1

PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

PRECISIONSM RESOLUTION TARGETS

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file - Votre référence

Our file - Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

p -INTEGRAL BASES OF ALGEBRAIC NUMBER FIELDS

by

Şaban Alaca

B.Sc. Karadeniz Technical University

M.Sc. University of New Brunswick

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfilment of
the requirements for the degree of
Doctor of Philosophy

Department of Mathematics and Statistics

Carleton University

Ottawa, Ontario

© Copyright

August 1994

National Library
of Canada

Bibliothèque nationale
du Canada

Acquisitions and
Bibliographic Services Branch

Direction des acquisitions et
des services bibliographiques

395 Wellington Street
Ottawa, Ontario
K1A 0N4

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Votre référence

THE AUTHOR HAS GRANTED AN
IRREVOCABLE NON-EXCLUSIVE
LICENCE ALLOWING THE NATIONAL
LIBRARY OF CANADA TO
REPRODUCE, LOAN, DISTRIBUTE OR
SELL COPIES OF HIS/HER THESIS BY
ANY MEANS AND IN ANY FORM OR
FORMAT, MAKING THIS THESIS
AVAILABLE TO INTERESTED
PERSONS.

L'AUTEUR A ACCORDE UNE LICENCE
IRREVOCABLE ET NON EXCLUSIVE
PERMETTANT A LA BIBLIOTHEQUE
NATIONALE DU CANADA DE
REPRODUIRE, PRETER, DISTRIBUER
OU VENDRE DES COPIES DE SA
THESE DE QUELQUE MANIERE ET
SOUS QUELQUE FORME QUE CE SOIT
POUR METTRE DES EXEMPLAIRES DE
CETTE THESE A LA DISPOSITION DES
PERSONNE INTERESSEES.

THE AUTHOR RETAINS OWNERSHIP
OF THE COPYRIGHT IN HIS/HER
THESIS. NEITHER THE THESIS NOR
SUBSTANTIAL EXTRACTS FROM IT
MAY BE PRINTED OR OTHERWISE
REPRODUCED WITHOUT HIS/HER
PERMISSION.

L'AUTEUR CONSERVE LA PROPRIETE
DU DROIT D'AUTEUR QUI PROTEGE
SA THESE. NI LA THESE NI DES
EXTRAITS SUBSTANTIELS DE CELLE-
CI NE DOIVENT ETRE IMPRIMES OU
AUTREMENT REPRODUITS SANS SON
AUTORISATION.

ISBN 0-315-98438-4

Name Saban ALACA

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

MATHEMATICS

SUBJECT TERM

0405

U·M·I

SUBJECT CODE

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS

Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION

General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0680
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0279
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523

Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0288
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS

Language
 General 0679
 Ancient 0289
 Linguistics 0290
 Modern 0291
Literature
 General 0401
 Classical 0294
 Comparative 0295
 Medieval 0297
 Modern 0298
 African 0316
 American 0591
 Asian 0305
 Canadian (English) 0352
 Canadian (French) 0355
 English 0593
 Germanic 0311
 Latin American 0312
 Middle Eastern 0315
 Romance 0313
 Slavic and East European 0314

PHILOSOPHY, RELIGION AND THEOLOGY

Philosophy 0422
Religion
 General 0318
 Biblical Studies 0321
 Clergy 0319
 History of 0320
 Philosophy of 0322
Theology 0469

SOCIAL SCIENCES

American Studies 0323
Anthropology
 Archaeology 0324
 Cultural 0326
 Physical 0327
Business Administration
 General 0310
 Accounting 0272
 Banking 0770
 Management 0454
 Marketing 0338
Canadian Studies 0385
Economics
 General 0501
 Agricultural 0503
 Commerce-Business 0505
 Finance 0508
 History 0509
 Labor 0510
 Theory 0511
Folklore 0358
Geography 0366
Gerontology 0351
History
 General 0578

Ancient 0579
Medieval 0581
Modern 0582
Black 0328
African 0331
Asia, Australia and Oceania 0332
Canadian 0334
European 0335
Latin American 0336
Middle Eastern 0333
United States 0337
History of Science 0585
Law 0398
Political Science
 General 0615
 International Law and Relations 0616
 Public Administration 0617
Recreation 0814
Social Work 0452
Sociology
 General 0626
 Criminology and Penology 0627
 Demography 0938
 Ethnic and Racial Studies 0631
 Individual and Family Studies 0628
 Industrial and Labor Relations 0629
 Public and Social Welfare 0630
 Social Structure and Development 0700
 Theory and Methods 0344
Transportation 0709
Urban and Regional Planning 0999
Women's Studies 0453

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES

Agriculture
 General 0473
 Agronomy 0285
 Animal Culture and Nutrition 0475
 Animal Pathology 0476
 Food Science and Technology 0359
 Forestry and Wildlife 0478
 Plant Culture 0479
 Plant Pathology 0480
 Plant Physiology 0817
 Range Management 0777
 Wood Technology 0746
Biology
 General 0306
 Anatomy 0287
 Biostatistics 0308
 Botany 0309
 Cell 0379
 Ecology 0329
 Entomology 0353
 Genetics 0369
 Limnology 0793
 Microbiology 0410
 Molecular 0307
 Neuroscience 0317
 Oceanography 0416
 Physiology 0433
 Radiation 0821
 Veterinary Science 0778
 Zoology 0472
Biophysics
 General 0786
 Medical 0760

Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleoecology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES

Environmental Sciences 0768
Health Sciences
 General 0566
 Audiology 0300
 Chemotherapy 0992
 Dentistry 0567
 Education 0350
 Hospital Management 0769
 Human Development 0758
 Immunology 0982
 Medicine and Surgery 0564
 Mental Health 0347
 Nursing 0569
 Nutrition 0570
 Obstetrics and Gynecology 0380
 Occupational Health and Therapy 0354
 Ophthalmology 0381
 Pathology 0571
 Pharmacology 0419
 Pharmacy 0572
 Physical Therapy 0382
 Public Health 0573
 Radiology 0574
 Recreation 0575

Speech Pathology 0460
Toxicology 0383
Home Economics 0386

PHYSICAL SCIENCES

Pure Sciences
 Chemistry
 General 0485
 Agricultural 0749
 Analytical 0486
 Biochemistry 0487
 Inorganic 0488
 Nuclear 0738
 Organic 0490
 Pharmaceutical 0491
 Physical 0494
 Polymer 0495
 Radiation 0754
 Mathematics 0405
 Physics
 General 0605
 Acoustics 0986
 Astronomy and Astrophysics 0606
 Atmospheric Science 0608
 Atomic 0748
 Electronics and Electricity 0607
 Elementary Particles and High Energy 0798
 Fluid and Plasma 0759
 Molecular 0609
 Nuclear 0610
 Optics 0752
 Radiation 0756
 Solid State 0611
Statistics 0463
Applied Sciences
 Applied Mechanics 0346
 Computer Science 0984

Engineering
 General 0537
 Aerospace 0538
 Agricultural 0539
 Automotive 0540
 Biomedical 0541
 Chemical 0542
 Civil 0543
 Electronics and Electrical 0544
 Heat and Thermodynamics 0348
 Hydraulic 0545
 Industrial 0546
 Marine 0547
 Materials Science 0794
 Mechanical 0548
 Metallurgy 0743
 Mining 0551
 Nuclear 0552
 Packaging 0549
 Petroleum 0765
 Sanitary and Municipal 0554
 System Science 0790
Geotechnology 0428
Operations Research 0796
Plastics Technology 0795
Textile Technology 0994

PSYCHOLOGY

General 0621
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0989
Psychobiology 0349
Psychometrics 0632
Social 0451

The undersigned hereby recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis,

p -INTEGRAL BASES OF ALGEBRAIC NUMBER FIELDS

submitted by

Şaban Alaca, B.Sc., M.Sc.

in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Dr. Vlastimil Dlab, Chair

Department of Mathematics and Statistics

Dr. Kenneth S. Williams, Thesis Supervisor

Dr. Blair K. Spearman, External Examiner

Carleton University

August 1994

**To my PARENTS
who passed away
during my studies**

Abstract

In this thesis the concept of a p -integral basis is developed. It is shown how a p -integral basis for an algebraic number field can be found. Application is then made to the determination of p -integral bases for both cubic and quartic fields. Integral bases and discriminants of these fields are then obtained from the corresponding p -integral bases.

Acknowledgements

I wish to express my gratitude to Dr. Kenneth S. Williams for his invaluable help and kindness throughout my studies leading to the completion of this thesis and also for financial support provided from his NSERC operating grant.

I would like to thank Karadeniz Technical University, Turkey, for its financial support until March 1993. I would also like to thank the Faculty of Graduate Studies and Research of Carleton University for the financial assistance given to me.

Thanks are also due to Dr. Blair K. Spearman and Dr. James G. Huard for reading a draft of this thesis.

I want to thank my wife Ayşe, who is also a Ph.D. student in the same program, for her help and moral support throughout my studies.

Last but not least I want to thank my mother-in-law, Fatma Bilgin, and my children Furkan, Zahide and Betül for their patience and for keeping me happy during my studies.

Contents

Abstract	i
Acknowledgements	ii
Introduction	v
1 THE RING OF p-INTEGRAL ELEMENTS OF AN ALGEBRAIC NUMBER FIELD	1
1.1 Basic Concepts From Algebraic Number Theory	1
1.2 Properties of p -Integral Algebraic Numbers	5
1.3 p -Integral Basis of an Algebraic Number Field	9
2 p-INTEGRAL BASIS OF A CUBIC FIELD	21
2.1 Properties of p -Integral Elements of a Cubic Field	22
2.2 2-Integral Basis of a Cubic Field	26
2.3 3-Integral Basis of a Cubic Field	39
2.4 $p(> 3)$ -Integral Basis of a Cubic Field	55
2.5 Evaluation of the Discriminant $d(K)$ of a Cubic Field K	60
2.6 Integral Basis of a Cubic Field	63
2.7 Numerical Examples	64
2.8 Integral Basis of a Pure Cubic Field	66
2.9 Alternative Form of an Integral Basis of a Cubic Field	68
2.10 Alternative Form of a p -Integral Basis of a Cubic Field	80
2.11 The Conductor of an Abelian Cubic Field	82

3	p-INTEGRAL BASIS OF A QUARTIC FIELD	86
3.1	Properties of p -Integral Elements of a Quartic Field	86
3.2	2-Integral Basis of a Quartic Field	97
3.3	3-Integral Basis of a Quartic Field	108
3.4	$p(> 3)$ -Integral Basis of a Quartic Field	118
3.5	Integral Basis and Discriminant of a Quartic Field	123
	Conclusion	125
	Bibliography	126

INTRODUCTION

Throughout this thesis Z denotes the domain of rational integers, Q the field of rational numbers, R the field of real numbers, and C the field of complex numbers. A complex number θ is said to be an algebraic number if it is the root of a monic polynomial with rational coefficients, and an algebraic integer if it is the root of a monic polynomial with integral coefficients. A subfield K of C is called an algebraic number field if $K = Q(\theta)$ for some algebraic number θ . The degree $n = [K : Q]$ of the algebraic number field K is the degree of the polynomial in $Q[x]$ of the least degree satisfied by θ .

The set of algebraic integers in K is an integral domain denoted by O_K . It is a classical result that there exist $\omega_1, \omega_2, \dots, \omega_n \in O_K$ such that

$$O_K = Z\omega_1 + Z\omega_2 + \dots + Z\omega_n.$$

The set $\{\omega_1, \omega_2, \dots, \omega_n\}$ is called an integral basis of K . For example when K is a quadratic field, that is $[K : Q] = n = 2$, K can be taken in the form $K = Q(\sqrt{m})$, where m is a squarefree integer, and it is well-known (see for example [56, p. 234]) that

$$O_K = Z + Z\sqrt{m}, \text{ if } m \equiv 2 \text{ or } 3 \pmod{4},$$

and

$$O_K = Z + Z((1 + \sqrt{m})/2), \text{ if } m \equiv 1 \pmod{4}.$$

When K is a cyclotomic field, that is, $K = Q(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$ and m is a positive integer with $m \geq 3$ and $m \not\equiv 2 \pmod{4}$, then $[K : Q] = n = \phi(m)$ (Euler's phi function), and

$$O_K = Z + Z\zeta_m + \cdots + Z\zeta_m^{\phi(m)-1},$$

see for example [55, p. 11].

