disc}_{K/\mathbb{Q}}(\theta)$ (if any) and construct from them an integral basis of K.

The next chapter covers the basic definitions and theorems in algebraic number theory, p-integral elements and their properties and p-integral bases of number fields. In the last chapter, we give theorem concerning p-integral bases, for every rational prime p, of our number field K.

Chapter II

p-Integral Bases of Number Fields

In this chapter, we discuss briefly a number of basic concepts that will be used in our subsequent development of p-integral bases of quintic fields. These include fundamental definitions and theorems of algebraic number theory, p-integral elements and their properties and p-integral bases of number fields. All of these results are appeared in [1], [3] and [4].

2.1 Algebraic Integers, Discriminant and Integral Bases

This section covers basic definitions and theorems of algebraic number theory.

Definition 2.1.1. A *number field* K is a finite extension of $\mathbb{Q}$.

Remark 2.1.2. Since $\mathrm{char}(\mathbb{Q}) = 0$, every number field is separable, i.e. there is an $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.

Definition 2.1.3. Let K be a field and A be a subring of K. $\alpha \in K$ is *integral over* A if and only if there exist $a_0, a_1, ..., a_{n-1} \in A$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. If $A = \mathbb{Z}$, K is a number field and $\alpha \in K$ is integral over $\mathbb{Z}$, then α is called an *algebraic integer* in K.

Theorem 2.1.4. *Let R be an integral domain and A be a subring of R containing* 1. *Then the set of all elements in R integral over A forms a ring.*

Definition 2.1.5. In a number field K, the ring of all algebraic integers in K is called the *ring of integers* in K and it is denoted by $\mathcal{O}_K$.

Definition 2.1.6. Let $\alpha_1, \ldots, \alpha_n \in K$. The *discriminant* in K over $\mathbb{Q}$ of $\alpha_1, \ldots, \alpha_n$, denoted by $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$, is given by $\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \det[\alpha_i^{(j)}]^2$, where $\{\alpha_i = \alpha_i^{(1)}, \alpha_i^{(2)}, \ldots, \alpha_i^{(n)}\}$ is the set of all conjugates of α_i $(1 \leq i \leq n)$ with respect to K. For $\alpha \in K$, we denote $\mathrm{disc}_{K/\mathbb{Q}}(\alpha) = \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$.

Definition 2.1.7. Let f be a monic irreducible polynomial of degree n in $\mathbb{Z}[x]$, θ a root of f and $K = \mathbb{Q}(\theta)$. The *discriminant* of f, denoted by $\mathrm{disc} f$, is defined by $\mathrm{disc} f = \mathrm{disc}_{K/\mathbb{Q}}(\theta)$.

Remark 2.1.8. $\mathrm{disc} f = (-1)^{\binom{n}{2}} \mathrm{N}_{K/\mathbb{Q}}(f'(\theta))$.

Theorem 2.1.9. *Let K be a number field of degree n. Then $\mathcal{O}_K$ is a free abelian group of rank n.*

Definition 2.1.10. A basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathcal{O}_K$ is called an *integral basis* of K.

Proposition 2.1.11. *Let* $\{\alpha_1, \ldots, \alpha_n\}$ *and* $\{\beta_1, \ldots, \beta_n\}$ *be any integral bases of* K. *Then* $\operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$.

Definition 2.1.12. The *discriminant* of a number field K, denoted by $d(K)$, is given by $d(K) = \operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ where $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K.

Proposition 2.1.13. *Let* $K = \mathbb{Q}(\theta)$ *where* θ *is a root of an irreducible polynomial* f. *If* $i(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]$, *then we have*

$$\operatorname{disc} f = \operatorname{disc}_{K/\mathbb{Q}}(\theta) = d(K)i(\theta)^2.$$

Definition 2.1.14. The number $i(\theta)$ is called the *index* of θ in $\mathcal{O}_K$.

2.2 p-Integral Bases of Number Fields

In this section, we give results concerning p-integral elements and p-integral bases of number fields, quoted from [1]. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. We know that $\mathcal{O}_K$ is a Dedekind domain, so every nonzero proper ideal can be decomposed uniquely as a product of prime ideals.

Definition 2.2.1. Let I be an $\mathcal{O}_K$-submodule of K. I is a *fractional ideal* of K if there exists a $d \in \mathcal{O}_K - \{0\}$ such that $dI \subseteq \mathcal{O}_K$. For each prime ideal P and each nonzero fractional ideal I of K, $\nu_P(I)$ denotes the exponent of P in the prime ideal decomposition of I. If $\alpha \in K$, then $\nu_P(\alpha) = \nu_P(\alpha\mathcal{O}_K)$. If $K = \mathbb{Q}$, p is a rational prime and $a \in K$, then $\nu_p(a) = \nu_{p\mathbb{Z}}(a)$.

Definition 2.2.2. Let P be a prime ideal of $\mathcal{O}_K$, p be a rational prime and let $\alpha \in K$. If $\nu_P(\alpha) \geq 0$, then α is called a *P-integral element* of K. If α is P-integral for each prime ideal P of K in the prime ideal decomposition of $p\mathcal{O}_K$, then α is called a *p-integral element* of K.

Remark 2.2.3. We note that

(1) the set of all p-integral elements of K, denoted by $\mathcal{O}_p$, forms a ring and

(2) $\{a/b \mid a, b \in \mathbb{Z}, (a, b) = 1 \text{ and } p \nmid b\}$ is the set of all p-integral elements of $\mathbb{Q}$.

Definition 2.2.4. Let $\alpha \in K$ and $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ be the conjugates of α with respect to K. The *characteristic polynomial* C_α of α in K is

$$C_\alpha(x) = \prod_{1\leq i\leq n} (x - \alpha^{(i)}) = \sum_{0\leq i\leq n} (-1)^{n-i} s_{n-i}(\alpha) x^i$$

and $s_k(\alpha)$ is called the k^{th} *elementary symmetric function* of $\alpha \in K$.

We have that $C_\alpha(x) = \det(xI - M_\alpha)$ where M_α is the matrix of the endomorphism of the $\mathbb{Q}$-vector space K obtained by multiplication of α with respect to the basis $\{1, \theta, \ldots, \theta^{n-1}\}$ of K.

Theorem 2.2.5. *Let p be a rational prime. Let $\alpha \in K$ and let $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ be the conjugates of α with respect to K. Then α is a p-integral element of K if and only if the elementary symmetric functions of α are p-integral elements of $\mathbb{Q}$.*

Definition 2.2.6. Let p be a rational prime and let $\{\omega_1, \ldots, \omega_n\}$ be a basis of K over $\mathbb{Q}$, where each ω_i $(1 \leq i \leq n)$ is a p-integral element of K. If every p-integral element α of K can be written as $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ where the a_i are p-integral elements of $\mathbb{Q}$, then $\{\omega_1, \ldots, \omega_n\}$ is called a *p-integral basis* of K.

Theorem 2.2.7. *Let p be a rational prime. For each i $(1 \leq i \leq n-1)$, let k_i be the largest integer for which there exist i integers $x_0^{(i)}, x_1^{(i)}, \ldots, x_{i-1}^{(i)}$ such that*

$$\beta_i := \frac{x_0^{(i)} + x_1^{(i)}\theta + \cdots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{k_i}}$$

is p-integral. Then

(i) $0 \leq k_1 \leq k_2 \leq \cdots \leq k_{n-1}$,

(ii) *a p-integral basis of K is $\{\beta_0 = 1, \beta_1, \beta_2, \ldots, \beta_{n-1}\}$ and*

(iii) $\nu_p(d(K)) = \nu_p(\operatorname{disc}_{K/\mathbb{Q}}(\theta)) - 2(k_1 + k_2 + \cdots + k_{n-1})$.

Theorem 2.2.8. *Let p be a rational prime. If $i(\theta) = 1$, then $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K. Otherwise, let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing $i(\theta)$. Let*

$$\left\{1, \frac{x_{r,0}^{(1)} + \theta}{p_r^{k_{r,1}}}, \ldots, \frac{x_{r,0}^{(n-1)} + x_{r,1}^{(n-1)}\theta + \cdots + x_{r,n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p_r^{k_{r,n-1}}}\right\}$$

be a p_r-integral basis of K $(r = 1, 2, \ldots, s)$ as given in Theorem 2.2.7. Define integers $X_i^{(j)}$ $(1 \leq j \leq n-1, 0 \leq i \leq j-1)$ by

$$X_i^{(j)} \equiv x_{r,i}^{(j)} \pmod{p_r^{k_{r,j}}} \quad (r = 1, 2, \ldots, s),$$

and let $T_j = \prod_{r=1}^{s} p_r^{k_{r,j}} (j = 1, 2, \ldots, n-1)$. Then an integral basis of K is

$$\left\{1, \frac{X_0^{(1)} + \theta}{T_1}, \ldots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \cdots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{T_{n-1}}\right\}.$$

Chapter III

p-Integral Bases of Some Quintic Fields

The main theme of this chapter is a p-integral basis, for every rational prime p, of a number field $K = \mathbb{Q}(\theta)$ where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbb{Z}[x]$ with $\nu_p(a) < 5$. First, we introduce preliminary theorems which have been restated as they apply specifically to our number field K from Theorems 2.2.5, 2.2.7 and 2.2.8. In the second section, we state and prove theorems about p-integral elements, for every rational prime p, of K. After that we apply those theorems to obtain tables giving p-integral bases and $\nu_p(d(K))$, for every rational prime p, of K. Finally, we give examples to illustrate how to use p-integral bases to find an integral basis and the discriminant of K.

3.1 Properties of p-Integral Elements in Some Quintic Fields

Let $K = \mathbb{Q}(\theta)$ where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbb{Z}[x]$ with $\nu_p(a) < 5$.

The following four theorems are special cases in which K is our number field, of Theorem 2.2.5. All of them are restated by computing the elementary symmetric functions of α, β, γ, and δ, respectively.

Theorem 3.1.1. *Let p be a rational prime, and let $\alpha = (t+\theta)/p^k$ where $t, k \in \mathbb{Z}$ and $k \geq 0$. Set*

$$A = 5t,$$
$$B = 10t^2,$$
$$C = 10t^3,$$
$$D = 5t^4 \text{ and}$$
$$E = -a + t^5.$$

Then α is a p-integral element if and only if

$$A \equiv 0 \pmod{p^k}, B \equiv 0 \pmod{p^{2k}}, C \equiv 0 \pmod{p^{3k}},$$
$$D \equiv 0 \pmod{p^{4k}} \text{ and } E \equiv 0 \pmod{p^{5k}}.$$

Theorem 3.1.2. *Let p be a rational prime, and let $\beta = (t + u\theta + \theta^2)/p^k$ where $t, u, k \in \mathbb{Z}$ and $k \geq 0$. Set*

$$A = 5t,$$
$$B = 10t^2,$$
$$C = 10t^3 - 5au,$$
$$D = 5t^4 - 10atu + 5au^3 \text{ and}$$
$$E = a^2 + t^5 - 5at^2u + 5atu^3 - au^5.$$

Then β is a p-integral element if and only if

$$A \equiv 0 \pmod{p^k}, B \equiv 0 \pmod{p^{2k}}, C \equiv 0 \pmod{p^{3k}},$$
$$D \equiv 0 \pmod{p^{4k}} \text{ and } E \equiv 0 \pmod{p^{5k}}.$$

Theorem 3.1.3. *Let p be a rational prime, and let $\gamma = (t + u\theta + v\theta^2 + \theta^3)/p^k$ where $t, u, v, k \in \mathbb{Z}$ and $k \geq 0$. Set*

$$\begin{aligned}
A &= 5t,\\
B &= 10t^2 + 5av,\\
C &= 10t^3 - 5au^2 + 15atv - 5auv^2,\\
D &= 5t^4 - 5a^2u - 10atu^2 + 15at^2v + 5au^3v + 5a^2v^2 - 10atuv^2 \text{ and}\\
E &= -a^3 + t^5 - 5a^2tu - 5at^2u - au^5 + 5at^3v + 5a^2u^2v + 5atu^3v + 5a^2tv^2\\
&\quad - 5at^2uv^2 - 5a^2uv^3 + a^2v^5.
\end{aligned}$$

Then γ is a p-integral element if and only if

$$A \equiv 0 \pmod{p^k}, B \equiv 0 \pmod{p^{2k}}, C \equiv 0 \pmod{p^{3k}},$$
$$D \equiv 0 \pmod{p^{4k}} \text{ and } E \equiv 0 \pmod{p^{5k}}.$$

Theorem 3.1.4. *Let p be a rational prime, and let $\delta = (t+u\theta+v\theta^2+w\theta^3+\theta^4)/p^k$ where $t, u, v, w, k \in \mathbb{Z}$ and $k \geq 0$. Set*

$$\begin{aligned}
A &= 5t,\\
B &= 10t^2 + 5au + 5avw,\\
C &= 10t^3 + 15atu + 5a^2v - 5auv^2 - 5au^2w + 15atvw + 5a^2w^2,\\
D &= -5t^4 - 15at^2u - 5a^2u^2 - 10a^2tv - 5au^3v + 10atuv^2 + 5a^2v^3 - 5a^3w\\
&\quad + 10atu^2w - 15at^2vw + 5a^2uvw - 10a^2tw^2 - 5a^2v^2w^2 + 5a^2uw^3 \text{ and}\\
E &= a^4 + t^5 + 5at^3u + 5a^2tu^2 - au^5 + 5a^2t^2v + 5a^3uv + 5atu^3v - 5at^2uv^2\\
&\quad + 5a^2u^2v^2 - 5a^2tv^3 + a^2v^5 + 5a^3tw - 5at^2u^2w - 5a^2u^3w + 5at^3vw\\
&\quad - 5a^2tuvw - 5a^3v^2w - 5a^2uv^3w + 5a^2t^2w^2 - 5a^3uw^2 + 5a^2u^2vw^2\\
&\quad + 5a^2tv^2w^2 - 5a^2tuw^3 + 5a^3vw^3 - a^3w^5.
\end{aligned}$$

Then δ is a p-integral element if and only if

$$A \equiv 0 \pmod{p^k}, B \equiv 0 \pmod{p^{2k}}, C \equiv 0 \pmod{p^{3k}},$$
$$D \equiv 0 \pmod{p^{4k}} \text{ and } E \equiv 0 \pmod{p^{5k}}.$$

Theorems 3.1.5 and 3.1.6 are special cases for $n = 5$ of Theorem 2.2.7 and Theorem 2.2.8, respectively.

Theorem 3.1.5. *Let p be a rational prime. For each i $(1 \leq i \leq 4)$, let k_i be the largest integer for which there exist i integers $x_0^{(i)}, x_1^{(i)}, \ldots, x_{i-1}^{(i)}$ such that*

$$\omega_i := \frac{x_0^{(i)} + x_1^{(i)}\theta + \cdots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{k_i}}$$

is p-integral. Then $\{1, \omega_1, \omega_2, \omega_3, \omega_4\}$ *is a p-integral basis of K and*

$$\nu_p(d(K)) = \nu_p(\mathrm{disc}_{K/\mathbb{Q}}(\theta)) - 2(k_1 + k_2 + k_3 + k_4).$$

Theorem 3.1.6. *If there are no rational primes dividing* $i(\theta)$*, then* $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ *is an integral basis of K. Let* $p_1, p_2, \ldots, p_s$ *be the distinct rational primes dividing* $i(\theta)$*. Let*

$$\left\{1, \frac{x_{r,0}^{(1)} + \theta}{p_r^{k_{r,1}}}, \ldots, \frac{x_{r,0}^{(4)} + x_{r,1}^{(4)}\theta + x_{r,2}^{(4)}\theta^2 + x_{r,3}^{(4)}\theta^3 + \theta^4}{p_r^{k_{r,4}}}\right\}$$

be a p_r*-integral basis of K* $(r = 1, 2, \ldots, s)$ *as given in Theorem* 3.1.5. *Define integers* $X_i^{(j)}$ $(i = 0, 1, \ldots, j-1, j = 1, 2, 3, 4)$ *by*

$$X_i^{(j)} \equiv x_{r,i}^{(j)} \pmod{p_r^{k_{r,j}}} \quad (r = 1, 2, \ldots, s),$$

and let $T_j = \prod_{r=1}^{s} p_r^{k_{r,j}}$ $(j = 1, 2, 3, 4)$. *Then an integral basis of K is*

$$\left\{1, \frac{X_0^{(1)} + \theta}{T_1}, \ldots, \frac{X_0^{(4)} + X_1^{(4)}\theta + X_2^{(4)}\theta^2 + X_3^{(4)}\theta^3 + \theta^4}{T_4}\right\}.$$

We will apply Theorems 3.1.1 to 3.1.6 to find a p-integral basis, for every rational prime p, of K in the next section.

In order to obtain such a k_i, for every $i \in \{1, 2, 3, 4\}$, in Theorem 3.1.5, we need a remark which can be proved by contradiction.

Remark 3.1.7. For each $i \in \{1, 2, 3, 4\}$, if there exists $m_i \in \mathbb{Z}^+$ such that

$$\omega_i := \frac{x_0^{(i)} + x_1^{(i)}\theta + \cdots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{m_i}}$$

is not a p-integral element, for all $x_0^{(i)}, x_1^{(i)}, \ldots, x_{i-1}^{(i)} \in \mathbb{Z}$, then for every $l_i \geq m_i$,

$$\varpi_i := \frac{y_0^{(i)} + y_1^{(i)}\theta + \cdots + y_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{l_i}}$$

is not a p-integral element, for all $y_0^{(i)}, y_1^{(i)}, \ldots, y_{i-1}^{(i)} \in \mathbb{Z}$.

By means of this remark, for each $i \in \{1, 2, 3, 4\}$, if we begin trying with $m_i = 1, 2, 3, \ldots$, then we will stop whenever we get the first m_i such that ω_i is not a p-integral element, and we have $k_i = m_i - 1$.

3.2 p-Integral Bases of Some Quintic Fields

In this section, we state and prove theorems about p-integral elements and bases, for every rational prime p, of K. According to Theorem 3.1.6, we will consider only the rational prime p dividing $\operatorname{disc}_{K/\mathbb{Q}}(\theta)$. We note that if $\operatorname{disc}_{K/\mathbb{Q}}(\theta) = 5^5a^4 \equiv 0 \pmod{p}$ and $p \neq 5$, then $\nu_p(a) \geq 1$. Thus it is not necessary to consider the case $\nu_p(a) = 0$ if $p \neq 5$.

The next remark will be used in this section. It is readily obtained from the Division Algorithm.

Remark 3.2.1. If there exist integers s, t, u, v, w, k with $k \geq 0$ such that $\varepsilon = (s + t\theta + u\theta^2 + v\theta^3 + w\theta^4)/p^k$ is a p-integral element, then there exist $s_0, t_0, u_0, v_0, w_0 \in \{0, 1, \ldots, p^k - 1\}$ and an $\alpha \in \mathbb{Z}[\theta]$ such that $\varepsilon_0 = (s_0 + t_0\theta + u_0\theta^2 + v_0\theta^3 + w_0\theta^4)/p^k = \varepsilon - \alpha$ and so ε_0 is a p-integral element. And also if p is odd and $k = 1$, then we can consider $s_0, t_0, u_0, v_0, w_0 \in \{-(p-1)/2, -(p-1)/2 + 1, \ldots, 0, \ldots, (p-1)/2 - 1, (p-1)/2\}$ instead.

We now give theorems concerning p-integral elements, for every rational prime p, in our number fields K by applying Theorems 3.1.1 to 3.1.4.

Theorem 3.2.2. *The largest nonnegative integer k for which there exists an integer t such that $\alpha = (t + \theta)/p^k$ is a p-integral element is $k = 0$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exists an integer t such that $\alpha = (t + \theta)/p^k$ is a p-integral element. Let A, B, C, D and E be as in Theorem 3.1.1.

Consider $k = 1$. Since $A \equiv 0 \pmod{p}$, $\nu_p(t) \geq 1$. Since $E \equiv 0 \pmod{p^5}$, $\nu_p(a) \geq 5$, a contradiction. Hence $k = 0$. □

Theorem 3.2.3. *Let k be the largest nonnegative integer for which there exist integers t and u such that $\beta = (t + u\theta + \theta^2)/p^k$ is a p-integral element. Then:*

(0) *If $\nu_p(a) = 0$, then $k = 0$.*

(1) *If $\nu_p(a) = 1$, then $k = 0$.*

(2) *If $\nu_p(a) = 2$, then $k = 0$.*

(3) *If $\nu_p(a) = 3$, then $k = 1$.*

(4) *If $\nu_p(a) = 4$, then $k = 1$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exist integers t and u such that $\beta = (t + u\theta + \theta^2)/p^k$ is a p-integral element. Let A, B, C, D and E be as in Theorem 3.1.2.

(0) and (1) Assume that $\nu_p(a) = 0$ or 1. Consider $k = 1$. Since $B \equiv 0 \pmod{p^2}$, $\nu_p(t) \geq 1$. Since $C \equiv 0 \pmod{p^3}$, $\nu_p(u) \geq 1$. Since $E \equiv 0 \pmod{p^5}$, $a^2 \equiv 0 \pmod{p^5}$ contradicting $\nu_p(a) \leq 1$. Hence $k = 0$.

(2) Assume that $\nu_p(a) = 2$. Consider $k = 1$. Since $B \equiv 0 \pmod{p^2}$, $\nu_p(t) \geq 1$. Since $D \equiv 0 \pmod{p^4}$, $\nu_p(u) \geq 1$. Since $E \equiv 0 \pmod{p^5}$, $a^2 \equiv 0 \pmod{p^5}$ contradicting $\nu_p(a) = 2$. Hence $k = 0$.

For $\nu_p(a) = 3$ or 4, θ^2/p is a p-integral element. Hence $k \geq 1$.

(3) Assume that $\nu_p(a) = 3$. Consider $k = 2$. Since $B \equiv 0 \pmod{p^4}$, $\nu_p(t) \geq 2$. Since $C \equiv 0 \pmod{p^6}$, $\nu_p(u) \geq 2$. Since $E \equiv 0 \pmod{p^{10}}$, $a^2 \equiv 0 \pmod{p^{10}}$ contradicting $\nu_p(a) = 3$. Hence $k = 1$.

(4) Assume that $\nu_p(a) = 4$. Consider $k = 2$. Since $B \equiv 0 \pmod{p^4}$, $\nu_p(t) \geq 2$. Since $D \equiv 0 \pmod{p^8}$, $\nu_p(u) \geq 2$. Since $E \equiv 0 \pmod{p^{10}}$, $a^2 \equiv 0 \pmod{p^{10}}$ contradicting $\nu_p(a) = 4$. Hence $k = 1$. □

The next two theorems are stated and proved for $p \neq 5$, so they do not have the case $\nu_5(a) = 0$.