The discriminant $d(K)$ of the algebraic number field K is the nonzero integer

$$d(\omega_1, \omega_2, \dots, \omega_n) = \begin{vmatrix} \omega_1 & \omega_2 & \cdots & \omega_n \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \vdots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2,$$

where $\{\omega_1, \omega_2, \dots, \omega_n\}$ is any integral basis of K and $\omega_i, \omega_i^{(2)}, \dots, \omega_i^{(n)}$ are the algebraic conjugates of ω_i ($i = 1, 2, \dots, n$). In the case of a quadratic field $K = Q(\sqrt{m})$, we have

$$d(K) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m, \text{ if } m \equiv 2 \text{ or } 3 \pmod{4},$$

and

$$d(K) = \begin{vmatrix} 1 & (1 + \sqrt{m})/2 \\ 1 & (1 - \sqrt{m})/2 \end{vmatrix}^2 = m, \text{ if } m \equiv 1 \pmod{4},$$

and, in the case of a cyclotomic field $K = Q(e^{2\pi i/m})$, we have

$$d(K) = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}},$$

see for example [55, p. 12]. The discriminant $d(K)$ is an extremely important quantity associated with the field. By a famous theorem of Dedekind [12] we know that the primes which divide $d(K)$ are precisely those which ramify in K . We can see this very easily when K is the quadratic field $Q(\sqrt{m})$ as

$$pO_K = \langle p, \sqrt{m} \rangle^2, \text{ if } p|m,$$

$$2O_K = \langle 2, \sqrt{m} \rangle^2, \text{ if } m \equiv 2 \pmod{4},$$

$$2O_K = \langle 2, 1 + \sqrt{m} \rangle^2, \text{ if } m \equiv 3 \pmod{4}.$$

As another example, we mention that for the cyclotomic field $K = Q(e^{2\pi i/p})$, where p is an odd prime, it is easy to check that

$$pO_K = \langle 1 - e^{2\pi i/p} \rangle^{p-1}.$$

Note that $d(K) = (-1)^{(p-1)/2} p^{p-2}$ in this case.

Generally, when $n = [K : Q] > 2$ the problem of determining an integral basis for K (and thus $d(K)$) is a difficult one. There are a great many papers in the literature devoted to this problem. Most are usually concerned with a special class of fields K and the point of view taken often falls under one of the following three headings:

- (1) calculation of numerical tables of integral bases and/or discriminants,
- (2) algorithms for determining integral bases and/or discriminants,
- (3) explicit formulae for an integral basis and/or discriminant.

We shall not be concerned in this thesis with the first two approaches but only with the third.

With respect to approach (1), we just mention that beginning in the 1940's, and continuing to the present time, a great deal of work has been done by various authors in constructing extensive tables of integral bases and/or discriminants of particular classes of algebraic number fields of small degree. We just mention that tables of cubic fields with small discriminants are given in Delone and Faddeev [15], Angell [4],[5], Llorente and Oneto [40]; and that tables of quartic fields with small discriminants appear in Delone, Billevich, Sominskii [14], Godwin [18],[19],[20],[22], Kwon [34] and Pohst [48]. Recent work, mostly unpublished, by Buchmann, Ford, Pohst, and others has significantly extended these and similar tables.

Regarding approach (2) we note that a method of determining an integral basis for an arbitrary algebraic number field K is explained in Berwick's book [8]. However, Berwick's algorithm is not easy to apply to obtain explicit integral bases, and does not work in every case. Arai [6], using ideas of Voronoi [54], has given an algorithm for determining an integral basis of a cubic field. Smadja [50] has given a different

algorithm.

The starting point of our approach lies in a concept discussed briefly in Hasse's monograph [27] on number theory which was first published in English in 1980. The idea introduced there is that of a p -integral basis of an algebraic number field, where p is a rational prime. Our aim in this thesis is to develop the theory behind this concept, and use it to find explicit p -integral bases, integral bases, and discriminants in the case of cubic and quartic fields. The basic properties of p -integral bases are developed in Chapter 1. These bases are easier to determine than ordinary integral bases, and moreover, if a p -integral basis in the form specified in Theorem 1.3.4 is known for every prime p then an integral basis for the field K can be constructed from them. In Chapter 2, the theory in Chapter 1 is applied to cubic fields and in Chapter 3 to quartic fields.

In the case of a cubic field K , we take K in the form

$$K = Q(\theta) , \theta^3 - a\theta + b = 0 ,$$

where $X^3 - aX + b \in Z[X]$ is irreducible. Any cubic field can be expressed in this form. A 2-integral basis for K is determined in Theorem 2.2.1, a 3-integral basis in Theorem 2.3.1, and a $p(> 3)$ -integral basis in Theorem 2.4.1. These results appear to be new. In Section 2.5 we use the results of Theorems 2.2.1, 2.3.1 and 2.4.1 to determine an explicit formula for the discriminant of the cubic field K . This formula was first obtained by Llorente and Nart [38] in 1983. Our proof is quite different from theirs. As a consequence of this theorem, we are able to obtain an explicit formula for the index of θ in terms of a and b , see Theorem 2.5.3. In Section 2.6, the p -integral bases for K constructed in Theorems 2.2.1, 2.3.1 and 2.4.1 are used to construct an integral basis for K , see Theorem 2.6.1. Numerical examples illustrating this theorem are provided in Section 2.7. In Section 2.8, Theorem 2.6.1 is specialized to give both an integral basis and the discriminant of the pure cubic field $K = Q(\sqrt[3]{t})$, where t is a cubefree rational integer, thereby reestablishing an old result of Dedekind [13]. Then, in Section 2.9, Theorem 2.6.1 is used to give a new compact form of an integral basis

for $K = Q(\theta)$, $\theta^3 - a\theta + b = 0$, involving (except in one special case) the solution to a pair of congruences of the form

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{n^2}, \\ 3t^2 - a \equiv 0 \pmod{n}, \end{cases}$$

where n is the largest square dividing the discriminant $4a^3 - 27b^2$ of the cubic polynomial $x^3 - ax + b$. This theorem gives an easy way of constructing an integral basis of a given cubic field. Some numerical examples are given at the end of Section 2.9. For other work on integral bases of a cubic field see Bergstrom [7], Mathews [45], Sergeev [49], Tornheim [53] and Maurer [46]. Our Theorem 2.6.1 contains as a special case the work of earlier authors who gave an integral basis in the case of an abelian cubic field, see Albert [2], Chatelet [9], and Martinet and Payan [44]. In Section 2.10, we give an alternative form of a p -integral basis of a cubic field K analogous to Theorem 2.9.1. Finally, in the case of an abelian cubic field, we use Theorem 2.5.1 to rederive the formula of Hasse [26] for the conductor $f(K)$ of the field. Different proofs of this result have been given by Girstmair [17] and Huard, Spearman and Williams [30].

In the case of a quartic field K so as to keep the algebra manageable, we take K in the form

$$K = Q(\theta), \quad \theta^4 + a\theta + b = 0,$$

where $X^4 + aX + b \in Z[X]$ is irreducible. As in the cubic case, we determine a 2-integral basis (except in one case), a 3-integral basis, and a $p(> 3)$ -integral basis for K . These results are new. An explicit integral basis for K can then be constructed from these and the discriminant $d(K)$ determined explicitly (except in the excluded case). A less explicit basis has been given by Grebenyuk [23],[24], which appears to be incorrect in certain cases. The integers of normal quartic fields were considered by Albert [1] in 1930 but as Xianke [58] (and other authors) have pointed out his work contains errors. Edgar and Peterson [16] determined somewhat imprecisely the form of the discriminant of a cyclic quartic field K in 1980. This discriminant was determined explicitly by

Hardy, Hudson, Richman, Williams and Holtz [25] in 1986. Two new proofs of this result have been given by Spearman and Williams [51],[52]. The integers of a cyclic quartic field were given by Hudson and Williams [31] in 1990. Amberg [3], Litver [37], Williams [57] and Motoda [47] have determined the integers and discriminant of a bicyclic quartic field. Integral bases and discriminants of quartic fields possessing a quadratic subfield have been given by Huard, Spearman and Williams [29], extending results of Ledermann and Van der Ploeg [36]. Our theorems are consistent with theirs where they overlap. Kientega and Barrucand [32] have given incomplete results for the discriminant of a quartic field whose Galois group is the symmetric group. We note that our theorem includes the results of Llorente, Nart and Vila [39], when $n = 4$. This work of Llorente, Nart and Vila extends the work of Komatsu [33].

Chapter 1

THE RING OF p -INTEGRAL ELEMENTS OF AN ALGEBRAIC NUMBER FIELD

In Section 1.1 we recall briefly the basic arithmetic properties of an algebraic number field. Proofs of these properties can be found in the standard textbooks on algebraic number theory Cohn [10],[11], Hecke [28], Lang [35], Long [41], Mann [42], Marcus [43], Weiss [56] . In Section 1.2 we introduce the concept of a p -integral element of an algebraic number field K , where p denotes a rational prime, and develop the properties of such elements. In Section 1.3 we define the concept of a p -integral basis of K and show how it can be used to determine the exact power of p dividing the discriminant of K . In Theorem 1.3.4 we show how to find a p -integral basis of K . Finally in Theorem 1.3.6 we show how an integral basis of K can be obtained from the p -integral bases given in Theorem 1.3.4.

1.1 Basic Concepts From Algebraic Number Theory

The field of complex numbers is denoted by C , the field of real numbers by R , the field of rational numbers by Q , and the domain of ordinary integers by Z . First we recall the definition of an algebraic number field and its ring of integers.

Definition 1.1.1 i) If $\alpha \in C$ is a root of a nonzero polynomial with rational coefficients then α is called an algebraic number.

If $\alpha \in C$ is a root of a monic polynomial with rational integer coefficients then α is called an algebraic integer.

ii) Let K be a subfield of C . If $[K : Q] = n$ is finite then K is called an algebraic number field of degree n .

The subset of K consisting of algebraic integers forms a ring O_K , which is called the ring of algebraic integers of K .

All the elements of an algebraic number field are algebraic numbers. The algebraic number field formed by adjoining an algebraic number θ to Q is denoted by $Q(\theta)$. Every algebraic number field is of the form $Q(\theta)$ for some algebraic number θ .

Definition 1.1.2 Let $K = Q(\theta)$ be an algebraic number field of degree n and let $\alpha \in K$. Then

$$\alpha = c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1}, \quad c_j \in Q, \quad 0 \leq j \leq n-1.$$

Let $\theta^{(1)} = \theta, \theta^{(2)}, \dots, \theta^{(n)}$ be the n conjugates of θ , that is, the roots of the minimal polynomial of θ over Q . For $i = 1, 2, \dots, n$ define

$$\alpha^{(i)} = c_0 + c_1\theta^{(i)} + c_2\theta^{(i)2} + \cdots + c_{n-1}\theta^{(i)n-1} \in K^{(i)} = Q(\theta^{(i)}).$$

The set of algebraic numbers

$$\{\alpha = \alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}\}$$

is called a complete set of conjugates of α with respect to K .

It is important to note that $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ do not depend upon the choice of θ defining K .

Definition 1.1.3 Let K be an algebraic number field of degree n , and let $\alpha_1, \alpha_2, \dots, \alpha_n$ be n elements of K . The discriminant $d(\alpha_1, \alpha_2, \dots, \alpha_n)$ of $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is defined by

$$d(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \cdots & \alpha_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}^2, \quad (1.1.1)$$

where for each i ($1 \leq i \leq n$) $\{\alpha_i^{(1)} = \alpha_i, \alpha_i^{(2)}, \dots, \alpha_i^{(n)}\}$ is a complete set of conjugates of α_i with respect to K .