Theorem 3.2.4. *Let k be the largest nonnegative integer for which there exist integers t, u and v such that $\gamma = (t + u\theta + v\theta^2 + \theta^3)/p^k$ is a p-integral element where $p \neq 5$. Then:*

(1) *If $\nu_p(a) = 1$, then $k = 0$.*

(2) *If $\nu_p(a) = 2$, then $k = 1$.*

(3) *If $\nu_p(a) = 3$, then $k = 1$.*

(4) *If $\nu_p(a) = 4$, then $k = 2$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exist integers t, u and v such that $\gamma = (t + u\theta + v\theta^2 + \theta^3)/p^k$ is a p-integral element where $p \neq 5$. Let A, B, C, D and E be as in Theorem 3.1.3.

(1) Assume that $\nu_p(a) = 1$. Consider $k = 1$. Since $A \equiv 0 \pmod{p}$, $\nu_p(t) \geq 1$. Since $B \equiv 0 \pmod{p^2}$, $\nu_p(v) \geq 1$. Since $C \equiv 0 \pmod{p^3}$, $\nu_p(u) \geq 1$. Since $E \equiv 0 \pmod{p^5}$, $\nu_p(a) \geq 2$ contradicting $\nu_p(a) = 1$. Hence $k = 0$.

For $\nu_p(a) = 2$ or 3, θ^3/p is a p-integral element. Hence $k \geq 1$

(2) Assume that $\nu_p(a) = 2$. Consider $k = 2$. Since $A \equiv 0 \pmod{p^2}$, $\nu_p(t) \geq 2$. Since $B \equiv 0 \pmod{p^4}$, $\nu_p(v) \geq 2$. Since $C \equiv 0 \pmod{p^6}$, $\nu_p(u) \geq 2$. Since $E \equiv 0 \pmod{p^{10}}$, $\nu_p(a) \geq 3$ contradicting $\nu_p(a) = 2$. Hence $k = 1$.

(3) Assume that $\nu_p(a) = 3$. Consider $k = 2$. Since $A \equiv 0 \pmod{p^2}$, $\nu_p(t) \geq 2$. Since $B \equiv 0 \pmod{p^4}$, $\nu_p(v) \geq 1$. Since $C \equiv 0 \pmod{p^6}$, $au^2 + auv^2 \equiv 0 \pmod{p^6}$, so $u(u + v^2) \equiv 0 \pmod{p^3}$. Since $\nu_p(v) \geq 1$, $\nu_p(u) \geq 2$. Since $E \equiv 0 \pmod{p^{10}}$, $\nu_p(a) \geq 4$ contradicting $\nu_p(a) = 3$. Hence $k = 1$.

(4) Assume that $\nu_p(a) = 4$. Then θ^3/p^2 is a p-integral element, so $k \geq 2$. Consider $k = 3$. Since $A \equiv 0 \pmod{p^3}$, $\nu_p(t) \geq 3$. Since $B \equiv 0 \pmod{p^6}$,

$\nu_p(v) \geq 2$. Since $C \equiv 0 \pmod{p^9}$, $au^2 + auv^2 \equiv 0 \pmod{p^9}$, so $u(u+v^2) \equiv 0 \pmod{p^5}$. Since $\nu_p(v) \geq 2$, $\nu_p(u) \geq 3$. Since $D \equiv 0 \pmod{p^{12}}$, $\nu_p(u) \geq 4$. Since $E \equiv 0 \pmod{p^{15}}$, $\nu_p(a) \geq 5$ contradicting $\nu_p(a) = 4$. Hence $k = 3$. □

Theorem 3.2.5. *Let k be the largest nonnegative integer for which there exist integers t, u, v and w such that $\delta = (t + u\theta + v\theta^2 + w\theta^3 + \theta^4)/p^k$ is a p-integral element where $p \neq 5$. Then:*

(1) *If $\nu_p(a) = 1$, then $k = 0$.*

(2) *If $\nu_p(a) = 2$, then $k = 1$.*

(3) *If $\nu_p(a) = 3$, then $k = 2$.*

(4) *If $\nu_p(a) = 4$, then $k = 3$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exist integers t, u, v and w such that $\delta = (t + u\theta + v\theta^2 + w\theta^3 + \theta^4)/p^k$ is a p-integral element where $p \neq 5$. Let A, B, C, D and E be as in Theorem 3.1.4. According to Remark 3.2.1, we may consider $0 \leq t, u, v, w < p^k$.

(1) Assume that $\nu_p(a) = 1$. Consider $k = 1$. Since $A \equiv 0 \pmod{p}$, $\nu_p(t) \geq 1$, so $t = 0$. Since $B \equiv 0 \pmod{p^2}$,

$$u + vw \equiv 0 \pmod{p}. \tag{3.1}$$

Since $C \equiv 0 \pmod{p^3}$,

$$av - uv^2 - u^2w + aw^2 \equiv 0 \pmod{p^2}. \tag{3.2}$$

Since $D \equiv 0 \pmod{p^4}$,

$$-au^2 - u^3v + av^3 - a^2w + auvw - av^2w^2 + auw^3 \equiv 0 \pmod{p^3}. \tag{3.3}$$

Since $E \equiv 0 \pmod{p^5}$,

$$\begin{aligned} &a^3 - u^5 + 5a^2uv + 5au^2v^2 + av^5 - 5au^3w - 5a^2v^2w - \\ &5auv^3w - 5a^2uw^2 + 5au^2vw^2 + 5a^2vw^3 - a^2w^5 \equiv 0 \pmod{p^4}. \end{aligned} \tag{3.4}$$

Case 1. $u = 0$. By (3.1), $v = 0$ or $w = 0$.

1.1. $v = 0$ and $w \neq 0$. By (3.3), $a^2w \equiv 0 \pmod{p^3}$, a contradiction.

1.2. $v \neq 0$ and $w = 0$. By (3.3), $av^3 \equiv 0 \pmod{p^3}$, a contradiction.

1.3. $\nu_p(v) = 1 = \nu_p(w)$. By (3.4), $a^3 \equiv 0 \pmod{p^4}$, a contradiction.

Case 2. $\nu_p(u) = 0$. By (3.1), $\nu_p(v) = \nu_p(w) = 0$. By (3.3), $u^3v \equiv 0 \pmod{p}$, a contradiction.
Hence $k = 0$.

(2) Assume that $\nu_p(a) = 2$. Then θ^4/p is a p-integral element, so $k \geq 2$. Consider $k = 2$. Since $A \equiv 0 \pmod{p^2}$, $\nu_p(t) \geq 2$, so $t = 0$. Since $B \equiv 0 \pmod{p^4}$,

$$u + vw \equiv 0 \pmod{p^2}. \tag{3.5}$$

Since $C \equiv 0 \pmod{p^6}$,

$$av - uv^2 - u^2w + aw^2 \equiv 0 \pmod{p^4}. \tag{3.6}$$

Since $D \equiv 0 \pmod{p^8}$,

$$-au^2 - u^3v + av^3 - a^2w + auvw - av^2w^2 + auw^3 \equiv 0 \pmod{p^6}. \tag{3.7}$$

Since $E \equiv 0 \pmod{p^{10}}$,

$$\begin{aligned} &a^3 - u^5 + 5a^2uv + 5au^2v^2 + av^5 - 5au^3w - 5a^2v^2w - \\ &5auv^3w - 5a^2uw^2 + 5au^2vw^2 + 5a^2vw^3 - a^2w^5 \equiv 0 \pmod{p^8}. \end{aligned} \tag{3.8}$$

Case 1. $u = 0$. By (3.5), $\nu_p(vw) \geq 2$. By (3.7), $av^3 \equiv 0 \pmod{p^4}$, so $v^3 \equiv 0 \pmod{p^2}$. Then $\nu_p(v) \geq 1$. By (3.6), $aw^2 \equiv 0 \pmod{p^3}$. By (3.8), $a^3 \equiv 0 \pmod{p^8}$, a contradiction.

Case 2. $\nu_p(u) = 0$. By (3.5), $\nu_p(v) = \nu_p(w) = 0$. By (3.7), $u^3v \equiv 0 \pmod{p^2}$, a contradiction.

Case 3. $\nu_p(u) = 1$. By (3.5), $\nu_p(v) = 1$ or $\nu_p(w) = 1$ but not both.

3.1. $\nu_p(v) = 1$ and $\nu_p(w) = 0$. By (3.7), $auw^3 \equiv 0 \pmod{p^4}$, a contradiction.

3.2. $\nu_p(v) = 0$ and $\nu_p(w) = 1$. By (3.6), $uv^2 \equiv 0 \pmod{p^2}$, a contradiction.

Hence $k = 1$.

(3) Assume that $\nu_p(a) = 3$. Then θ^4/p^2 is a p-integral element, so $k \geq 2$. Consider $k = 3$. Since $A \equiv 0 \pmod{p^3}$, $\nu_p(t) \geq 3$, so $t = 0$. Since $B \equiv 0 \pmod{p^6}$,

$$u + vw \equiv 0 \pmod{p^3}. \tag{3.9}$$

Since $C \equiv 0 \pmod{p^9}$,

$$av - uv^2 - u^2w + aw^2 \equiv 0 \pmod{p^6}. \tag{3.10}$$

Since $D \equiv 0 \pmod{p^{12}}$,

$$-au^2 - u^3v + av^3 - a^2w + auvw - av^2w^2 + auw^3 \equiv 0 \pmod{p^9}. \tag{3.11}$$

Since $E \equiv 0 \pmod{p^{15}}$,

$$\begin{aligned} &a^3 - u^5 + 5a^2uv + 5au^2v^2 + av^5 - 5au^3w - 5a^2v^2w - \\ &5auv^3w - 5a^2uw^2 + 5au^2vw^2 + 5a^2vw^3 - a^2w^5 \equiv 0 \pmod{p^{12}}. \end{aligned} \tag{3.12}$$

Case 1. $u = 0$. By (3.10), $v + w^2 \equiv 0 \pmod{p^3}$. Then $\nu_p(v) \neq 1$.

1.1. $\nu_p(v) = 0$. Then $\nu_p(w) = 0$ contradicting (3.9).

1.2. $v = 0$ or $\nu_p(v) \geq 2$. Then $\nu_p(w) \geq 1$. By (3.12), $\nu_p(a) > 3$, a contradiction.

Case 2. $\nu_p(u) = 0$. By (3.9), $\nu_p(v) = 0 = \nu_p(w)$. By (3.11), $u^3 v \equiv 0 \pmod{p^3}$, a contradiction.

Case 3. $\nu_p(u) = 1$. By (3.9), $\nu_p(v) < 2, \nu_p(w) < 2$ and $\nu_p(v) = 1$ or $\nu_p(w) = 1$ but not both.

3.1. $\nu_p(v) = 1$ and $\nu_p(w) = 0$. By (3.10), $u^2 w \equiv 0 \pmod{p^3}$, a contradiction.

3.2. $\nu_p(v) = 0$ and $\nu_p(w) = 1$. By (3.10), $uv^2 \equiv 0 \pmod{p^3}$, a contradiction.

Case 4. $\nu_p(u) = 2$. By (3.9), $\nu_p(vw) = 2$. By (3.11), $\nu_p(v) \geq 1$.

4.1. $\nu_p(v) = 1$. Then $\nu_p(w) = 1$. By (3.12), $\nu_(a) > 3$, a contradiction.

4.2. $\nu_p(v) = 2$. Then $\nu_p(w) = 0$. By (3.10), $aw^2 \equiv 0 \pmod{p^4}$, a contradiction.

Hence $k = 2$.