It is easy to see that if the elements $\omega_1, \omega_2, \dots, \omega_n$ of K are related to the elements $\alpha_1, \alpha_2, \dots, \alpha_n$ of K by

$$\omega_i = \sum_{j=1}^n c_{ij} \alpha_j; \quad c_{ij} \in Q, \quad 1 \leq i, j \leq n, \quad (1.1.2)$$

then

$$d(\omega_1, \omega_2, \dots, \omega_n) = \det(c_{ij})^2 d(\alpha_1, \alpha_2, \dots, \alpha_n). \quad (1.1.3)$$

Definition 1.1.4 Let K be an algebraic number field of degree n , and let $\alpha_1, \alpha_2, \dots, \alpha_n$ be n elements of K . If

$$O_K = \alpha_1 Z + \alpha_2 Z + \cdots + \alpha_n Z$$

then $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is called an integral basis of K .

It is well-known that every algebraic number field K possesses an integral basis. Moreover, it is easy to see that if $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ and $\{\omega_1, \omega_2, \dots, \omega_n\}$ are two integral bases of K then

$$d(\alpha_1, \alpha_2, \dots, \alpha_n) = d(\omega_1, \omega_2, \dots, \omega_n).$$

Definition 1.1.5 Let K be an algebraic number field of degree n , and let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be an integral basis of K . Then the discriminant of K is defined by

$$d(K) = d(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Definition 1.1.6 Let $K = Q(\theta)$ be an algebraic number field of degree n , and let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be an integral basis of K . Let $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ and $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be related by

$$\theta^i = \sum_{j=1}^n c_{ij} \alpha_j ; c_{ij} \in Q, 1 \leq i, j \leq n.$$

Then by (1.1.3) we have

$$d(1, \theta, \theta^2, \dots, \theta^{n-1}) = \det(c_{ij})^2 d(K).$$

The positive integer $|\det(c_{ij})|$ is called the index of θ and is denoted by $i(\theta)$.

We denote $d(1, \theta, \theta^2, \dots, \theta^{n-1})$ by $d(\theta)$, so that

$$d(\theta) = \{i(\theta)\}^2 d(K). \quad (1.1.4)$$

Definition 1.1.7 Let K be an algebraic number field. A fractional ideal (or ideal) of K is a nonempty subset A of K with the following properties:

- i) If $\alpha \in A$ and $\beta \in A$ then $\alpha \pm \beta \in A$.
- ii) If $\alpha \in A$ and $r \in O_K$ then $r\alpha \in A$.
- iii) There exists $\gamma (\neq 0) \in O_K$ such that $\gamma A \subseteq O_K$.

It is a classical result that in an algebraic number field K , every nonzero ideal A of K can be expressed uniquely as a product

$$A = \prod_i P_i^{m_i},$$

where the P_i are distinct prime ideals of O_K and the m_i are integers with only finitely many of them nonzero.

We define

$$\nu_{P_i}(A) = m_i.$$

If $A = \alpha O_K$ is a principal ideal then we use the notation

$$\nu_P(A) = \nu_P(\alpha).$$

We also set

$$\nu_P(0) = +\infty.$$

1.2 Properties of p -Integral Algebraic Numbers

In this section we develop the basic properties of p -integral elements of an algebraic number field.

Definition 1.2.1 *Let K be an algebraic number field and let O_K denote the ring of integral elements of K .*

i) Let P be a prime ideal of O_K and let $\alpha \in K$. If $\nu_P(\alpha) \geq 0$ then α is called a P -integral element of K .

ii) Let p be a rational prime. If $\alpha \in K$ is P -integral for every prime ideal P of O_K such that $P|pO_K$ then α is called a p -integral element of K .

Theorem 1.2.1 *Let K be an algebraic number field.*

i) Let P be a prime ideal of O_K . Then the P -integral elements of K form an integral domain $O_P \supseteq O_K$.

ii) Let p be a rational prime. Then the p -integral elements of K form an integral domain O_p .

iii) Let p be a rational prime. Then

$$O_p = \bigcap_{P|pO_K} O_P. \quad (1.2.1)$$

Proof: i) Let P be a prime ideal of K and let $\alpha, \beta \in O_P$. Then $\nu_P(\alpha) \geq 0$ and

$\nu_p(\beta) \geq 0$. Since

$$\nu_p(\alpha + \beta) \geq \min\{\nu_p(\alpha), \nu_p(\beta)\} \geq 0 \quad (1.2.2)$$

and

$$\nu_p(\alpha\beta) = \nu_p(\alpha) + \nu_p(\beta) \geq 0, \quad (1.2.3)$$

we have $\alpha + \beta \in O_P$ and $\alpha\beta \in O_P$. Hence O_P is an integral domain.

ii) Let p be a rational prime and let $\alpha, \beta \in O_p$. Let P be any prime ideal of O_K such that $P|pO_K$. Then $\nu_P(\alpha) \geq 0$ and $\nu_P(\beta) \geq 0$. By (1.2.2) and (1.2.3) we have $\nu_P(\alpha + \beta) \geq 0$ and $\nu_P(\alpha\beta) \geq 0$. Hence $\alpha + \beta$ and $\alpha\beta$ are both P -integral elements of K for every prime ideal P of O_K dividing pO_K . Thus $\alpha + \beta \in O_P$ and $\alpha\beta \in O_P$. Hence O_p is an integral domain.

iii) This follows from i) and ii). ■

We use the following theorem in Chapter 2 (and in Chapter 3) to give a test whether a given element α of a cubic field K (and of a quartic field K) is p -integral or not for a rational prime p .

Theorem 1.2.2 *Let K be an algebraic number field of degree n and let p denote a rational prime. Let $\alpha \in K$ and let $\alpha = \alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ 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 in $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$, namely,*

$$\left. \begin{array}{l} \alpha^{(1)} + \alpha^{(2)} + \dots + \alpha^{(n)}, \\ \alpha^{(1)}\alpha^{(2)} + \alpha^{(1)}\alpha^{(3)} + \dots + \alpha^{(n-1)}\alpha^{(n)}, \\ \vdots \\ \alpha^{(1)}\alpha^{(2)} \dots \alpha^{(n)}, \end{array} \right\} \quad (1.2.4)$$

are p -integral elements of Q .

Proof: Let α be p -integral element of K . We can express α in the form

$$\alpha = \gamma/d, \text{ where } \gamma \in O_K, d \in Z, d \neq 0, \quad (1.2.5)$$

and there does not exist a rational integer ($\neq \pm 1$) dividing both γ and d . We show that $p \nmid d$. If $p|d$ then

$$d = p^l t, \text{ where } l, t \in Z \text{ with } l \geq 1 \text{ and } p \nmid t.$$

Let

$$pO_K = P_1^{m_1} P_2^{m_2} \dots P_k^{m_k}$$

be the prime decomposition of p in O_K . Then

$$\alpha O_K = d^{-1} \gamma O_K = p^{-l} t^{-1} \gamma O_K = P_1^{-lm_1} \dots P_k^{-lm_k} t^{-1} \gamma O_K.$$

Since α is a p -integral element of K then

$$\nu_{P_i}(\alpha) = \nu_{P_i}(\gamma) - lm_i \geq 0, \quad i = 1, 2, \dots, k.$$

Hence

$$\nu_{P_i}(\gamma) \geq m_i, \quad 1 \leq i \leq k,$$

so that p is a rational integer factor of γ which is a contradiction. Thus $p \nmid d$. Hence

$$\alpha = \gamma/d, \text{ where } \gamma \in O_K, d \in Z, p \nmid d. \quad (1.2.6)$$

As $\gamma \in O_K$ the elementary symmetric functions

$$\left. \begin{array}{l} \gamma^{(1)} + \gamma^{(2)} + \dots + \gamma^{(n)}, \\ \gamma^{(1)}\gamma^{(2)} + \gamma^{(1)}\gamma^{(3)} + \dots + \gamma^{(n-1)}\gamma^{(n)}, \\ \vdots \\ \gamma^{(1)}\gamma^{(2)} \dots \gamma^{(n)}, \end{array} \right\} \quad (1.2.7)$$

are rational integers. Hence, as $p \nmid d$, we see that

$$\left. \begin{aligned} \alpha^{(1)} + \alpha^{(2)} + \dots + \alpha^{(n)} &= (\gamma^{(1)} + \gamma^{(2)} + \dots + \gamma^{(n)})/d, \\ \alpha^{(1)}\alpha^{(2)} + \alpha^{(1)}\alpha^{(3)} + \dots + \alpha^{(n-1)}\alpha^{(n)} &= (\gamma^{(1)}\gamma^{(2)} + \gamma^{(1)}\gamma^{(3)} + \dots + \gamma^{(n-1)}\gamma^{(n)})/d^2, \\ &\dots \\ \alpha^{(1)}\alpha^{(2)} \dots \alpha^{(n)} &= (\gamma^{(1)}\gamma^{(2)} \dots \gamma^{(n)})/d^n, \end{aligned} \right\} \quad (1.2.8)$$

are p -integral elements of Q .

Conversely suppose that α is an element of K such that the quantities (1.2.4) are p -integral elements of Q . If α is not a p -integral element of K then there exists a prime ideal P of K with $P|pO_K$ such that $\nu_P(\alpha) < 0$. The quantities (1.2.4) are the coefficients up to sign of a monic polynomial with rational coefficients which are P -integral, say

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0.$$

As $\alpha^{(1)} = \alpha$ is a root of this polynomial, we have

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0. \quad (1.2.9)$$

Then, using (1.2.9), we obtain

$$\begin{aligned} n\nu_P(\alpha) &= \nu_P(\alpha^n) \\ &= \nu_P(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) \\ &\geq \min(\nu_P(a_{n-1}\alpha^{n-1}), \nu_P(a_{n-2}\alpha^{n-2}), \dots, \nu_P(a_0)) \\ &\geq \min(\nu_P(\alpha^{n-1}), \nu_P(\alpha^{n-2}), \dots, \nu_P(\alpha), 0) \\ &= \nu_P(\alpha^{n-1}) \\ &= (n-1)\nu_P(\alpha), \end{aligned}$$

and so $\nu_P(\alpha) \geq 0$, a contradiction. ■

1.3 p -Integral Basis of an Algebraic Number Field

We begin by defining a p -integral basis of an algebraic number field.

Definition 1.3.1 *Let K be an algebraic number field of degree n and let p denote a rational prime. Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be a basis of K over 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 has the representation

$$\alpha = a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n,$$

where each coefficient a_i is a p -integral element of Q , then $\{\omega_1, \omega_2, \dots, \omega_n\}$ is called a p -integral basis of K .

The next theorem shows the existence of p -integral bases.

Theorem 1.3.1 *Let K be an algebraic number field of degree n and let p denote a rational prime. Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be a basis of K over Q such that the ω_i are p -integral elements of K with $\nu_p(d(\omega_1, \omega_2, \dots, \omega_n))$ minimal. Then $\{\omega_1, \omega_2, \dots, \omega_n\}$ is a p -integral basis of K .*

If $\{u_1, u_2, \dots, u_n\}$ is another p -integral basis of K then

$$\nu_p(d(\omega_1, \omega_2, \dots, \omega_n)) = \nu_p(d(u_1, u_2, \dots, u_n)). \quad (1.3.1)$$

Proof: Since $\nu_p(d(\omega_1, \omega_2, \dots, \omega_n))$ is a nonnegative integer for any basis $\{\omega_1, \omega_2, \dots, \omega_n\}$ of K over Q consisting of p -integral elements of K then such a basis of K over Q exists with $\nu_p(d(\omega_1, \omega_2, \dots, \omega_n))$ minimal. Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be such a basis of K over Q and let ω be a p -integral element of K . Express ω as

$$\omega = a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n ; a_i \in Q, 1 \leq i \leq n.$$

We need to show that the a_i are p -integral elements of Q .