(4) Assume that $\nu_p(a) = 4$. Then θ^4/p^3 is a p-integral element, so $k \geq 3$. Consider $k = 3$. Since $A \equiv 0 \pmod{p^4}$, $\nu_p(t) \geq 4$, so $t = 0$. Since $B \equiv 0 \pmod{p^8}$,

$$u + vw \equiv 0 \pmod{p^4}. \tag{3.13}$$

Since $C \equiv 0 \pmod{p^{12}}$,

$$av - uv^2 - u^2 w + aw^2 \equiv 0 \pmod{p^8}. \tag{3.14}$$

Since $D \equiv 0 \pmod{p^{16}}$,

$$-au^2 - u^3 v + av^3 - a^2 w + auvw - av^2 w^2 + auw^3 \equiv 0 \pmod{p^{12}}. \tag{3.15}$$

Since $E \equiv 0 \pmod{p^{20}}$,

$$\begin{aligned} &a^3 - u^5 + 5a^2 uv + 5au^2 v^2 + av^5 - 5au^3 w - 5a^2 v^2 w - \\ &5auv^3 w - 5a^2 uw^2 + 5au^2 vw^2 + 5a^2 vw^3 - a^2 w^5 \equiv 0 \pmod{p^{16}}. \end{aligned} \tag{3.16}$$

Case 1. $u = 0$. By (3.14), $v + w^2 \equiv 0 \pmod{p^4}$. Then $v = 0$ or $\nu_p(v)$ is even.

1.1. $v = 0$. Then $\nu_p(w) \geq 2$. By (3.16), $\nu_p(a) > 4$, a contradiction.

1.2. $\nu_p(v) = 0$. Then $\nu_p(w) = 0$ contradicting (3.13).

1.3. $\nu_p(v) = 2$. Then $\nu_p(w) = 1$ contradicting (3.13).

Case 2. $\nu_p(u) = 0$. By (3.13), $\nu_p(v) = \nu_p(w) = 0$. By (3.15), $u^3 v \equiv 0 \pmod{p^4}$, a contradiction.

Case 3. $\nu_p(u) = 1$. By (3.13), $\nu_p(v) < 2, \nu_p(w) < 2$ and $\nu_p(v) = 1$ or $\nu_p(w) = 1$ but not both.

3.1. $\nu_p(v) = 1$ and $\nu_p(w) = 0$. By (3.14), $u^2w \equiv 0 \pmod{p^3}$, a contradiction.

3.2. $\nu_p(v) = 0$ and $\nu_p(w) = 1$. By (3.14), $uv^2 \equiv 0 \pmod{p^3}$, a contradiction.

Case 4. $\nu_p(v) = 2$. By (3.13), $\nu_p(vw) = 2$. By (3.15), $\nu_p(v) \geq 1$.

4.1. $\nu_p(v) = 1$. Then $\nu_p(w) = 1$. By (3.14), $uv^2 \equiv 0 \pmod{p^5}$, a contradiction.

4.2. $\nu_p(v) = 2$. Then $\nu_p(w) = 0$. By (3.15), $auw^3 \equiv 0 \pmod{p^8}$, a contradiction.

Case 5. $\nu_p(v) = 3$. By (3.13), $\nu_p(vw) = 3$. By (3.15), $\nu_p(v) \geq 2$.

5.1. $\nu_p(v) = 2$. Then $\nu_p(w) = 1$. By (3.15), $a^2w \equiv 0 \pmod{p^{10}}$, a contradiction.

5.2. $\nu_p(v) = 3$. Then $\nu_p(w) = 0$. By (3.14), $aw^2 \equiv 0 \pmod{p^7}$, a contradiction.

Hence $k = 3$. □

The next two theorems are stated and proved for $p = 5$ of Theorems 3.2.4 and 3.2.5, respectively.

Theorem 3.2.6. *Let k be the largest nonnegative integer for which there exist integers t, u and v such that $\gamma = (t + u\theta + v\theta^2 + \theta^3)/5^k$ is a 5-integral element. Then:*

(0) *If $\nu_5(a) = 0$, then $k = 0$.*

(1) *If $\nu_5(a) = 1$, then $k = 0$.*

(2) *If $\nu_5(a) = 2$, then $k = 1$.*

(3) *If $\nu_5(a) = 3$, then $k = 1$.*

(4) *If $\nu_5(a) = 4$, then $k = 2$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exist integers t, u and v such that $\gamma = (t + u\theta + v\theta^2 + \theta^3)/5^k$ is a 5-integral element. Let A, B, C, D and E be as in Theorem 3.1.3.

(0) Assume that $\nu_5(a) = 0$. Consider $k = 1$. According to Remark 3.2.1, we may assume that $t, u, v \in \{-2, -1, 0, 1, 2\}$. Since $B \equiv 0 \pmod{5^2}$,

$$2t^2 \equiv -av \pmod{5}. \tag{3.17}$$

Since $C \equiv 0 \pmod{5^3}$,

$$2t^3 - au^2 + 3atv - auv^2 \equiv 0 \pmod{5^2}. \tag{3.18}$$

Since $D \equiv 0 \pmod{5^4}$,

$$t^4 - a^2u - 2atu^2 + 3at^2v + au^3v + a^2v^2 - 2atuv^2 \equiv 0 \pmod{5^3}. \qquad (3.19)$$

Case 1. $t = 0$. By (3.17) and $\nu_5(a) = 0$, we have $v = 0$. By (3.18), $u = 0$. Since $E \equiv 0 \pmod{5^5}$, $a^3 \equiv 0 \pmod{5^3}$, a contradiction.

Case 2. $t = 1$. By (3.17), $av \equiv -2 \pmod 5$.

2.1. $a \equiv -1 \pmod 5$ and $v = 2$. By (3.18), $u^2 - u + 1 \equiv 0 \pmod 5$, a contradiction.

2.2. $a \equiv 2 \pmod 5$ and $v = -1$. By (3.18), $u^2 + u + 2 \equiv 0 \pmod 5$, a contradiction.

2.3. $a \equiv -2 \pmod 5$ and $v = 1$. By (3.18), $u^2 + u - 2 = (u-1)(u+2) \equiv 0 \pmod 5$, so $u = -2$ or $u = 1$. By substituting t, u, v and a in (3.19), we have a contradiction.

2.4. $a \equiv 1 \pmod 5$ and $v = -2$. By (3.18), $u^2 + 4u + 4 = (u+2)^2 \equiv 0 \pmod 5$, so $u = -2$. By substituting t, u and v in A, B, C, D and E, we have $A = 5$, $B = 10 - 10a$, $C = 10 - 10a$, $D = 5 + 90a + 30a^2$ and $E = 1 + 122a - 122a^2 - a^3$. Since $D \equiv 0 \pmod{5^4}$, $1 + 18a + 6a^2 \equiv 0 \pmod{5^3}$. Since $a \equiv 1 \pmod 5$, $a = 5m + 1$ for some $m \in \mathbb{Z}$. Then $1 + 18(5m+1) + 6(5m+1)^2 = 25 + 150m + 150m^2 \equiv 0 \pmod{5^3}$, so $1+6m+6m^2 \equiv 0 \pmod 5$. Thus $1+m+m^2 \equiv 0 \pmod 5$, a contradiction.

Case 3. $t = -1$. By 3.17, $av \equiv -2 \pmod 5$.

3.1. $a \equiv -2 \pmod 5$ and $v = 1$. By (3.18), $u^2 + u + 2 \equiv 0 \pmod 5$, a contradiction.

3.2. $a \equiv 1 \pmod 5$ and $v = -2$. By (3.18), $u^2 + u - 1 \equiv 0 \pmod 5$, a contradiction.

3.3. $a \equiv 2 \pmod 5$ and $v = -1$. By (3.18), $u^2 + u - 2 = (u-1)(u+2) \equiv 0 \pmod 5$, so $u = -2$ or $u = 1$. By substituting t, u, v and a in (3.19), we have a contradiction.

3.4. $a \equiv -1 \pmod 5$ and $v = 2$. By (3.18), $u^2 + 4u + 4 = (u+2)^2 \equiv 0 \pmod 5$, so $u = -2$. By substituting t, u and v in A, B, C, D and E, we have $A = 5$, $B = 10 + 10a$, $C = 10 + 10a$, $D = 5 - 90a + 30a^2$ and $E = -1 + 122a + 122a^2 - a^3$. Since $D \equiv 0 \pmod{5^4}$, $1 - 18a + 6a^2 \equiv 0 \pmod{5^3}$. Since $a \equiv -1 \pmod 5$, $a = 5m - 1$ for some $m \in \mathbb{Z}$. Then $1 - 18(5m-1) + 6(5m-1)^2 = 25 - 150m + 150m^2 \equiv 0 \pmod{5^3}$, so $1+6m+6m^2 \equiv 0 \pmod 5$. Thus $1+m+m^2 \equiv 0 \pmod 5$, a contradiction.

Case 4. $t = 2$. By 3.17, $av \equiv 2 \pmod 5$.

4.1. $a \equiv 1 \pmod 5$ and $v = 2$. By (3.18), $-u^2 + u - 2 \equiv 0 \pmod 5$, a contradiction.

4.2. $a \equiv 2 \pmod 5$ and $v = 1$. By (3.18), $u^2 + u + 1 \equiv 0 \pmod 5$, a contradiction.

4.3. $a \equiv -1 \pmod 5$ and $v = -2$. By (3.18), $u^2 - u - 2 = (u+1)(u-2) \equiv 0 \pmod 5$, so $u = -1$ or $u = 2$. By substituting t, u, v and a in (3.19), we have a contradiction.

4.4. $a \equiv -2 \pmod 5$ and $v = -1$. By (3.18), $u^2 - 4u + 4 = (u-2)^2 \equiv 0 \pmod 5$, so $u = 2$. By substituting t, u and v in A, B, C, D and E, we have $A = 10$, $B = 40 - 5a$, $C = 80 - 60a$, $D = 80 - 220a - 5a^2$ and $E = 32 - 272a - 21a^2 - a^3$. Since $a \equiv -2 \pmod 5$, $a = 5m - 2$ for some $m \in \mathbb{Z}$. Since $E \equiv 0 \pmod{5^5}$, $32 - 272(5m-2) - 21(5m-2)^2 - (5m-2)^3 = 500 - 1000m - 375m^2 - 125m^3 \equiv 0 \pmod{5^5}$, so

$$4 - 8m - 3m^2 - m^3 \equiv 0 \pmod{5^2} \tag{3.20}$$

Since $D \equiv 0 \pmod{5^4}$, $-80 + 220(5m-2) + 5(5m-2)^2 = -500 + 1000m + 125m^2 \equiv 0 \pmod{5^4}$, so $m^2 - 2m + 1 = (m-1)^2 \equiv 0 \pmod 5$. Then $m \equiv 1 \pmod 5$, so

$$m^2 - 2m + 1 \equiv 0 \pmod{5^2}. \tag{3.21}$$

By (3.20) and (3.21), we have $m^3 + 7m^2 \equiv 0 \pmod{5^2}$. Since $m \equiv 1 \pmod 5$, $m \equiv -7 \pmod{5^2}$, so $m \equiv -2 \pmod 5$, a contradiction.

Case 5. $t = -2$. By 3.17, $av \equiv 2 \pmod 5$.

5.1. $a \equiv -1 \pmod 5$ and $v = -2$. By (3.18), $u^2 - u + 2 \equiv 0 \pmod 5$, a contradiction.

5.2. $a \equiv -2 \pmod 5$ and $v = -1$. By (3.18), $u^2 + u + 1 \equiv 0 \pmod 5$, a contradiction.

5.3. $a \equiv 1 \pmod 5$ and $v = 2$. By (3.18), $u^2 - u - 2 = (u+1)(u-2) \equiv 0 \pmod 5$, so $u = -1$ or $u = 2$. By substituting t, u, v and a in (3.19), we have a contradiction.