Suppose some a_i is not a p -integral element of Q . Without loss of generality we may take a_i to be a_1 . Then express a_1 as

$$a_1 = \frac{a}{p^k} ; a \in Q , \nu_p(a) = 0 \text{ and } k \geq 1. \quad (1.3.2)$$

As ω is a p -integral element of K then

$$\{\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n, \omega_2, \omega_3, \cdots, \omega_n\}$$

is a basis of K over Q consisting of p -integral elements of K . Using (1.3.2) we obtain

$$\begin{aligned} \nu_p(d(\omega_1, \omega_2, \cdots, \omega_n)) &= \nu_p(d(\frac{a}{p^k}\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n, \omega_2, \cdots, \omega_n)) \\ &= \nu_p(d((\frac{a}{p^k})^2 d(\omega_1, \omega_2, \cdots, \omega_n))) \\ &= -2k + \nu_p(d(\omega_1, \omega_2, \cdots, \omega_n)) \\ &< \nu_p(d(\omega_1, \omega_2, \cdots, \omega_n)), \end{aligned}$$

which is a contradiction. Hence the a_i are p -integral elements of Q , and so $\{\omega_1, \omega_2, \cdots, \omega_n\}$ is a p -integral basis of K . Let $\{u_1, u_2, \cdots, u_n\}$ be another p -integral basis of K . Let $\{u_1, u_2, \cdots, u_n\}$ and $\{\omega_1, \omega_2, \cdots, \omega_n\}$ be related by

$$\omega_i = \sum_{j=1}^n c_{ij}u_j ; c_{ij} \in Q , 1 \leq i, j \leq n,$$

where the c_{ij} are p -integral elements of Q . Then, by (1.1.3),

$$d(\omega_1, \omega_2, \cdots, \omega_n) = \det(c_{ij})^2 d(u_1, u_2, \cdots, u_n),$$

and thus

$$\nu_p(d(\omega_1, \omega_2, \cdots, \omega_n)) = \nu_p(\det(c_{ij})^2) + \nu_p(d(u_1, u_2, \cdots, u_n)). \quad (1.3.3)$$

Since the c_{ij} are p -integral elements of Q then $\det(c_{ij})^2$ is a p -integral element of Q , and so $\nu_p(\det(c_{ij})^2) \geq 0$. Thus, by (1.3.3), we have

$$\nu_p(d(u_1, u_2, \cdots, u_n)) \leq \nu_p(d(\omega_1, \omega_2, \cdots, \omega_n)).$$

Since $\nu_p(d(\omega_1, \omega_2, \dots, \omega_n))$ is minimal, we must have

$$\nu_p(d(u_1, u_2, \dots, u_n)) = \nu_p(d(\omega_1, \omega_2, \dots, \omega_n)).$$

This completes the proof. ■

Theorem 1.3.2 *Let K be an algebraic number field of degree n . Then $\{\omega_1, \omega_2, \dots, \omega_n\}$ is an integral basis of K if and only if it is a p -integral basis of K for every rational prime p .*

Proof: Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be an integral basis of K . Then the ω_i are p -integral elements of K for every rational prime p . Let α be a p -integral element of K , and by (1.2.4) we can express α as

$$\alpha = \gamma/d, \text{ where } \gamma \in O_K, d \in \mathbb{Z} \text{ and } p \nmid d.$$

Then

$$\gamma = b_1\omega_1 + b_2\omega_2 + \dots + b_n\omega_n, \quad b_i \in \mathbb{Z},$$

and

$$\alpha = a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n, \quad a_i = \frac{b_i}{d} \in Q.$$

As $p \nmid d$ and the $b_i = a_i d$ are rational integers, the a_i are p -integral elements of Q .

Conversely suppose that $\{\omega_1, \omega_2, \dots, \omega_n\}$ is a p -integral basis for every rational prime p . By Theorem 1.2.2 each ω_i ($1 \leq i \leq n$) satisfies a monic polynomial whose coefficients are p -integral elements of Q for every rational prime p . Hence the coefficients of the monic polynomial of each ω_i are integral elements of K .

Let α be an integral element of K . Then α is a p -integral element of K for every rational prime p . We can express α as

$$\alpha = a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n,$$

where the a_i are p -integral elements of Q for every rational prime p . Then the a_i are rational integers. Thus $\{\omega_1, \omega_2, \dots, \omega_n\}$ is an integral basis of K . ■

Theorem 1.3.3 (Discriminant Divisor Theorem) *Let K be an algebraic number field of degree n and let p denote a rational prime. Then*

$$\nu_p(d(K)) = \nu_p(d(\omega_1, \omega_2, \dots, \omega_n)) \quad (1.3.4)$$

for any p -integral basis $\{\omega_1, \omega_2, \dots, \omega_n\}$ of K .

Proof: Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be an integral basis of K . Thus

$$d(K) = d(\alpha_1, \alpha_2, \dots, \alpha_n),$$

and so for any prime p we have

$$\nu_p(d(K)) = \nu_p(d(\alpha_1, \alpha_2, \dots, \alpha_n)).$$

As $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is also a p -integral basis of K (Theorem 1.3.2) we have

$$\nu_p(d(\alpha_1, \alpha_2, \dots, \alpha_n)) = \nu_p(d(\omega_1, \omega_2, \dots, \omega_n))$$

for any p -integral basis of K (Theorem 1.3.1). Hence

$$\nu_p(d(K)) = \nu_p(d(\omega_1, \omega_2, \dots, \omega_n)),$$

and the proof is complete. ■

Lemma 1.3.1 *Let θ be a root of a monic irreducible polynomial of degree n with rational integral coefficients, so that $K = Q(\theta)$ is an algebraic number field of degree n . Let p be a rational prime. Let i be an integer with $1 \leq i \leq n-1$. If $x_0, x_1, \dots, x_{i-1}$ and j are rational integers such that*

$$\frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}$$

is p -integral then

$$j \leq \frac{1}{2}(\nu_p(d(\theta)) - \nu_p(d(K))).$$

Proof: Let $\omega_1, \omega_2, \dots, \omega_n$ be a p -integral basis of K . As

$$1, \theta, \theta^2, \dots, \theta^{i-1}, \frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}, \theta^{i+1}, \dots, \theta^{n-1}$$

are n p -integral elements of K , we have by Theorem 1.3.1

$$\nu_p(d(1, \theta, \theta^2, \dots, \theta^{i-1}, \frac{x_0 + x_1\theta + \dots + x_{i-1}\theta^{i-1} + \theta^i}{p^j}, \theta^{i+1}, \dots, \theta^{n-1})) \geq \nu_p(d(\omega_1, \omega_2, \dots, \omega_n)).$$

Hence, by Theorem 1.3.3, we have

$$\nu_p\left(\frac{d(\theta)}{p^{2j}}\right) \geq \nu_p(d(K)),$$

and so

$$\nu_p(d(\theta)) - 2j \geq \nu_p(d(K)),$$

that is

$$j \leq \frac{1}{2} (\nu_p(d(\theta)) - \nu_p(d(K)))$$

as asserted. ■

In the following theorem we show how to find a p -integral basis of an algebraic number field $K = Q(\theta)$ for a rational prime p .

Theorem 1.3.4 *Let θ be the root of a monic irreducible polynomial of degree n with rational integral coefficients. Set $K = Q(\theta)$. 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 $x_0^{(i)}, x_1^{(i)}, \dots, x_{i-1}^{(i)}$ such that*

$$\frac{x_0^{(i)} + x_1^{(i)}\theta + \dots + x_{i-1}^{(i)}\theta^{i-1} + \theta^i}{p^{k_i}}$$

is p -integral. [Clearly k_i exists and is nonnegative, and, by Lemma 1.3.1, we know that

$$k_i \leq \frac{1}{2} (\nu_p(d(\theta)) - \nu_p(d(K))).]$$

Then

$$i) \quad 0 \leq k_1 \leq k_2 \leq \dots \leq k_{n-1},$$

$$ii) \quad \left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a p -integral basis of K ,

and

$$iii) \quad \nu_p(d(K)) = \nu_p(d(\theta)) - 2(k_1 + k_2 + \dots + k_{n-1}).$$

Proof: It is well-known, see for example [42], that K has an integral basis of the form

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{d_1}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{d_2}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{d_{n-1}} \right\},$$

where $y_0^{(1)}, y_0^{(2)}, y_1^{(2)}, \dots, y_0^{(n-1)}, y_1^{(n-1)}, \dots, y_{n-2}^{(n-1)}$ are rational integers and $d_1, d_2, \dots, d_{n-1}$ are positive integers satisfying

$$d_i \equiv 0 \pmod{d_{i-1}} \quad (i = 2, 3, \dots, n-1) \quad \text{and} \quad d_1 d_2 \dots d_{n-1} = i(\theta).$$

As an integral basis of K is always a p -integral basis of K , for any prime p , we see that K has a p -integral basis of the form

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{p^{m_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{m_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right\},$$

where the nonnegative integers $m_1, m_2, \dots, m_{n-1}$ are such that

$$\left. \begin{aligned} p^{m_i} \parallel d_i \quad (i = 1, 2, \dots, n-1) \\ m_1 \leq m_2 \leq \dots \leq m_{n-1} \end{aligned} \right\} \quad (1.3.5)$$

and

$$m_1 + m_2 + \dots + m_{n-1} = \nu_p(i(\theta)). \quad (1.3.6)$$

The maximality of k_i ensures that

$$m_i \leq k_i \quad (i = 1, 2, \dots, n-1). \quad (1.3.7)$$

Now

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a set of n p -integral elements of K so

$$\begin{aligned} & \nu_p \left(d \left(1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right) \right) \\ & \geq \nu_p \left(d \left(1, \frac{y_0^{(1)} + \theta}{p^{m_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{m_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{m_{n-1}}} \right) \right), \end{aligned}$$

that is

$$\nu_p \left(\frac{d(\theta)}{p^{2(k_1+k_2+\dots+k_{n-1})}} \right) \geq \nu_p \left(\frac{d(\theta)}{p^{2(m_1+m_2+\dots+m_{n-1})}} \right).$$

Hence

$$\nu_p(d(\theta)) - 2(k_1 + k_2 + \dots + k_{n-1}) \geq \nu_p(d(\theta)) - 2(m_1 + m_2 + \dots + m_{n-1}),$$

and thus

$$m_1 + m_2 + \dots + m_{n-1} \geq k_1 + k_2 + \dots + k_{n-1}.$$

But, from (1.3.7), we have

$$m_1 + m_2 + \dots + m_{n-1} \leq k_1 + k_2 + \dots + k_{n-1},$$

so that

$$m_1 + m_2 + \dots + m_{n-1} = k_1 + k_2 + \dots + k_{n-1}. \quad (1.3.8)$$

Then, in view of (1.3.7) and (1.3.8), we deduce that

$$m_i = k_i \quad , \quad i = 1, 2, \dots, n-1.$$

Hence

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{p^{k_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a p -integral basis of K . From (1.3.5) we see that

$$0 \leq k_1 \leq k_2 \leq \dots \leq k_{n-1},$$

which is (i).

As $(x_0^{(1)} + \theta)/p^{k_1}$ and $(y_0^{(1)} + \theta)/p^{k_1}$ are both p -integral, their difference $(y_0^{(1)} - x_0^{(1)})/p^{k_1}$ is p -integral, and thus

$$y_0^{(1)} \equiv x_0^{(1)} \pmod{p^{k_1}}.$$

Hence there exists an integer l such that

$$y_0^{(1)} = x_0^{(1)} + p^{k_1} l,$$

and so

$$\frac{y_0^{(1)} + \theta}{p^{k_1}} = \frac{x_0^{(1)} + \theta}{p^{k_1}} + l.$$

Thus

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a p -integral basis for K .