5.4. $a \equiv 2 \pmod 5$ and $v = 1$. By (3.18), $u^2 - 4u + 4 = (u-2)^2 \equiv 0 \pmod 5$, so $u = 2$. By substituting t, u and v in A, B, C, D and E, we have $A = 10$, $B = 40 + 5a$, $C = 80 + 60a$, $D = 80 + 220a - 5a^2$ and $E = -32 - 272a + 21a^2 - a^3$. Since $a \equiv 2 \pmod 5$, $a = 5m + 2$ for some $m \in \mathbb{Z}$. Since $E \equiv 0 \pmod{5^5}$, $-32 - 272(5m+2) + 21(5m+2)^2 - (5m+2)^3 = -500 - 1000m + 375m^2 - 125m^3 \equiv 0 \pmod{5^5}$, so

$$4 + 8m - 3m^2 + m^3 \equiv 0 \pmod{5^2} \tag{3.22}$$

Since $D \equiv 0 \pmod{5^4}$, $80 + 220(5m+2) - 5(5m+2)^2 = 500 + 1000m - 125m^2 \equiv 0 \pmod{5^4}$, so $m^2 + 2m + 1 = (m+1)^2 \equiv 0 \pmod 5$. Then $m \equiv -1 \pmod 5$, so

$$m^2 + 2m + 1 \equiv 0 \pmod{5^2}. \tag{3.23}$$

By (3.22) and (3.23), we have $m^3 + 7m^2 \equiv 0 \pmod{5^2}$. Since $m \equiv -1 \pmod 5$, $m \equiv 7 \pmod{5^2}$, so $m \equiv 2 \pmod 5$, a contradiction.

Hence $k = 0$.

(1) Assume that $\nu_5(a) = 1$. Consider $k = 1$. Since $B \equiv 0 \pmod{5^2}$, $\nu_5(t) \geq 1$. Since $C \equiv 0 \pmod{5^3}$, $u(u+v^2) \equiv 0 \pmod 5$, so $u \equiv 0 \pmod 5$ or $u + v^2 \equiv 0 \pmod 5$.
Case 1. $u \equiv 0 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $\nu_5(v) \geq 1$. Since $E \equiv 0 \pmod{5^5}$, $a^3 \equiv 0 \pmod{5^5}$, a contradiction.
Case 2. $u+v^2 \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^5}$, $\nu_5(u) \geq 1$. Then $\nu_5(v) \geq 1$, and so $a^3 \equiv 0 \pmod{5^5}$, a contradiction.
Hence $k = 0$.

For $\nu_5(a) = 2$ or 3, $\theta^3/5$ is a 5-integral element. Hence $k \geq 1$.

(2) Assume that $\nu_5(a) = 2$. Consider $k = 2$. Since $A \equiv 0 \pmod{5^2}$, $\nu_5(t) \geq 1$. Suppose that $\nu_5(t) > 1$. Since $B \equiv 0 \pmod{5^4}$, $\nu_5(v) \geq 1$. Since $C \equiv 0 \pmod{5^6}$, $\nu_5(u) \geq 1$. Since $E \equiv 0 \pmod{5^{10}}$, $\nu_5(a) > 2$, a contradiction. Thus we have $\nu_5(t) = 1$. Since $C \equiv 0 \pmod{5^6}$,

$$u(u+v^2) \equiv 0 \pmod 5. \tag{3.24}$$

Assume that $\nu_5(u) \geq 1$. Since $E \equiv 0 \pmod{5^{10}}$, $\nu_5(v) \geq 1$. Since $D \equiv 0 \pmod{5^8}$, $\nu_5(t) > 1$, a contradiction. Then from (3.24), we have $u \equiv -v^2 \pmod 5$ and so $\nu_5(u) = \nu_5(v) = 0$. Since $D \equiv 0 \pmod{5^8}$, $u^3 v \equiv 0 \pmod 5$, a contradiction. Hence $k = 1$.

(3) Assume that $\nu_5(a) = 3$. Consider $k = 2$. Since $B \equiv 0 \pmod{5^4}$, $\nu_5(t) \geq 2$. Since $C \equiv 0 \pmod{5^6}$,

$$u(u+v^2) \equiv 0 \pmod{5^2}. \tag{3.25}$$

Since $D \equiv 0 \pmod{5^8}$, $u^3 v \equiv 0 \pmod 5$. Then $u \equiv 0 \pmod 5$ or $v \equiv 0 \pmod 5$.
Case 1. $u \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{10}}$, $\nu_5(v) \geq 1$, and so $a^3 \equiv 0 \pmod{5^{10}}$, a contradiction.
Case 2. $v \equiv 0 \pmod 5$. By (3.25), $u \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{10}}$, $a^3 \equiv 0 \pmod{5^{10}}$, a contradiction.
Hence $k = 1$.

(4) Assume that $\nu_5(a) = 4$. Then $\theta^3/5^2$ is a 5-integral element, so $k \geq 2$. Consider $k = 3$. Since $A \equiv 0 \pmod{5^3}$, $\nu_5(t) \geq 2$. Suppose that $\nu_5(t) > 2$.

Since $B \equiv 0 \pmod{5^6}$, $\nu_5(v) \geq 1$. Since $C \equiv 0 \pmod{5^9}$, $u^2 \equiv -uv^2 \pmod{5^4}$, so $\nu_5(u) \geq 2$. Since $E \equiv 0 \pmod{5^{15}}$, $\nu_5(a) > 4$, a contradiction. Then we have $\nu_5(t) = 2$. Since $B \equiv 0 \pmod{5^6}$, $\nu_5(v) = 0$. Since $C \equiv 0 \pmod{5^9}$, $u^2 + uv^2 \equiv 0 \pmod{5^2}$, so $\nu_5(u) \neq 1$. Since $D \equiv 0 \pmod{5^{12}}$, $u^2 \equiv 2tv \pmod{5^7}$, $\nu_5(u) = 1$, a contradiction. Hence $k = 2$. ☐

Theorem 3.2.7. *Let k be the largest nonnegative integer for which there exist integers t, u, v and w such that $\delta = (t + u\theta + v\theta^2 + w\theta^3 + \theta^4)/5^k$ is a 5-integral element. Then:*

(0) *If $\nu_5(a) = 0$, then $k = 1$ whenever $a \equiv 1 \pmod{5^2}$ or $a \equiv -1 \pmod{5^2}$ or ($a = 5m - 2$ and $m \equiv -1 \pmod 5$) or ($a = 5m + 2$ and $m \equiv 1 \pmod 5$), and $k = 0$ otherwise.*

(1) *If $\nu_5(a) = 1$, then $k = 0$.*

(2) *If $\nu_5(a) = 2$, then $k = 1$.*

(3) *If $\nu_5(a) = 3$, then $k = 2$.*

(4) *If $\nu_5(a) = 4$, then $k = 3$.*

Proof. Let $k \in \mathbb{Z}_0^+$. Suppose that there exist integers t, u, v and w such that $\delta = (t + u\theta + v\theta^2 + w\theta^3 + \theta^4)/5^k$ is a 5-integral element. Let A, B, C, D and E be as in Theorem 3.1.4.

(0) Assume that $\nu_5(a) = 0$. Consider $k = 2$. Since $A \equiv 0 \pmod{5^2}$, $t \equiv 0 \pmod 5$. Since $B \equiv 0 \pmod{5^4}$,

$$u + vw \equiv 0 \pmod{5^2}. \tag{3.26}$$

Since $C \equiv 0 \pmod{5^6}$,

$$av - uv^2 - u^2w + aw^2 \equiv 0 \pmod 5. \tag{3.27}$$

Case 1. $v \equiv 0 \pmod 5$. By (3.26), $u \equiv 0 \pmod 5$. By (3.27), $w \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{10}}$, $\nu_5(a) > 1$, a contradiction.

Case 2. $v \equiv 1 \pmod 5$. By (3.26), $u \equiv -w \pmod 5$. By (3.27), $\nu_5(u) = 0$.

2.1. $u \equiv \pm 1 \pmod 5$. By (3.27), $2a \equiv 0 \pmod 5$, a contradiction.

2.2. $u \equiv \pm 2 \pmod 5$. By (3.27), $\pm 1 \equiv 0 \pmod 5$, a contradiction.

Case 3. $v \equiv -1 \pmod 5$. By (3.26), $u \equiv w \pmod 5$. Since $C \equiv 0 \pmod{5^6}$, $\nu_5(u) = 0$.

3.1. $u \equiv \pm 1 \pmod 5$. By (3.27), $\pm 2 \equiv 0 \pmod 5$, a contradiction.

3.2. $u \equiv \pm 2 \pmod 5$. By (3.27), $2a \equiv 0 \pmod 5$, a contradiction.

Case 4. $v \equiv 2 \pmod 5$. By (3.26), $u \equiv -2w \pmod 5$. Since $C \equiv 0 \pmod{5^6}$, $\nu_5(u) = 0$.

4.1. $u \equiv 2 \pmod 5$ and $w \equiv -1 \pmod 5$. By (3.27), $a \equiv -2 \pmod 5$. Since $D \equiv 0 \pmod{5^8}$, $2 \equiv 0 \pmod 5$, a contradiction.

4.2. $u \equiv -2 \pmod 5$ and $w \equiv 1 \pmod 5$. By (3.27), $a \equiv 2 \pmod 5$. Since $D \equiv 0 \pmod{5^8}$, $2 \equiv 0 \pmod 5$, a contradiction.

Case 5. $v \equiv -2 \pmod 5$. By (3.26), $u \equiv 2w \pmod 5$. Since By (3.27), $\nu_5(u) = 0$.

5.1. $u \equiv 2 \pmod 5$ and $w \equiv 1 \pmod 5$. By (3.27), $a \equiv -2 \pmod 5$. Since $D \equiv 0 \pmod{5^8}$, $1 \equiv 0 \pmod 5$, a contradiction.

5.2. $u \equiv -2 \pmod 5$ and $w \equiv -1 \pmod 5$. By (3.27), $a \equiv 2 \pmod 5$. Since $D \equiv 0 \pmod{5^8}$, $1 \equiv 0 \pmod 5$, a contradiction.

Hence $k \leq 1$.

Consider $k = 1$. According to Remark 3.2.1, we may assume that $t, u, v, w \in \{-2, -1, 0, 1, 2\}$. Since $B \equiv 0 \pmod{5^2}$,

$$2t^2 + au + avw \equiv 0 \pmod 5. \tag{3.28}$$

Since $C \equiv 0 \pmod{5^3}$,

$$2t^3 + 3atu + a^2v - auv^2 - au^2w + 3atvw + a^2w^2 \equiv 0 \pmod{5^2}. \tag{3.29}$$

Since $D \equiv 0 \pmod{5^4}$,

$$\begin{aligned} &- t^4 - 3at^2u - a^2u^2 - 2a^2tv - au^3v + 2atuv^2 + a^2v^3 - a^3w \\ &+ 2atu^2w - 3at^2vw + a^2uvw - 2a^2tw^2 - a^2v^2w^2 + a^2uw^3 \equiv 0 \pmod{p^4}. \end{aligned} \tag{3.30}$$

Case 1. $t = 0$. By (3.28),

$$u + vw \equiv 0 \pmod 5. \tag{3.31}$$

By (3.29),

$$av - uv^2 - u^2w + aw^2 \equiv 0 \pmod{5^2}. \tag{3.32}$$

1.1. $v = 0$. By (3.31), $u = 0$. By (3.32), $w = 0$. Since $E \equiv 0 \pmod{5^5}$, $\nu_5(a) \geq 1$, a contradiction.