As

$$\frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}} \quad \text{and} \quad \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}}$$

are both p -integral, their difference

$$\frac{(y_0^{(2)} - x_0^{(2)}) + (y_1^{(2)} - x_1^{(2)})\theta}{p^{k_2}}$$

is p -integral. Hence there exist p -integral elements a_0 and a_1 of Q such that

$$\frac{(y_0^{(2)} - x_0^{(2)}) + (y_1^{(2)} - x_1^{(2)})\theta}{p^{k_2}} = a_0 + a_1 \left(\frac{x_0^{(1)} + \theta}{p^{k_1}} \right).$$

Thus

$$y_0^{(2)} = x_0^{(2)} + p^{k_2} a_0 + p^{k_2 - k_1} a_1 x_0^{(1)},$$

$$y_1^{(2)} = x_1^{(2)} + p^{k_2 - k_1} a_1,$$

and so

$$\frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{p^{k_2}} = \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}} + a_0 + a_1 \left(\frac{x_0^{(1)} + \theta}{p^{k_1}} \right).$$

This shows that

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \frac{y_0^{(3)} + y_1^{(3)}\theta + y_2^{(3)}\theta^2 + \theta^3}{p^{k_3}}, \dots, \right. \\ \left. \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a p -integral basis of K . Continuing in this way, we deduce that

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \frac{x_0^{(3)} + x_1^{(3)}\theta + x_2^{(3)}\theta^2 + \theta^3}{p^{k_3}}, \dots, \right. \\ \left. \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\} \quad (1.3.9)$$

is a p -integral basis of K , proving (ii).

As (1.3.9) is a p -integral basis of K , it follows from Definitions 1.1.3 and 1.1.5 that

$$d(K) = \frac{d(\theta)}{p^{2(k_1 + k_2 + \dots + k_{n-1})}}.$$

Hence

$$\nu_p(d(K)) = \nu_p(d(\theta)) - 2(k_1 + k_2 + \dots + k_{n-1}),$$

which is (iii). ■

We remark that in view of part (i) of Theorem 1.3.4 if any $k_i = 0$ then $k_1 = k_2 = \dots = k_{i-1} = 0$. Thus, for example, if we establish for a certain field $K = Q(\theta)$ that $(y + z\theta + \theta^2)/p$ is not p -integral for any rational integers y, z then $(x + \theta)/p$ is not p -integral for any rational integer x .

Theorem 1.3.5 *Let θ be the root of a monic irreducible polynomial of degree n with rational integral coefficients. Set $K = Q(\theta)$. Let p and q be distinct rational primes. Let*

$$\left\{ 1, \frac{x_0^{(1)} + \theta}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{x_0^{(n-1)} + x_1^{(n-1)}\theta + \dots + x_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

be a p -integral basis of K . Let

$$\left\{ 1, \frac{y_0^{(1)} + \theta}{q^{l_1}}, \frac{y_0^{(2)} + y_1^{(2)}\theta + \theta^2}{q^{l_2}}, \dots, \frac{y_0^{(n-1)} + y_1^{(n-1)}\theta + \dots + y_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{q^{l_{n-1}}} \right\},$$

be a q -integral basis of K . Define integers $X_i^{(j)}$ ($i = 0, 1, \dots, j-1$; $j = 1, 2, \dots, n-1$) by

$$\begin{cases} X_i^{(j)} \equiv x_i^{(j)} \pmod{p^{k_j}}, \\ X_i^{(j)} \equiv y_i^{(j)} \pmod{q^{l_j}}. \end{cases}$$

Then

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1} q^{l_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2} q^{l_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}} q^{l_{n-1}}} \right\}$$

is both a p -integral and a q -integral basis of K .

Proof: Define integers $t_i^{(j)}$ ($i = 0, 1, \dots, j-1$; $j = 1, 2, \dots, n-1$) by

$$X_i^{(j)} = x_i^{(j)} + p^{k_j} t_i^{(j)}.$$

As p and q are distinct primes,

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1} q^{l_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2} q^{l_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}} q^{l_{n-1}}} \right\}$$

is a p -integral basis of K if and only if

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{p^{k_1}}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{p^{k_2}}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p^{k_{n-1}}} \right\}$$

is a p -integral basis of K . However this set is a p -integral basis of K as, for $j = 1, 2, \dots, n-1$,

$$\begin{aligned} \frac{X_0^{(j)} + X_1^{(j)}\theta + \dots + X_{j-1}^{(j)}\theta^{j-1} + \theta^j}{p^{k_j}} = \\ \left(\frac{x_0^{(j)} + x_1^{(j)}\theta + \dots + x_{j-1}^{(j)}\theta^{j-1} + \theta^j}{p^{k_j}} \right) + (t_0^{(j)} + t_1^{(j)}\theta + \dots + t_{j-1}^{(j)}\theta^{j-1}). \end{aligned}$$

This completes the proof. ■

Finally in the following theorem we show how an integral basis of K can be obtained from the p -integral bases as given in the form specified in Theorem 1.3.4.

Theorem 1.3.6 *Let θ be the root of a monic irreducible polynomial of degree n with rational integral coefficients. Set $K = Q(\theta)$. Let p denote a rational prime.*

If $p \nmid i(\theta)$ then

$$\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$$

is a p -integral basis for K .

Otherwise let $p_1, p_2, \dots, p_s$ be the distinct primes dividing $i(\theta)$. Let

$$\left\{ 1, \frac{x_{r0}^{(1)} + \theta}{p_r^{k_{r1}}}, \frac{x_{r0}^{(2)} + x_{r1}^{(2)}\theta + \theta^2}{p_r^{k_{r2}}}, \dots, \frac{x_{r0}^{(n-1)} + x_{r1}^{(n-1)}\theta + \dots + x_{r,n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{p_r^{k_{r,n-1}}} \right\}$$

be a p_r -integral basis of K ($r = 1, 2, \dots, s$) as given in Theorem 1.3.4.

Define the integers $X_i^{(j)}$ ($i = 0, 1, \dots, j-1$, $j = 1, 2, \dots, n-1$) by

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

and let

$$T_j = \prod_{r=1}^s p_r^{k_{rj}} \quad (j = 1, 2, \dots, n-1).$$

Then

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{T_1}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{T_2}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\theta + \dots + X_{n-2}^{(n-1)}\theta^{n-2} + \theta^{n-1}}{T_{n-1}} \right\}$$

is an integral basis of K .

Proof: The proof follows by induction from Theorem 1.3.5. ■

Chapter 2

p - INTEGRAL BASIS OF A CUBIC FIELD

Let $K = Q(\theta)$ be a cubic field where θ is a root of the irreducible polynomial

$$f(x) = x^3 - ax + b, \quad a, b \in Z.$$

Let p denote a rational prime. In Section 2.1 we develop the particular properties of p -integral elements of the cubic field K that we shall need. In Section 2.2 and in Section 2.3 we determine respectively a 2-integral basis and a 3-integral basis of K . In Section 2.4 we determine a p -integral basis of K for every rational prime $p > 3$. Using these results in Section 2.5 and in Section 2.6 we give the discriminant $d(K)$ of K and an integral basis of K , respectively. In Section 2.7 we illustrate the results with some numerical examples. In Section 2.8 we deduce some results regarding real cubic fields. In Section 2.9 we give an alternative form of an integral basis of a cubic field and illustrate it with some examples, and in Section 2.10 we give an alternative form of a p -integral basis of a cubic field. Finally in Section 2.11 we rederive the formula of Hasse [26] for the conductor $f(K)$ of an abelian cubic field in a form equivalent to that given by Huard, Spearman and Williams [30].

2.1 Properties of p -Integral Elements of a Cubic Field

Let K be a cubic field. We can suppose that $K = Q(\theta)$, where θ is a root of the irreducible cubic polynomial

$$f(x) = x^3 - ax + b ; \ a, b \in Z. \quad (2.1.1)$$

Clearly $\theta \in O_K$. If for any rational prime p we have $\nu_p(a) \geq 2$ and $\nu_p(b) \geq 3$ then θ/p is an algebraic integer of K whose irreducible polynomial is

$$x^3 - (a/p^2)x + b/p^3.$$

Therefore we can assume that for every rational prime p

$$\nu_p(a) < 2 \quad \text{or} \quad \nu_p(b) < 3. \quad (2.1.2)$$

The discriminant of $f(x)$ (or θ) is the nonzero integer

$$\Delta = d(\theta) = 4a^3 - 27b^2. \quad (2.1.3)$$

By (1.1.4) we have

$$\Delta = i(\theta)^2 d(K), \quad (2.1.4)$$

where $d(K)$ is the discriminant of K and the positive integer $i(\theta)$ is the index of θ . For each prime p , we set

$$s_p = \nu_p(\Delta) \quad \text{and} \quad \Delta_p = \Delta/p^{s_p}, \quad (2.1.5)$$

so that $p \nmid \Delta_p$.

Theorem 2.1.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial (2.1.1) which is assumed to satisfy the simplifying assumption (2.1.2). Let*

$$\alpha = \frac{x + y\theta + z\theta^2}{p^m}, \quad (2.1.6)$$

where $x, y, z, m \in \mathbb{Z}$, $m \geq 0$, and p is a rational prime. Set

$$\left. \begin{aligned} X &= 3x + 2az, \\ Y &= 3x^2 + 4axz - ay^2 + a^2z^2 + 3byz, \\ Z &= x^3 + 2ax^2z - axy^2 + 3bxyz + a^2xz^2 - by^3 + b^2z^3 + abyx^2. \end{aligned} \right\} \quad (2.1.7)$$

Then α is p -integral if and only if

$$X \equiv 0 \pmod{p^m}, Y \equiv 0 \pmod{p^{2m}}, Z \equiv 0 \pmod{p^{3m}}. \quad (2.1.8)$$

Proof: Let $\alpha^{(1)} = \alpha, \alpha^{(2)}, \alpha^{(3)}$ denote the conjugates of α with respect to K . By Theorem 1.2.2, we know that α is p -integral if and only if $\alpha + \alpha^{(2)} + \alpha^{(3)}$, $\alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha^{(2)}\alpha^{(3)}$ and $\alpha\alpha^{(2)}\alpha^{(3)}$ are p -integral in Q . To prove the theorem it is enough to show that

$$\begin{aligned} \alpha + \alpha^{(2)} + \alpha^{(3)} &= X/p^m, \\ \alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha^{(2)}\alpha^{(3)} &= Y/p^{2m}, \\ \alpha\alpha^{(2)}\alpha^{(3)} &= Z/p^{3m}. \end{aligned}$$

Let $\theta, \theta^{(2)}, \theta^{(3)}$ be the three roots of $f(x) = x^3 - ax + b$, so that

$$\left. \begin{aligned} \theta + \theta^{(2)} + \theta^{(3)} &= 0, \\ \theta\theta^{(2)} + \theta\theta^{(3)} + \theta^{(2)}\theta^{(3)} &= -a, \\ \theta\theta^{(2)}\theta^{(3)} &= -b \end{aligned} \right\} \quad (2.1.9)$$

We now use (2.1.9) to compute the three symmetric polynomials

$$\begin{aligned} &\theta^2 + \theta^{(2)2} + \theta^{(3)2}, \\ &\theta^2\theta^{(2)2} + \theta^2\theta^{(3)2} + \theta^{(2)2}\theta^{(3)2}, \\ &\theta\theta^{(2)2} + \theta^2\theta^{(2)} + \theta\theta^{(3)2} + \theta^2\theta^{(3)} + \theta^{(2)}\theta^{(3)2} + \theta^{(2)2}\theta^{(3)}. \end{aligned}$$

First

$$\theta^2 + \theta^{(2)2} + \theta^{(3)2} = (\theta + \theta^{(2)} + \theta^{(3)})^2 - 2(\theta\theta^{(2)} + \theta\theta^{(3)} + \theta^{(2)}\theta^{(3)}) = 2a. \quad (2.1.10)$$

Secondly

$$\theta^2\theta^{(2)^2} + \theta^2\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)^2} = (\theta\theta^{(2)} + \theta\theta^{(3)} + \theta^{(2)}\theta^{(3)})^2 - 2\theta\theta^{(2)}\theta^{(3)}(\theta + \theta^{(2)} + \theta^{(3)}) = a^2. \quad (2.1.11)$$

Thirdly

$$\begin{aligned} & \theta\theta^{(2)^2} + \theta^2\theta^{(2)} + \theta\theta^{(3)^2} + \theta^2\theta^{(3)} + \theta^{(2)}\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)} \\ &= \theta\theta^{(2)}(\theta^{(2)} + \theta) + \theta\theta^{(3)}(\theta^{(3)} + \theta) + \theta^{(2)}\theta^{(3)}(\theta^{(3)} + \theta^{(2)}) \\ &= -3\theta\theta^{(2)}\theta^{(3)} = 3b. \end{aligned} \quad (2.1.12)$$