1.2. $v = 1$. By (3.31), $u = -w$. By (3.32), $\nu_5(u) = 0$.

1.2.1. $u = \pm 1$. Since $C \equiv 0 \pmod{5^3}$, $2a \equiv 0 \pmod 5$, a contradiction.

1.2.2. $u = \pm 2$. Since $C \equiv 0 \pmod{5^3}$, $\pm 1 \equiv 0 \pmod 5$, a contradiction.

1.3. $v = -1$. By (3.31), $u = w$. Since $C \equiv 0 \pmod{5^3}$, $\nu_5(u) = 0$.

1.3.1. $u = \pm 1$. By (3.32), $\pm 2 \equiv 0 \pmod 5$, a contradiction.

1.3.2. $u = \pm 2$. By (3.32), $2a \equiv 0 \pmod 5$, a contradiction.

1.4. $v = 2$. By (3.31), $u = -2w$. Since $C \equiv 0 \pmod{5^3}$, $\nu_5(u) = 0$.

1.4.1. $u = 2$ and $w = -1$. By (3.32), $a \equiv -2 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $2 \equiv 0 \pmod 5$, a contradiction.

1.4.2. $u = -2$ and $w = 1$. By (3.32), $a \equiv 2 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $2 \equiv 0 \pmod 5$, a contradiction.

1.5. $v = -2$. By (3.31), $u = 2w$. Since $C \equiv 0 \pmod{5^3}$, $\nu_5(u) = 0$.

1.5.1. $u = 2$ and $w = 1$. By (3.32), $a \equiv -2 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $1 \equiv 0 \pmod 5$, a contradiction.

1.5.2. $u = -2$ and $w = -1$. By (3.32), $a \equiv 2 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $1 \equiv 0 \pmod 5$, a contradiction.

Case 2. $t = 1$. By (3.28), $au + avw \equiv -2 \pmod 5$.

2.1. $a \equiv 1 \pmod 5$. Then $u + vw \equiv -2 \pmod 5$.

2.1.1. $u = 0$. Then $vw \equiv -2 \pmod 5$.

2.1.1.1. $v = 1$ and $w = -2$.

2.1.1.2. $v = -1$ and $w = 2$.

2.1.1.3. $v = 2$ and $w = -1$.

2.1.1.4. $v = -2$ and $w = 1$.

The subcases 2.1.1.1 to 2.1.1.3 contradict (3.29). The subcase 2.1.1.4 contradicts (3.30).

2.1.2. $u = 1$. Then $vw \equiv 2 \pmod 5$.

2.1.2.1. $v = 1$ and $w = 2$.

2.1.2.2. $v = -1$ and $w = -2$.

2.1.2.3. $v = 2$ and $w = 1$.

2.1.2.4. $v = -2$ and $w = -1$.

The subcases 2.1.2.1, 2.1.2.3 and 2.1.2.4 contradict (3.29). The subcase 2.1.2.2 contradicts (3.30).

2.1.3. $u = -1$. Then $vw \equiv -1 \pmod 5$.

2.1.3.1. $v = 1$ and $w = -1$.

2.1.3.2. $v = -1$ and $w = 1$.

2.1.3.3. $v = 2$ and $w = 2$.

2.1.3.4. $v = -2$ and $w = -2$.

The subcases 2.1.3.2 to 2.1.3.4 contradict (3.29). For the subcase 2.1.3.1, we substitute t, u, v and w in A, B, C, D and E, so we have $A = 5$, $B = 10 - 10a$, $C = 10 - 20a + 10a^2$, $D = -5 + 15a - 15a^2 + 5a^3$ and $E = 1 - 4a + 6a^2 - 4a^3 + a^4$. Since $E \equiv 0 \pmod{5^5}$, $a \equiv 1 \pmod{5^2}$. Then δ is a 5-integral element, so $k = 1$.

2.1.4. $u = 2$. Then $vw \equiv 1 \pmod 5$.

2.1.4.1. $v = 1$ and $w = 1$.

2.1.4.2. $v = -1$ and $w = -1$.

2.1.4.3. $v = 2$ and $w = -2$.

2.1.4.4. $v = -2$ and $w = 2$.

The subcases 2.1.4.1 to 2.1.4.4 contradict (3.29).

2.1.5. $u = -2$. Then $vw \equiv 0 \pmod 5$.

2.1.5.1. $v = 0$. By (3.29), we have, $w^2 - 4w - 4 \equiv 0 \pmod 5$, a contradiction.

2.1.5.2. $w = 0$. By (3.29), we have, $2v^2 + v - 4 \equiv 0 \pmod 5$, a contradiction.

2.2. $a \equiv -1 \pmod 5$. Then $u + vw \equiv 2 \pmod 5$.

2.2.1. $u = 0$. Then $vw \equiv 2 \pmod 5$.

2.2.1.1. $v = 1$ and $w = 2$.

2.2.1.2. $v = -1$ and $w = -2$.

2.2.1.3. $v = 2$ and $w = 1$.

2.2.1.4. $v = -2$ and $w = -1$.

The subcases 2.2.1.1 to 2.2.1.3 contradict (3.29). The subcase 2.2.1.4 contradicts (3.30).

2.2.2. $u = 1$. Then $vw \equiv 1 \pmod 5$.

2.2.2.1. $v = 1$ and $w = 1$.

2.2.2.2. $v = -1$ and $w = -1$.

2.2.2.3. $v = 2$ and $w = -2$.

2.2.2.4. $v = -2$ and $w = 2$.

The subcases 2.2.2.2 to 2.2.2.4 contradict (3.29). For the subcase 2.2.2.1, we substitute t, u, v and w in A, B, C, D and E, so we have $A = 5$, $B = 10 + 10a$, $C = 10 + 20a + 10a^2$, $D = -5 - 15a - 15a^2 - 5a^3$ and $E = 1 + 4a + 6a^2 + 4a^3 + a^4$. Since $E \equiv 0 \pmod{5^5}$, $a \equiv -1 \pmod{5^2}$. Then δ is a 5-integral element, so $k = 1$.

2.2.3. $u = -1$. Then $vw \equiv -2 \pmod 5$.

2.2.3.1. $v = 1$ and $w = -2$.

2.2.3.2. $v = -1$ and $w = 2$.

2.2.3.3. $v = 2$ and $w = -1$.

2.2.3.4. $v = -2$ and $w = 1$.

The subcases 2.2.3.1, 2.2.3.3 and 2.2.3.4 contradict (3.29). The subcase 2.2.3.2 contradicts (3.30).

2.2.4. $u = 2$. Then $vw \equiv 0 \pmod 5$.

2.2.4.1. $v = 0$. By (3.29), we have, $w^2 - 4w - 4 \equiv \ \pmod 5$, a contradiction.

2.2.4.2. $w = 0$. By (3.29), we have, $2v^2 + v - 4 \equiv \ \pmod 5$, a contradiction.

2.2.5. $u = -2$. Then $vw \equiv -1 \pmod 5$.

2.2.5.1. $v = 1$ and $w = -1$.

2.2.5.2. $v = -1$ and $w = 1$.

2.2.5.3. $v = 2$ and $w = 2$.

2.2.5.4. $v = -2$ and $w = -2$.

The subcases 2.2.5.1 to 2.2.5.4 contradict (3.29).

2.3. $a \equiv 2 \pmod 5$. Then $u + vw \equiv -1 \pmod 5$.

2.3.1. $u = 0$. Then $vw \equiv -1 \pmod 5$.

2.3.1.1. $v = 1$ and $w = -1$.

2.3.1.2. $v = -1$ and $w = 1$.

2.3.1.3. $v = 2$ and $w = 2$.

2.3.1.4. $v = -2$ and $w = -2$.

The subcases 2.3.1.1, 2.3.1.2 and 2.3.1.4 contradict (3.29). The subcase 2.3.1.3 contradicts (3.30).

2.3.2. $u = 1$. Then $vw \equiv -2 \pmod 5$.

2.3.2.1. $v = 1$ and $w = -2$.

2.3.2.2. $v = -1$ and $w = 2$.

2.3.2.3. $v = 2$ and $w = -1$.

2.3.2.4. $v = -2$ and $w = 1$.

The subcases 2.3.2.1 to 2.3.2.4 contradict (3.29).

2.3.3. $u = -1$. Then $vw \equiv 0 \pmod 5$.

2.3.3.1. $v = 0$. By (3.29), we have, $4w^2 - 2w - 4 \equiv 0 \pmod 5$, a contradiction.

2.3.3.2. $w = 0$. By (3.29), we have, $2v^2 + 4v - 4 \equiv 0 \pmod 5$, a contradiction.

2.3.4. $u = 2$. Then $vw \equiv 2 \pmod 5$.

2.3.4.1. $v = 1$ and $w = 2$.

2.3.4.2. $v = -1$ and $w = -2$.

2.3.4.3. $v = 2$ and $w = 1$.

2.3.4.4. $v = -2$ and $w = -1$.

The subcases 2.3.4.1, 2.3.4.3 and 2.3.4.4 contradict (3.29). For the subcase 2.3.4.2, we substitute t, u, v and w in A, B, C, D and E, so we have $A = 5$, $B = 10 + 20a$, $C = 2 + 18a + 32a^2$, $D = -1 - 16a - 27a^2 + 2a^3$ and $E = 1 - 22a + 119a^2 + 22a^3 + a^4$. Since $a \equiv 2 \pmod 5$, $a = 5m + 2$ for some $m \in \mathbb{Z}$. Since $E \equiv 0 \pmod{5^5}$, $1 + 6m + 11m^2 + 6m^3 + m^4 \equiv 0 \pmod 5$, so $m \equiv 1 \pmod 5$. Then δ is a 5-integral element , so $k = 1$.

2.3.5. $u = -2$. Then $vw \equiv 1 \pmod 5$.

2.3.5.1. $v = 1$ and $w = 1$.

2.3.5.2. $v = -1$ and $w = -1$.

2.3.5.3. $v = 2$ and $w = -2$.

2.3.5.4. $v = -2$ and $w = 2$.

The subcases 2.3.5.2 to 2.3.5.4 contradict (3.29). The subcase 2.3.5.1 contradicts (3.30).

2.4. $a \equiv -2 \pmod 5$. Then $u + vw \equiv 1 \pmod 5$.

2.4.1. $u = 0$. Then $vw \equiv 1 \pmod 5$.

2.4.1.1. $v = 1$ and $w = 1$.

2.4.1.2. $v = -1$ and $w = -1$.

2.4.1.3. $v = 2$ and $w = -2$.

2.4.1.4. $v = -2$ and $w = 2$.

The subcases 2.4.1.1, 2.4.1.2 and 2.4.1.4 contradict (3.29). The subcase 2.4.1.3 contradicts (3.30).

2.4.2. $u = 1$. Then $vw \equiv 0 \pmod 5$.

2.4.2.1. $v = 0$. By (3.29), we have, $4w^2 + 2w - 4 \equiv 0 \pmod 5$, a contradiction.

2.4.2.2. $w = 0$. By (3.29), we have, $2v^2 + 4v - 4 \equiv 0 \pmod 5$, a contradiction.

2.4.3. $u = -1$. Then $vw \equiv 2 \pmod 5$.

2.4.3.1. $v = 1$ and $w = 2$.

2.4.3.2. $v = -1$ and $w = -2$.

2.4.3.3. $v = 2$ and $w = 1$.

2.4.3.4. $v = -2$ and $w = -1$.

The subcases 2.4.3.1 to 2.4.3.4 contradict (3.29).

2.4.4. $u = 2$. Then $vw \equiv -1 \pmod 5$.