As $\alpha, \alpha^{(2)}, \alpha^{(3)}$ are the conjugates of α with respect to K , we have

$$\alpha = \frac{x + y\theta + z\theta^2}{p^m}, \quad \alpha^{(2)} = \frac{x + y\theta^{(2)} + z\theta^{(2)^2}}{p^m}, \quad \alpha^{(3)} = \frac{x + y\theta^{(3)} + z\theta^{(3)^2}}{p^m}.$$

We now make use of (2.1.9)–(2.1.12) to determine

$$\alpha + \alpha^{(2)} + \alpha^{(3)}, \alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha^{(2)}\alpha^{(3)} \quad \text{and} \quad \alpha\alpha^{(2)}\alpha^{(3)}.$$

First

$$\begin{aligned} \alpha + \alpha^{(2)} + \alpha^{(3)} &= [3x + y(\theta + \theta^{(2)} + \theta^{(3)}) + z(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2})]/p^m \\ &= (3x + 2az)/p^m = X/p^m. \end{aligned}$$

Secondly

$$\begin{aligned} & \alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha^{(2)}\alpha^{(3)} \\ &= \frac{1}{p^{2m}} [(x + y\theta + z\theta^2)(x + y\theta^{(2)} + z\theta^{(2)^2}) + (x + y\theta + z\theta^2)(x + y\theta^{(3)} + z\theta^{(3)^2}) \\ & \quad + (x + y\theta^{(2)} + z\theta^{(2)^2})(x + y\theta^{(3)} + z\theta^{(3)^2})] \\ &= \frac{1}{p^{2m}} [3x^2 + 2xz(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2}) + y^2(\theta\theta^{(2)} + \theta\theta^{(3)} + \theta^{(2)}\theta^{(3)}) \\ & \quad + z^2(\theta^2\theta^{(2)^2} + \theta^2\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)^2}) + yz(\theta\theta^{(2)^2} + \theta^2\theta^{(2)} + \theta\theta^{(3)^2} + \theta^2\theta^{(3)} \\ & \quad + \theta^{(2)}\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)})] \\ &= \frac{1}{p^{2m}} (3x^2 + 4axz - ay^2 + a^2z^2 + 3byz) = Y/p^{2m}. \end{aligned}$$

Thirdly

$$\begin{aligned}
\alpha\alpha^{(2)}\alpha^{(3)} &= (x + y\theta + z\theta^2)(x + y\theta^{(2)} + z\theta^{(2)^2})(x + y\theta^{(3)} + z\theta^{(3)^2})/p^{3m} \\
&= [x^3 + x^2z(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2}) + xy^2(\theta^{(2)}\theta^{(3)} + \theta\theta^{(3)} + \theta\theta^{(2)}) \\
&\quad + xyz(\theta^{(2)}\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)} + \theta\theta^{(3)^2} + \theta^2\theta^{(3)} + \theta\theta^{(2)^2} + \theta^2\theta^{(2)}) \\
&\quad + xz^2(\theta^{(2)^2}\theta^{(3)^2} + \theta^2\theta^{(3)^2} + \theta^2\theta^{(2)^2}) + y^3\theta\theta^{(2)}\theta^{(3)} + z^3\theta^2\theta^{(2)^2}\theta^{(3)^2} \\
&\quad + y^2z(\theta\theta^{(2)}\theta^{(3)^2} + \theta\theta^{(2)^2}\theta^{(3)} + \theta^2\theta^{(2)}\theta^{(3)}) \\
&\quad + yz^2(\theta\theta^{(2)^2}\theta^{(3)^2} + \theta^2\theta^{(2)}\theta^{(3)^2} + \theta^2\theta^{(2)^2}\theta^{(3)})]/p^{3m} \\
&= (x^3 + 2ax^2z - axy^2 + 3bxyz + a^2xz^2 \\
&\quad - by^3 + b^2z^3 + abyz^2)/p^{3m} \\
&= Z/p^{3m}
\end{aligned}$$

which completes the proof. ■

Theorem 2.1.2 *With the same notation as in Theorem 2.1.1, set*

$$U = 9by - 2a^2z,$$

$$V = 2ay - 3bz,$$

$$X = 3x + 2az,$$

Then,

$$Y = \frac{1}{2^2 3 a^2} (2^2 a^2 X^2 - U^2 - 3 \Delta y^2), \quad (2.1.13)$$

$$\begin{aligned}
Z &= \frac{1}{2^2 3^3 a^3} (2^2 a^3 X^3 - 3aXU^2 - 3^2 a \Delta X y^2 - 3U^3 - 3^2 \Delta U y^2 \\
&\quad + 2a \Delta U z^2 + 3^3 b V^3 + 23^2 b \Delta V z^2 - \Delta^2 z^3). \quad (2.1.14)
\end{aligned}$$

Proof: Substituting U, V and X into the expressions on the right sides of (2.1.13) and (2.1.14), we obtain the respective left sides. ■

We end this section with the following theorem which plays an important role in the calculation of an integral basis of a cubic field. This theorem is the special case $n = 3$ of Theorem 1.3.4.

Theorem 2.1.3 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial (2.1.1), which is assumed to satisfy the simplifying assumption (2.1.2). Let*

p be a rational prime. Let

$$\frac{u + \theta}{p^i} \quad (u \in Z) \quad \text{and} \quad \frac{x + y\theta + \theta^2}{p^j} \quad (x, y \in Z)$$

be p -integral elements of K having the integers i and j as large as possible. Then

$$\left\{ 1, \frac{u + \theta}{p^i}, \frac{x + y\theta + \theta^2}{p^j} \right\} \quad (2.1.15)$$

is a p -integral basis of K , and

$$\nu_p(d(K)) = s_p - 2(i + j). \quad (2.1.16)$$

As $\nu_p(d(K)) \geq 0$ for every prime p , we see from (2.1.16) that

$$i + j \leq s_p/2. \quad (2.1.17)$$

We deduce from (2.1.17) that if $s_p = 0$ or 1 we have $i = j = 0$, and if $s_p = 2$ or 3 we have $(i, j) = (0, 0), (1, 0)$ or $(0, 1)$. Use will be made of these simple remarks in sections 2.2, 2.3 and 2.4.

2.2 2-Integral Basis of a Cubic Field

In this section we determine a 2-integral basis of a cubic field.

Theorem 2.2.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b; \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Then a 2-integral basis of K is given in the following table. (Note that the notation $a \equiv b \pmod{m}$ has been shortened to $a \equiv b(m)$ in the table.)

Case	Condition	2-integral basis	s_2	$\nu_2(d(K))$
A1	$b \equiv 1(2)$	$\{1, \theta, \theta^2\}$	0	0
A2	$a \equiv 0(2)$ and $b \equiv 2(4)$	$\{1, \theta, \theta^2\}$	2	2
A3	$a \equiv 0(2)$ and $b \equiv 4(8)$	$\{1, \theta, \theta^2/2\}$	4	2
A4	$a \equiv 2(4)$ and $b \equiv 0(8)$	$\{1, \theta, \theta^2/2\}$	5	3
A5	$a \equiv 1(4)$ and $b \equiv 0(4)$	$\{1, \theta, (\theta + \theta^2)/2\}$	2	0
A6	$a \equiv 3(4)$ and $b \equiv 0(4)$	$\{1, \theta, \theta^2\}$	2	2
A7	$a \equiv 1(4)$ and $b \equiv 2(4)$	$\{1, \theta, \theta^2\}$	3	3
A8	$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 1(2)$	$\{1, \theta, (x + y\theta + \theta^2)/2^m\}$ $m = (s_2 - 3)/2$ $3x \equiv -2a \ (2^m)$ $ay \equiv 3(b/2) \ (2^m)$	$s_2 \geq 5$ $s_2 \equiv 1(2)$	3
A9	$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 0(2)$ $\Delta_2 \equiv 3(4)$	$\{1, \theta, (x + y\theta + \theta^2)/2^m\}$ $m = (s_2 - 2)/2$ $3x \equiv -2a \ (2^m)$ $ay \equiv 3(b/2) \ (2^m)$	$s_2 \geq 4$ $s_2 \equiv 0(2)$	2
A10	$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 0(2)$ $\Delta_2 \equiv 1(4)$	$\{1, \theta, (x + y\theta + \theta^2)/2^{m+1}\}$ $m = (s_2 - 2)/2$ $3x \equiv -2a \ (2^{m+1})$ $ay \equiv 3(b/2) + 2^m \ (2^{m+1})$	$s_2 \geq 4$ $s_2 \equiv 0(2)$	0

Table A

Proof: The following flowchart shows that A1-A10 comprise all cases.

Recall that

$$\Delta = 2^2 a^3 - 3^3 b^2, \quad \Delta_2 = \Delta/2^{s_2} \equiv 1 \pmod{2}. \quad (2.2.1)$$

Case A1 : $b \equiv 1 \pmod{2}$.

By (2.2.1), $s_2 = 0$ and $\Delta_2 \equiv 1 \pmod{4}$. Then, by (2.1.16), we have $\nu_2(d(K)) = 0$ and $\{1, \theta, \theta^2\}$ is a 2-integral basis of K .

Case A2 : $a \equiv 0 \pmod{2}$ and $b \equiv 2 \pmod{4}$.

By (2.2.1), $s_2 = 2$ and $\Delta_2 \equiv 1 \pmod{4}$. We show that for every pair of integers x, y , the element $(x+y\theta+\theta^2)/2$ of K is not a 2-integral element of K . Suppose $(x+y\theta+\theta^2)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{2}, \quad (2.2.2)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^2}, \quad (2.2.3)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^3}. \quad (2.2.4)$$

It follows from (2.2.2) that $x \equiv 0 \pmod{2}$. Taking (2.2.4) modulo 4 we obtain $y \equiv 0 \pmod{2}$. Then (2.2.4) becomes $4 \equiv 0 \pmod{8}$, which is a contradiction. By the remark following Theorem 1.3.4, $(x + \theta)/2$ is not a 2-integral element of K for any rational integer x . Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 2$.

Case A3 : $a \equiv 0 \pmod{2}$ and $b \equiv 4 \pmod{8}$.

By (2.2.1), $s_2 = 4$. First we show that for every integer x the element $(x + \theta)/2$ of K is not a 2-integral element of K . Suppose $(x + \theta)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{2},$$

$$3x^2 - a \equiv 0 \pmod{2^2},$$

$$x^3 - ax - b \equiv 0 \pmod{2^3}.$$

Hence $x \equiv 0 \pmod{2}, a \equiv 0 \pmod{4}, b \equiv 0 \pmod{8}$, a contradiction.

Secondly we show that $\theta^2/2$ is a 2-integral element of K . By Theorem 2.1.1, $\theta^2/2$ is a 2-integral element of K if and only if

$$2a \equiv 0 \pmod{2}, \quad a^2 \equiv 0 \pmod{2^2}, \quad b^2 \equiv 0 \pmod{2^3},$$

which clearly holds.

Finally we show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/2^2$ of K is not a 2-integral element of K . Suppose $(x + y\theta + \theta^2)/2^2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{2^2}, \quad (2.2.5)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^4}, \quad (2.2.6)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^6}. \quad (2.2.7)$$

It follows from (2.2.5) that $x \equiv 0 \pmod{4}$. Using this in (2.2.6) and (2.2.7) yields

$$-ay^2 + a^2 + 3by \equiv 0 \pmod{16}, \quad (2.2.8)$$

$$-axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{64}. \quad (2.2.9)$$

Taking (2.2.9) modulo 16 we obtain

$$-axy^2 - by^3 + aby \equiv 0 \pmod{16}. \quad (2.2.10)$$

If $y \equiv 1 \pmod{2}$ (2.2.8) taken modulo 4 gives $a \equiv 0 \pmod{4}$. Then (2.2.10) gives $b \equiv 0 \pmod{16}$, a contradiction. If $y \equiv 0 \pmod{2}$ and $a \equiv 2 \pmod{4}$ then (2.2.8) modulo 8 becomes $4 \equiv 0 \pmod{8}$, a contradiction. If $y \equiv 0 \pmod{2}$ and $a \equiv 0 \pmod{4}$ then (2.2.8) gives $y \equiv 0 \pmod{4}$. Then (2.2.9) gives $16 \equiv 0 \pmod{64}$, a contradiction. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 2$.