2.4.4.1. $v = 1$ and $w = -1$.

2.4.4.2. $v = -1$ and $w = 1$.

2.4.4.3. $v = 2$ and $w = 2$.

2.4.4.4. $v = -2$ and $w = -2$.

The subcases 2.4.4.2 to 2.4.4.4 contradict (3.29). The subcase 2.4.4.1 contradicts (3.30).

2.4.5. $u = -2$. Then $vw \equiv -2 \pmod 5$.

2.4.5.1. $v = 1$ and $w = -2$.

2.4.5.2. $v = -1$ and $w = 2$.

2.4.5.3. $v = 2$ and $w = -1$.

2.4.5.4. $v = -2$ and $w = 1$.

The subcases 2.4.5.1, 2.4.5.3 and 2.4.5.4 contradict (3.29). For the subcase 2.4.5.2, we substitute t, u, v and w in A, B, C, D and E, so we have $A = 5$, $B = 10 - 20a$, $C = 2 - 18a + 3a^2$, $D = -1 + 16a - 27a^2 - 2a^3$ and $E = 1 + 22a + 119a^2 - 22a^3 + a^4$. Since $a \equiv -2 \pmod 5$, $a = 5m - 2$ for some $m \in \mathbb{Z}$. Since $E \equiv 0 \pmod{5^5}$, $1 - 6m + 11m^2 - 6m^3 + m^4 \equiv 0 \pmod 5$, so $m \equiv -1 \pmod 5$. Then δ is a 5-integral element, so $k = 1$.

In the cases $t = -1$, $t = 2$ and $t = -2$, we separate them into subcases as same as we do in the case $t = 1$. All subcases of them have a contradiction which is similar to the case $t = 1$. Also they do not have any subcases in which we can get $k = 1$. Thus they are not mentioned here.

Hence we have $k = 1$ whenever $a \equiv 1 \pmod{5^2}$ or $a \equiv -1 \pmod{5^2}$ or ($a = 5m - 2$ and $m \equiv -1 \pmod 5$) or ($a = 5m + 2$ and $m \equiv 1 \pmod 5$), and $k = 0$ otherwise.

(1) Assume that $\nu_5(a) = 1$. Consider $k = 1$. Since $B \equiv 0 \pmod{5^2}$, $\nu_5(t) \geq 1$. Since $C \equiv 0 \pmod{5^3}$, $u(v^2 - uw) \equiv 0 \pmod 5$, so $u \equiv 0 \pmod 5$ or $v^2 - uw \equiv 0 \pmod 5$.

Case 1. $u \equiv 0 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $v^2(v - w^2) \equiv 0 \pmod 5$, so $v \equiv 0 \pmod 5$ or $v - w^2 \equiv 0 \pmod 5$.

1.1. $v \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^5}$, $a^4 - a^3w^5 \equiv 0 \pmod{5^5}$, so $a \equiv w^5 \pmod{5^2}$. Since $\nu_5(a) = 1$, we have a contradiction.

1.2. $v - w^2 \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^5}$, $v \equiv 0 \pmod 5$. Then $w \equiv 0 \pmod 5$, so $a^4 \equiv 0 \pmod{5^5}$, a contradiction.

Case 2. $v^2 - uw \equiv 0 \pmod 5$.

2.1. $uw \equiv 0 \pmod 5$. Then ($u \equiv 0 \pmod 5$ or $w \equiv 0 \pmod 5$) and $v \equiv 0 \pmod 5$.

2.1.1. $u \equiv 0 \pmod 5$ and $v \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^5}$, $a^4 - a^3w^5 \equiv 0 \pmod{5^5}$, so $a \equiv w^5 \pmod{5^2}$. Since $\nu_5(a) = 1$, we have a contradiction.

2.1.2. $w \equiv 0 \pmod 5$ and $v \equiv 0 \pmod 5$. Since $D \equiv 0 \pmod{5^4}$, $u \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^5}$, $a^4 \equiv 0 \pmod{5^5}$, a contradiction.

2.2 $\nu_5(uw) = 0$. Then $\nu_5(u) = \nu_5(v) = \nu_5(w) = 0$. Since $D \equiv 0 \pmod{5^4}$, $u^3v \equiv 0 \pmod 5$, a contradiction.

Hence $k = 0$.

(2) Assume that $\nu_5(a) = 2$. Then $\theta^4/5$ is a 5-integral element, so $k \geq 1$. Consider $k = 2$. According to Remark 3.2.1 we may consider $0 \leq t, u, v, w < 5^2$. Since $A \equiv 0 \pmod{5^2}$, $\nu_5(t) \geq 1$. Suppose that $\nu_5(t) > 1$. Then $t = 0$. Since $B \equiv 0 \pmod{5^4}$,

$$u + vw \equiv 0 \pmod 5. \tag{3.33}$$

Since $C \equiv 0 \pmod{5^6}$,

$$u(v^2 + uw) \equiv 0 \pmod{5^2}. \tag{3.34}$$

Case 1. $u = 0$. By (3.33), $\nu_5(vw) \geq 1$. Since $E \equiv 0 \pmod{5^{10}}$,

$$a^4 + 5a^3vw^3 - a^3w^5 \equiv 0 \pmod{5^9} \tag{3.35}$$

and

$$a^3w^5 \equiv 0 \pmod{5^7}. \tag{3.36}$$

By (3.36), $\nu_5(w) \geq 1$. By (3.35), $\nu_5(a) > 2$, a contradiction.

Case 2. $\nu_5(u) = 0$. Since $E \equiv 0 \pmod{5^{10}}$, $au^5 \equiv 0 \pmod{5^4}$, so $\nu_5(a) > 2$, a contradiction.

Case 3. $\nu_5(u) = 1$. By (3.34), $\nu_5(v) \geq 1$. Since $D \equiv 0 \pmod{5^8}$, $\nu_5(w) \geq 1$. Since $E \equiv 0 \pmod{5^{10}}$, $au^5 \equiv 0 \pmod{5^8}$, a contradiction.
Thus $\nu_5(t) = 1$.

Case 1. $\nu_5(u) = 0$. Since $E \equiv 0 \pmod{5^{10}}$, $au^5 \equiv 0 \pmod{5^4}$, so $\nu_5(a) > 2$, a contradiction.

Case 2. $u = 0$ or $\nu_5(u) = 1$. Since $E \equiv 0 \pmod{5^{10}}$, $a^2v^5 \equiv 0 \pmod{5^5}$, so $\nu_5(v) \geq 1$. Since $B \equiv 0 \pmod{5^4}$, $\nu_5(t) > 1$, a contradiction.
Hence $k = 1$.

(3) Assume that $\nu_5(a) = 3$. Then $\theta^4/5^2$ is a 5-integral element, so $k \geq 2$. Consider $k = 3$. Since $A \equiv 0 \pmod{5^3}$, $\nu_5(t) \geq 2$. Since $B \equiv 0 \pmod{5^6}$,

$$u + vw \equiv 0 \pmod 5. \tag{3.37}$$

Since $C \equiv 0 \pmod{5^9}$,

$$u(v^2 + uw) \equiv 0 \pmod{5^2}. \tag{3.38}$$

Since $D \equiv 0 \pmod{5^{12}}$,

$$u^3 v \equiv 0 \pmod{5^2}. \tag{3.39}$$

Case 1. $u = 0$.

1.1. $t = 0$. Since $B \equiv 0 \pmod{5^6}$, $vw \equiv 0 \pmod{5^2}$.

1.1.1. $\nu_5(v) = 0$. Then $\nu_5(w) \geq 2$. Since $C \equiv 0 \pmod{5^9}$, $5a^2 v \equiv 0 \pmod{5^8}$, a contradiction.

1.1.2. $\nu_5(v) = 1$. Then $\nu_5(w) \geq 1$. Since $C \equiv 0 \pmod{5^9}$, $5a^2 v \equiv 0 \pmod{5^9}$, a contradiction.

1.1.3. $v = 0$ or $\nu_5(v) = 2$. Since $C \equiv 0 \pmod{5^9}$, $\nu_5(w) \geq 1$. Since $E \equiv 0 \pmod{5^{15}}$, $a^4 \equiv 0 \pmod{5^{14}}$, a contradiction.

1.2 $\nu_5(t) = 2$. Since $B \equiv 0 \pmod{5^6}$, $\nu_5(v) < 2, \nu_5(w) < 2$ and $\nu_p(v) = 1$ or $\nu(w) = 1$ but not both.

1.2.1. $\nu_5(v) = 1$ and $\nu_5(w) = 0$. Since $C \equiv 0 \pmod{5^9}$, $5a^2 w^2 \equiv 0 \pmod{5^8}$, a contradiction.

1.2.2. $\nu_5(v) = 0$ and $\nu_5(w) = 1$. Since $E \equiv 0 \pmod{5^{15}}$, $a^2 v^5 \equiv 0 \pmod{5^7}$, a contradiction.

Case 2. $\nu_5(u) = 0$. By (3.37), $\nu_5(v) = \nu_5(w) = 0$ contradicting (3.39).

Case 3. $\nu_5(u) = 1$. By (3.37), $vw \equiv 0 \pmod 5$. By (3.38), $v \equiv 0 \pmod 5$. Since $D \equiv 0 \pmod{5^{12}}$, $w \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{15}}$, $au^5 \equiv 0 \pmod{5^9}$, a contradiction.

Case 4. $\nu_5(u) = 2$. By (3.37), $vw \equiv 0 \pmod 5$. Since $C \equiv 0 \pmod{5^9}$, $5auv^2 \equiv 0 \pmod{5^7}$, so $v \equiv 0 \pmod 5$.

4.1. $\nu_5(v) = 1$.

4.1.1. $t = 0$. Since $B \equiv 0 \pmod{5^6}$, $w \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{15}}$, $a^2 v^5 \equiv 0 \pmod{5^{12}}$, a contradiction.

4.1.2. $\nu_5(t) = 2$. Since $B \equiv 0 \pmod{5^6}$, $\nu_5(w) = 0$. Since $E \equiv 0 \pmod{5^{15}}$, $a^3 w^5 \equiv 0 \pmod{5^{10}}$, a contradiction.

4.2. $v = 0$ or $\nu_5(v) = 2$. Since $B \equiv 0 \pmod{5^6}$, $\nu_5(t) = 3$. Since $C \equiv 0 \pmod{5^9}$, $5a^2 w^2 \equiv 0 \pmod{5^9}$, so $w \equiv 0 \pmod 5$. Since $E \equiv 0 \pmod{5^{15}}$, $a^4 \equiv 0 \pmod{5^{13}}$, a contradiction.

Hence $k = 2$.

(4) Assume that $\nu_5(a) = 4$. Then $\theta^4/5^3$ is a 5-integral element, so $k \geq 3$. Consider $k = 4$. According to Remark 3.2.1, we may consider $0 \leq t, u, v, w < 5^4$. Since $A \equiv 0 \pmod{5^4}$, $\nu_5(t) \geq 3$. Suppose that $\nu_5(t) > 3$. Then $t = 0$. Since $B \equiv 0 \pmod{5^8}$,

$$u + vw \equiv 0 \pmod{5^3}. \tag{3.40}$$

Since $C \equiv 0 \pmod{5^{12}}$,

$$u(v^2 + uw) \equiv 0 \pmod{5^4}. \tag{3.41}$$

Case 1. $\nu_5(u) = 0$. Since $E \equiv 0 \pmod{5^{20}}$, $au^5 \equiv 0 \pmod{5^8}$, so $\nu_5(a) > 4$, a contradiction.

Case 2. $\nu_5(u) = 1$. By (3.41), $\nu_5(v) \geq 1$. Since $D \equiv 0 \pmod{5^{16}}$, $\nu_5(w) \geq 1$. Since $E \equiv 0 \pmod{5^{20}}$, $au^5 \equiv 0 \pmod{5^{10}}$, a contradiction.

Case 3. $\nu_5(u) = 2$. By (3.40), $\nu_5(vw) = 2$. By (3.41), $\nu_5(v) \geq 1$.

3.1 $\nu_5(v) = 1$ and $\nu_5(w) = 1$. Since $E \equiv 0 \pmod{5^{20}}$, $a^2v^5 \equiv 0 \pmod{5^{14}}$, a contradiction.

3.2 $\nu_5(v) = 2$ and $\nu_5(w) = 0$. Since $D \equiv 0 \pmod{5^{16}}$, $\nu_5(w) \geq 1$, a contradiction.

Case 4. $u = 0$ or $\nu_5(u) = 3$. By (3.40), $\nu_5(vw) \geq 3$. Since $D \equiv 0 \pmod{5^{16}}$, $\nu_5(v) \geq 1$. Since $E \equiv 0 \pmod{5^{20}}$,

$$a^4 + 5a^3vw^3 - a^3w^5 \equiv 0 \pmod{5^{17}} \tag{3.42}$$

and

$$a^3w^5 \equiv 0 \pmod{5^{13}}. \tag{3.43}$$

By (3.43), $\nu_5(w) \geq 1$. By (3.42), $\nu_5(a) > 4$, a contradiction.
Thus $\nu_5(t) = 3$. Since $B \equiv 0 \pmod{5^8}$,

$$u + vw \equiv 0 \pmod{5^3}. \tag{3.44}$$

Since $C \equiv 0 \pmod{5^{12}}$,

$$u(v^2 + uw) \equiv 0 \pmod{5^7}. \tag{3.45}$$

4.1. $u = 0$. By (3.44), $\nu_5(vw) \geq 3$. Since $D \equiv 0 \pmod{p^{16}}$, $\nu_5(v) > 2$. Since $E \equiv 0 \pmod{5^{20}}$, $a^3w^5 \equiv 0 \pmod{5^{13}}$, so $\nu_5(w) \geq 1$. Since $B \equiv 0 \pmod{5^8}$, $\nu_5(t) > 3$, a contradiction.

4.2. $\nu_5(u) = 0$. Since $E \equiv 0 \pmod{5^{20}}$, $au^5 \equiv 0 \pmod{5^8}$, a contradiction.

4.3. $\nu_5(u) = 1$. Since $E \equiv 0 \pmod{5^{20}}$, $a^2v^5 \equiv 0 \pmod{5^9}$, so $\nu_5(v) \geq 1$. Since $B \equiv 0 \pmod{5^8}$, $u + vw \equiv 0 \pmod{5^2}$, so $\nu_5(v) = 1$ and $\nu_5(w) = 0$ contradicting (3.45).

4.4. $\nu_5(u) = 2$. By (3.45), $\nu_5(w) \neq 1$. Since $B \equiv 0 \pmod{5^8}$, $\nu_5(vw) \geq 2$.

4.4.1. $\nu_5(w) = 0$. By (3.45), $\nu_5(v) = 1$, a contradiction.

4.4.2. $\nu_5(w) \geq 2$. By (3.45), $\nu_5(v) \geq 2$. Since $E \equiv 0 \pmod{5^{20}}$, $au^5 \equiv 0 \pmod{5^{15}}$, so $\nu_5(u) > 2$, a contradiction.

4.5. $\nu_5(u) = 3$. By (3.45), $\nu_5(v) \geq 2$ and $\nu_5(w) \geq 1$. Since $B \equiv 0 \pmod{5^8}$, so $\nu_5(t) > 3$, a contradiction.

Hence $k = 3$. □

Corollary 3.2.8. *(i) If $a \equiv 1 \pmod{5^2}$, then $(1 - \theta + \theta^2 - \theta^3 + \theta^4)/5$ is a 5-integral element.*

(ii) If $a \equiv -1 \pmod{5^2}$, then $(1 + \theta + \theta^2 + \theta^3 + \theta^4)/5$ is a 5-integral element.

(iii) If $a = 5m + 2$ and $m \equiv 1 \pmod 5$, then $(1 + 2\theta - \theta^2 - 2\theta^3 + \theta^4)/5$ is a 5-integral element.

(iv) If $a = 5m - 2$ and $m \equiv -1 \pmod 5$, then $(1 - 2\theta - \theta^2 + 2\theta^3 + \theta^4)/5$ is a 5-integral element.

Proof. They follow from the proof of Theorem 3.2.7 for $\nu_5(a) = 0$ in the subcases 2.1.3.1, 2.2.2.1, 2.3.4.2 and 2.4.5.2, respectively. □

We now conclude to obtain a p-integral basis, for every rational prime p, of $K = \mathbb{Q}(\theta)$ where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbb{Z}[x]$ with $\nu_p(a) < 5$ as follows.

Theorem 3.2.9. *Let $K = \mathbb{Q}(\theta)$ where θ is a root of the irreducible polynomial $x^5 + a$ in $\mathbb{Z}[x]$ with $\nu_p(a) < 5$. Then a 5-integral basis and $p(\neq 5)$-integral basis of K are given in Table A and Table B, respectively.*

Table A

Condition	5 − integral basis	$\nu_5(d(K))$
$\nu_5(a) = 0$		
$a \equiv 1 \pmod{5^2}$	$\{1, \theta, \theta^2, \theta^3, \delta_1\}$	3
$a \equiv -1 \pmod{5^2}$	$\{1, \theta, \theta^2, \theta^3, \delta_2\}$	3
$a = 5m + 2$ *and* $m \equiv 1 \pmod 5$	$\{1, \theta, \theta^2, \theta^3, \delta_3\}$	3
$a = 5m - 2$ *and* $m \equiv -1 \pmod 5$	$\{1, \theta, \theta^2, \theta^3, \delta_4\}$	3
Otherwise	$\{1, \theta, \theta^2, \theta^3, \theta^4\}$	5
$\nu_5(a) = 1$	$\{1, \theta, \theta^2, \theta^3, \theta^4\}$	9
$\nu_5(a) = 2$	$\{1, \theta, \theta^2, \theta^3/5, \theta^4/5\}$	9
$\nu_5(a) = 3$	$\{1, \theta, \theta^2/5, \theta^3/5, \theta^4/5^2\}$	9
$\nu_5(a) = 4$	$\{1, \theta, \theta^2/5, \theta^3/5^2, \theta^4/5^3\}$	9

In table A, $\delta_1 = (1 - \theta + \theta^2 - \theta^3 + \theta^4)/5$, $\delta_2 = (1 + \theta + \theta^2 + \theta^3 + \theta^4)/5$, $\delta_3 = (1 + 2\theta - \theta^2 - 2\theta^3 + \theta^4)/5$ and $\delta_4 = (1 - 2\theta - \theta^2 + 2\theta^3 + \theta^4)/5$.

Table B

Condition	$p(\neq 5)$ − integral basis	$\nu_p(d(K))$
$\nu_p(a) = 1$	$\{1, \theta, \theta^2, \theta^3, \theta^4\}$	4
$\nu_p(a) = 2$	$\{1, \theta, \theta^2, \theta^3/p, \theta^4/p\}$	4
$\nu_p(a) = 3$	$\{1, \theta, \theta^2/p, \theta^3/p, \theta^4/p^2\}$	4
$\nu_p(a) = 4$	$\{1, \theta, \theta^2/p, \theta^3/p^2, \theta^4/p^3\}$	4

Proof. Table A is obtained from Theorems 3.1.5, 3.2.2, 3.2.3, 3.2.6, 3.2.7 and Corollary 3.2.8. Table B is obtained from Theorems 3.1.5, 3.2.2, 3.2.3, 3.2.4 and 3.2.5. □

We now give examples to illustrate how to use our tables.

Example 3.2.10. Let $K = \mathbb{Q}(\theta)$, where $\theta^5+1500 = 0$. Here $a = 1500 = 2^2\cdot 3\cdot 5^3$. Then $\mathrm{disc}_{K/\mathbb{Q}}(\theta) = 2^8 \cdot 3^4 \cdot 5^{17}$. Consider 2-integral basis, 3-integral basis and 5-integral basis. By Table A, 5-integral basis is $\{1, \theta, \theta^2/5, \theta^3/5, \theta^4/5^2\}$. By Table B, 2-integral basis is $\{1, \theta, \theta^2, \theta^3/2, \theta^4/2\}$ and 3-integral basis is $\{1, \theta, \theta^2, \theta^3, \theta^4\}$. Thus by Theorem 3.1.6, an integral basis of K is $\{1, \theta, \theta^2/5, \theta^3/10, \theta^4/50\}$. From Table A and Table B, $d(K) = 2^4 \cdot 3^4 \cdot 5^9$.

Example 3.2.11. Let $K = \mathbb{Q}(\theta)$, where $\theta^5 + 57 = 0$. Here $a = 57 = 3 \cdot 19$. Then $\mathrm{disc}_{K/\mathbb{Q}}(\theta) = 3^4 \cdot 5^5 \cdot 19^4$. Consider 3-integral basis, 5-integral basis and 19-integral basis. By Table A, 5-integral basis is $\{1, \theta, \theta^2, \theta^3, (1 + 2\theta - \theta^2 - 2\theta^3 + \theta^4)/5\}$. By Table B, 3-integral basis and 19-integral basis are $\{1, \theta, \theta^2, \theta^3, \theta^4\}$. Thus by Theorem 3.1.6, an integral basis of K is $\{1, \theta, \theta^2, \theta^3, (1+2\theta-\theta^2-2\theta^3 + \theta^4)/5\}$. From Table A and Table B, $d(K) = 3^4 \cdot 5^3 \cdot 19^4$.

Example 3.2.12. Let $K = \mathbb{Q}(\theta)$, where $\theta^5 - 19551 = 0$. Here $a = -19551 = -3 \cdot 7^3 \cdot 19$. Then $\mathrm{disc}_{K/\mathbb{Q}}(\theta) = 3^4 \cdot 5^5 \cdot 7^{12} \cdot 19^4$. Consider 3-integral basis, 5-integral basis, 7-integral basis and 19-integral basis. By Table A, 5-integral basis is $\{1, \theta, \theta^2, \theta^3, (1-\theta+\theta^2-\theta^3+\theta^4)/5\}$. By Table B, 3-integral basis and 19-integral basis are $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ and 7-integral basis is $\{1, \theta, \theta^2/7, \theta^3/7, \theta^4/7^2\}$. Thus by Theorem 3.1.6 and the Chinese Remainder Theorem, an integral basis of K is $\{1, \theta, \theta^2/7, \theta^3/7, (-49 + 49\theta - 49\theta^2 + 49\theta^3 + \theta^4)/245\}$. From Table A and Table B, $d(K) = 3^4 \cdot 5^3 \cdot 7^4 \cdot 19^4$.

REFERENCES

1. Alaca, S. p-Integral Bases of Algebraic Number Fields. Util. Math. 56 (1999): 97-106.

2. Alaca, S. p-Integral Bases of A Cubic Field. Proc. Amer. Math. Soc. 126 (1998): 1949-1953.

3. Cohen, H. A Course in Computational Algebraic Number Theory. Berlin: Springer-Verlag, 1993.

4. Marcus, D. A. Number Fields. Berlin: Springer-Verlag, 1977.

VITA

Name: Mr. Yotsanan Meemark

Degree: Bachelor of Science (1st Class Degree Honours), 1998,

Chulalongkorn University, Bangkok, Thailand.