Case A4 : $a \equiv 2 \pmod{4}$ and $b \equiv 0 \pmod{8}$.

By (2.2.1), $s_2 = 5$. First we show that for every integer x the element $(x + \theta)/2$ of K is not a 2-integral element of K . Suppose $(x + \theta)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{2}, \quad (2.2.11)$$

$$3x^2 - a \equiv 0 \pmod{2^2}, \quad (2.2.12)$$

$$x^3 - ax - b \equiv 0 \pmod{2^3}. \quad (2.2.13)$$

It follows from (2.2.11) that $x \equiv 0 \pmod{2}$. Then (2.2.12) implies that $a \equiv 0 \pmod{4}$, which is a contradiction.

By Theorem 2.1.1, $\theta^2/2$ is a 2-integral element of K if and only if

$$2a \equiv 0 \pmod{2}, \quad a^2 \equiv 0 \pmod{2^2}, \quad b^2 \equiv 0 \pmod{2^3},$$

which clearly holds.

Next we show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/2^2$ of K is not a 2-integral element of K . Suppose $(x + y\theta + \theta^2)/2^2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{2^2}, \quad (2.2.14)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^4}, \quad (2.2.15)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^6}. \quad (2.2.16)$$

It follows from (2.2.14) that $x \equiv 0 \pmod{4}$. Taking (2.2.15) modulo 8, we get $-ay^2 + 4 \equiv 0 \pmod{8}$, which is impossible.

Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 3$.

Case A5 : $a \equiv 1 \pmod{4}$ and $b \equiv 0 \pmod{4}$.

By (2.2.1), $s_2 = 2$ and

$$\Delta_2 = a^3 - 27(b/2)^2 \equiv 1 \pmod{4}.$$

By Theorem 2.1.1, $(\theta + \theta^2)/2$ is a 2-integral element of K if and only if

$$\begin{cases} 2a \equiv 0 \pmod{2}, \\ -a + a^2 + 3b \equiv 0 \pmod{2^2}, \\ -b + b^2 + ab \equiv 0 \pmod{2^3}, \end{cases}$$

which obviously holds. Then, by (2.1.16), $\nu_2(d(K)) = 0$ and $\{1, \theta, (\theta + \theta^2)/2\}$ is a 2-integral basis of K .

Case A6 : $a \equiv 3 \pmod{4}$ and $b \equiv 0 \pmod{4}$.

By (2.2.1), $s_2 = 2$ and

$$\Delta_2 = a^3 - 27(b/2)^2 \equiv 3 \pmod{4}.$$

We show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/2$ of K is not a 2-integral element of K . Suppose $(x + y\theta + \theta^2)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{2}, \quad (2.2.17)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^2}, \quad (2.2.18)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^3}. \quad (2.2.19)$$

It follows from (2.2.17) that $x \equiv 0 \pmod{2}$. Then (2.2.18) implies that $-3y^2 + 1 \equiv 0 \pmod{4}$ which is impossible. By the remarks following Theorem 1.3.4, $(x + \theta)/2$ is not a 2-integral element of K for any rational integer x . Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 2$.

Case A7 : $a \equiv 1 \pmod{4}$ and $b \equiv 2 \pmod{4}$.

By (2.2.1) we have $s_2 = 3$. We show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/2$ of K is not a 2-integral element of K . Suppose $(x + y\theta + \theta^2)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{2}, \quad (2.2.20)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{2^2}, \quad (2.2.21)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{2^3}. \quad (2.2.22)$$

The congruence (2.2.20) implies that $x \equiv 0 \pmod{2}$. It follows from (2.2.21) that

$$-y^2 + 1 + 2y \equiv 0 \pmod{4}, \quad (2.2.23)$$

which is impossible. By the remark following Theorem 1.3.4, $(x + \theta)/2$ is not 2-integral for any $x \in Z$. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 3$.

Case A8 : $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$ and $s_2 \equiv 1 \pmod{2}$.

As $a \equiv -1 \pmod{4}$ and $b \equiv 2 \pmod{4}$ we have

$$\Delta = 4a^3 - 27b^2 \equiv -4 + 20 \equiv 16 \equiv 0 \pmod{16}, \quad (2.2.24)$$

so that $s_2 = \nu_2(\Delta) \geq 4$. Moreover, as s_2 is odd, we have $s_2 \geq 5$ and we may define a positive integer m by

$$m = \frac{1}{2}(s_2 - 3). \quad (2.2.25)$$

Note that $2^{2m+3} \parallel \Delta$. Define integers x, y and z by

$$\begin{cases} 3x \equiv -2a \pmod{2^m}, \\ ay \equiv 3(b/2) \pmod{2^m}, \\ z = 1. \end{cases} \quad (2.2.26)$$

Then, in the notation of Theorem 2.1.2, we have

$$X = 3x + 2az = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^m}. \quad (2.2.27)$$

Also

$$\begin{aligned} 3bU &= 3b(9by - 2a^2z) \\ &= 27b^2y - 6a^2b \\ &= (4a^3 - \Delta)y - 6a^2b \\ &= 4a^2(ay) - \Delta y - 6a^2b \\ &\equiv 4a^2(3b/2) - 6a^2b \pmod{2^{m+2}} \\ &\equiv 0 \pmod{2^{m+2}}, \end{aligned}$$

so that, as $2 \parallel 3b$, we have

$$U \equiv 0 \pmod{2^{m+1}}.$$

Further

$$V = 2ay - 3bz = 2ay - 3b \equiv 0 \pmod{2^{m+1}}.$$

It follows from (2.1.13) and (2.1.14) that

$$Y \equiv 0 \pmod{2^{2m}} \text{ and } Z \equiv 0 \pmod{2^{3m}}. \quad (2.2.28)$$

Thus it follows from (2.2.27), (2.2.28) and Theorem 2.1.1 that

$$\frac{x + y\theta + \theta^2}{2^m}$$

is a 2-integral element of K , where x and y are given by (2.2.26) and m is given by (2.2.25).

Next we show that for every pair of integers x, y the element

$$\frac{x + y\theta + \theta^2}{2^{m+1}}$$

is not a 2-integral element of K , where m is given by (2.2.25). If $(x + y\theta + \theta^2)/2^{m+1}$ is a 2-integral element of K , then by Theorem 2.1.1, we have

$$2^{m+1} \mid X, \quad 2^{2m+2} \mid Y, \quad 2^{3m+3} \mid Z, \quad \text{where } z = 1. \quad (2.2.29)$$

It follows from (2.1.13) and (2.2.29) that

$$2^{2m+4} \mid U^2 + 3\Delta y^2. \quad (2.2.30)$$

From (2.1.7) it follows that $x \equiv 2 \pmod{4}$ and $y \equiv 1 \pmod{2}$. As $2^{2m+3} \parallel \Delta$ it then follows from (2.2.30) that $2^{2m+3} \parallel U^2$, which is a contradiction.

Finally we show that for every integer x the element $(x+\theta)/2$ of K is not a 2-integral element of K . Suppose $(x+\theta)/2$ is a 2-integral element of K . Then, by Theorem 2.1.1,

we have

$$3x \equiv 0 \pmod{2}, \quad (2.2.31)$$

$$3x^2 - a \equiv 0 \pmod{2^2}, \quad (2.2.32)$$

$$x^3 - ax - b \equiv 0 \pmod{2^3}. \quad (2.2.33)$$

It follows from (2.2.31) and (2.2.32) that $a \equiv 0 \pmod{4}$, which is a contradiction.

Thus, by Theorem 2.1.3, $\{1, \theta, (x+y\theta+\theta^2)/2^m\}$ is a 2-integral basis of K where x and y are given by (2.2.26) and m is given by (2.2.25). Moreover $\nu_2(d(K)) = s_2 - 2m = 3$.

Cases A9–A10 : $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$ and $s_2 \equiv 0 \pmod{2}$.

As $a \equiv -1 \pmod{4}$ and $b \equiv 2 \pmod{4}$ we have

$$\Delta = 4a^3 - 27b^2 \equiv -4 + 20 \equiv 16 \equiv 0 \pmod{16},$$

so that $s_2 = \nu_2(\Delta) \geq 4$. As s_2 is even, we may define a positive integer m by

$$m = \frac{1}{2}(s_2 - 2). \quad (2.2.34)$$

Note that $2^{2m+2} \parallel \Delta$.

Case A9 : $\Delta_2 \equiv 3 \pmod{4}$.

Define integers x, y and z by

$$\begin{cases} 3x \equiv -2a \pmod{2^m}, \\ ay \equiv 3(b/2) \pmod{2^m}, \\ z = 1. \end{cases} \quad (2.2.35)$$

Then, in the notation of Theorem 2.1.2, we have

$$X = 3x + 2az = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^m}. \quad (2.2.36)$$

Also

$$\begin{aligned}
3bU &= 3b(9by - 2a^2z) \\
&= 27b^2y - 6a^2b \\
&= (4a^3 - \Delta)y - 6a^2b \\
&= 4a^2(ay) - \Delta y - 6a^2b \\
&\equiv 4a^2(3b/2) - 6a^2b \pmod{2^{m+2}} \\
&\equiv 0 \pmod{2^{m+2}},
\end{aligned}$$

so that, as $2 \parallel 3b$, we have

$$U \equiv 0 \pmod{2^{m+1}}.$$

Further

$$V = 2ay - 3bz = 2ay - 3b \equiv 3b - 3b \equiv 0 \pmod{2^{m+1}}.$$

It follows from (2.1.13) and (2.1.14) that

$$Y \equiv 0 \pmod{2^{2m}} \text{ and } Z \equiv 0 \pmod{2^{3m}}. \quad (2.2.37)$$

Thus it follows from (2.2.36), (2.2.37) and Theorem 2.1.1 that

$$\frac{x + y\theta + \theta^2}{2^m}$$

is a 2-integral element of K , where x and y are given by (2.2.35) and m is given by (2.2.34).

Next we show that for every pair of integers x, y the element

$$\frac{x + y\theta + \theta^2}{2^{m+1}}$$

is not a 2-integral element of K , where m is given by (2.2.34). If $(x + y\theta + \theta^2)/2^{m+1}$ is a 2-integral element of K , then by Theorem 2.1.1, we have

$$2^{m+1} \mid X, \quad 2^{2m+2} \mid Y, \quad 2^{3m+3} \mid Z, \quad \text{where } z = 1. \quad (2.2.38)$$

It follows from (2.1.13) and (2.2.38) that

$$2^{2m+4}|U^2 + 3\Delta y^2. \quad (2.2.39)$$

From (2.1.7) we see that $x \equiv 2 \pmod{4}$ and $y \equiv 1 \pmod{2}$. As $2^{2m+2} \parallel \Delta$ it then follows from (2.2.39) that

$$2^{2m+2} \parallel U^2 \text{ and } 1 + 3\Delta_2 \equiv 0 \pmod{4},$$

which is impossible as $\Delta_2 \equiv 3 \pmod{4}$.

As in Case A8 the element $(x + \theta)/2$ of K , where $x \in Z$, is not a 2-integral element of K . Thus, by Theorem 2.1.3,

$$\{1, \theta, \frac{x + y\theta + \theta^2}{2^m}\}$$

is a 2-integral basis of K , where x and y are given by (2.2.35) and m is given by (2.2.34).

In addition $\nu_2(d(K)) = s_2 - 2m = 2$.

Case A10 : $\Delta_2 \equiv 1 \pmod{4}$.

Here we define integers x, y and z by

$$\begin{cases} 3x \equiv -2a \pmod{2^{m+1}}, \\ ay \equiv 3(b/2) + 2^m \pmod{2^{m+1}}, \\ z = 1. \end{cases} \quad (2.2.40)$$

Then, in the notation of Theorem 2.1.2, we have

$$X = 3x + 2az = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{2^{m+1}}. \quad (2.2.41)$$

Also

$$\begin{aligned} 3bU &= 3b(9by - 2a^2z) \\ &= 27b^2y - 6a^2b \\ &= (4a^3 - \Delta)y - 6a^2b \\ &= 4a^2(ay) - \Delta y - 6a^2b \\ &\equiv 4a^2(3b/2 + 2^m) - 6a^2b \pmod{2^{m+3}} \\ &\equiv 6a^2b + 2^{m+2}a^2 - 6a^2b \pmod{2^{m+3}} \\ &\equiv 2^{m+2} \pmod{2^{m+3}}, \end{aligned}$$

so that, as $2 \parallel 3b$, we have

$$U \equiv 2^{m+1} \pmod{2^{m+2}}.$$

Further

$$V = 2ay - 3bz = 2ay - 3b \equiv 3b + 2^{m+1} - 3b \equiv 2^{m+1} \pmod{2^{m+2}}.$$

It follows from (2.1.13) that $Y \equiv 0 \pmod{2^{2m+2}}$. Note that Z can be expressed as

$$\begin{aligned} Z = \frac{1}{2^2 3^3 a^3} & \left(\frac{1}{2a^3} (2a^2 X + 9bV - \Delta z)^3 - \frac{3}{a^2} (2a^2 X + 9bV - \Delta z)^2 U + \right. \\ & \frac{3^2}{2a} (2a^2 X + 9bV - \Delta z)(-\Delta y^2 + U^2) - 2^2 U^3 + \\ & \left. 3^2 bV(3V^2 + 2z^2 \Delta) + 2az^2 U \Delta - \Delta^2 z^3 \right). \end{aligned} \quad (2.2.42)$$

We see from (2.2.42) that $Z \equiv 0 \pmod{2^{3m+3}}$. Thus, it follows from Theorem 2.1.1 that

$$\frac{x + y\theta + \theta^2}{2^{m+1}}$$

is a 2-integral element of K , where x and y are given by (2.2.39), and m is given by (2.2.34). Thus, by Theorem 2.1.4,

$$\left\{ 1, \theta, \frac{x + y\theta + \theta^2}{2^{m+1}} \right\}$$

is a 2-integral basis of K and $\nu_2(d(K)) = s_2 - 2(m+1) = 0$.

This completes the treatment of all the cases. ■

Corollary 2.2.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2).

Define integers R_2, S_2, T_2 by

$$\begin{cases} 3R_2 \equiv -2a \pmod{2^{\lfloor s_2/2 \rfloor}} & , \text{ if } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, \\ R_2 = 0 & , \text{ otherwise ;} \end{cases}$$

$$\begin{cases} aS_2 \equiv 3(b/2) + 2^{\lfloor s_2/2 \rfloor - 1} \pmod{2^{\lfloor s_2/2 \rfloor}} & , \text{ if } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, \\ S_2 = 1 & , \text{ if } a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}, \\ S_2 = 0 & , \text{ otherwise ;} \end{cases}$$

$$T_2 = \begin{cases} s_2/2 & , \text{ if } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}, \Delta_2 \equiv 1 \pmod{4}, \\ (s_2 - 2)/2 & , \text{ if } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}, \Delta_2 \equiv 3 \pmod{4}, \\ (s_2 - 3)/2 & , \text{ if } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 1 \pmod{2}, \\ 1 & , \text{ if } a \equiv 0 \pmod{2}, b \equiv 4 \pmod{8} \text{ or} \\ & a \equiv 2 \pmod{4}, b \equiv 0 \pmod{8} \text{ or} \\ & a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4}, \\ 0 & , \text{ otherwise.} \end{cases}$$

Then

$$\left\{ 1, \theta, \frac{R_2 + S_2\theta + \theta^2}{2T_2} \right\}$$

is a 2-integral basis of K .

Proof: This follows immediately from Table A of Theorem 2.2.1. ■

2.3 3-Integral Basis of a Cubic Field

In this section we determine a 3-integral basis of a cubic field.

Theorem 2.3.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in \mathbb{Z},$$

where a and b satisfy the simplifying assumption (2.1.2). Then a 3-integral basis of K is given in the following table.

Case	Condition	3-integral basis	s_3	$\nu_3(d(K))$
B1	$\nu_3(a) = 0$	$\{1, \theta, \theta^2\}$	0	0
B2	$\nu_3(a) = \nu_3(b) = 1$	$\{1, \theta, \theta^2\}$	3	3
B3	$1 = \nu_3(b) < \nu_3(a)$	$\{1, \theta, \theta^2\}$	5	5
B4	$2 = \nu_3(b) = \nu_3(a)$	$\{1, \theta, \theta^2/3\}$	6	4
B5	$2 = \nu_3(b) < \nu_3(a)$	$\{1, \theta, \theta^2/3\}$	7	5
B6	$1 = \nu_3(a) < \nu_3(b)$	$\{1, \theta, \theta^2/3\}$	3	1
B7	$\nu_3(b) = 0, \nu_3(a) \geq 1$ $a \not\equiv 3 \pmod{9}$ $b^2 \equiv a + 1 \pmod{9}$	$\{1, \theta, (1 - b\theta + \theta^2)/3\}$	3	1
B8	$\nu_3(b) = 0, \nu_3(a) \geq 1$ $a \not\equiv 3 \pmod{9}$ $b^2 \not\equiv a + 1 \pmod{9}$	$\{1, \theta, \theta^2\}$	3	3
B9	$\nu_3(b) = 0$ $a \equiv 3 \pmod{9}$ $b^2 \equiv 4 \pmod{9}$ $b^2 \not\equiv a + 1 \pmod{27}$	$\{1, \theta, (1 - b\theta + \theta^2)/3\}$	5	3
B10	$\nu_3(b) = 0$ $a \equiv 3 \pmod{9}$ $b^2 \not\equiv 4 \pmod{9}$	$\{1, \theta, \theta^2\}$	4	4
B11	$\nu_3(b) = 0$ $a \equiv 3 \pmod{9}$ $b^2 \equiv a + 1 \pmod{27}$	$\{1, (b + \theta)/3, (x + y\theta + \theta^2)/3^m\}$ $m = [(s_3 - 2)/2]$ $x \equiv (-2a/3) \pmod{3^m}$ $2ay \equiv 3b \pmod{3^{m+2}}$	$s_3 \geq 6$	$s_3 - 2[s_3/2]$

Table B

Proof: The following flowchart shows that B1-B11 comprise all cases.

Recall that

$$\Delta = 2^2 a^3 - 3^3 b^2, \quad s_3 = \nu_3(\Delta). \quad (2.3.1)$$

Case B1 : $\nu_3(a) = 0$.

By (2.3.1), $s_3 = 0$. Then, by (2.1.16), $\nu_3(d(K)) = 0$ and $\{1, \theta, \theta^2\}$ is a 3-integral basis of K .

Case B2 : $\nu_3(a) = \nu_3(b) = 1$.

By (2.3.1), $s_3 = 3$. We show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/3$ of K is not a 3-integral element of K . Suppose on the contrary that $(x + y\theta + \theta^2)/3$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3}, \quad (2.3.2)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}, \quad (2.3.3)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \quad (2.3.4)$$

It follows from (2.3.4) that $x \equiv 0 \pmod{3}$. Then (2.3.3) implies that $y \equiv 0 \pmod{3}$. Then, from (2.3.4), we deduce $b^2 \equiv 0 \pmod{27}$, which is a contradiction. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 3$.

Case B3 : $1 = \nu_3(b) < \nu_3(a)$.

By (2.3.1), $s_3 = 5$. We show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/3$ of K is not a 3-integral element of K . Suppose that $(x + y\theta + \theta^2)/3$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3}, \quad (2.3.5)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}, \quad (2.3.6)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \quad (2.3.7)$$

It follows from (2.3.6) that $x \equiv 0 \pmod{3}$. Then (2.3.7) modulo 9 implies that $y \equiv 0 \pmod{3}$. Finally (2.3.7) gives $b^2 \equiv 0 \pmod{27}$, which is a contradiction. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 5$.

Case B4 : $\nu_3(a) = \nu_3(b) = 2$.

By (2.3.1), $s_3 = 6$. First we show that the element $(x + \theta)/3$ of K , where $x \in \mathbb{Z}$, is not a 3-integral element of K .

Suppose $(x + \theta)/3$ is a 3-integral element of K then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{3}, \quad (2.3.8)$$

$$3x^2 - a \equiv 0 \pmod{3^2}, \quad (2.3.9)$$

$$x^3 - ax - b \equiv 0 \pmod{3^3}. \quad (2.3.10)$$

It follows from (2.3.9) that $x \equiv 0 \pmod{3}$. Then (2.3.10) implies that $b \equiv 0 \pmod{27}$, which is a contradiction.

Secondly, by Theorem 2.1.1, $\theta^2/3$ is a 3-integral element of K if and only if

$$2a \equiv 0 \pmod{3}, \quad a^2 \equiv 0 \pmod{3^2}, \quad b^2 \equiv 0 \pmod{3^3},$$

which is clearly satisfied.

Thirdly, we show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/3^2$ of K is not a 3-integral element of K . Suppose $(x + y\theta + \theta^2)/3^2$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3^2}, \quad (2.3.11)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}, \quad (2.3.12)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \quad (2.3.13)$$

It follows from (2.3.11) that $x \equiv 0 \pmod{3}$. Then, (2.3.12) implies that $y \equiv 0 \pmod{3}$. Next, it follows from (2.3.13) modulo 3^4 that $x \equiv 0 \pmod{9}$. Then (2.3.13) modulo 3^5 gives $b^2 \equiv 0 \pmod{3^5}$, which is a contradiction. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/3\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 6 - 2 = 4$.

Case B5 : $2 = \nu_3(b) < \nu_3(a)$.

By (2.3.1), $s_3 = 7$. First we show that for every integer x , the element $(x + \theta)/3$ of K is not a 3-integral element of K . Suppose $(x + \theta)/3$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{3}, \quad (2.3.14)$$

$$3x^2 - a \equiv 0 \pmod{3^2}, \quad (2.3.15)$$

$$x^3 - ax - b \equiv 0 \pmod{3^3}. \quad (2.3.16)$$

It follows from (2.3.15) that $x \equiv 0 \pmod{3}$. Then (2.3.16) implies that $b \equiv 0 \pmod{3^3}$, which is a contradiction.

Secondly, by Theorem 2.1.1, $\theta^2/3$ is a 3-integral element of K if and only if

$$2a \equiv 0 \pmod{3}, \quad a^2 \equiv 0 \pmod{3^2}, \quad b^2 \equiv 0 \pmod{3^3},$$

which is clearly the case.

Thirdly we show that for every pair of integers x, y the element $(x + y\theta + \theta^2)/3^2$ of K is not a 3-integral element of K . Suppose that $(x + y\theta + \theta^2)/3^2$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3^2}, \quad (2.3.17)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}, \quad (2.3.18)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \quad (2.3.19)$$

It follows from (2.3.17) that $x \equiv 0 \pmod{3}$. Then, from (2.3.19) modulo 3^3 , we see that $y \equiv 0 \pmod{3}$. Next from (2.3.18) we deduce that $x \equiv 0 \pmod{9}$. Finally, from (2.3.19), we obtain $b^2 \equiv 0 \pmod{3^6}$, which is a contradiction. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/3\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 7 - 2 = 5$.

Case B6 : $1 = \nu_3(a) < \nu_3(b)$.

By (2.3.1), $s_3 = 3$. By Theorem 2.1.1, $\theta^2/3$ is a 3-integral element of K if and only if

$$2a \equiv 0 \pmod{3}, \quad a^2 \equiv 0 \pmod{3^2}, \quad b^2 \equiv 0 \pmod{3^3},$$

which is clearly true. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/3\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 3 - 2 = 1$.

Case B7 : $\nu_3(a) \geq 1, \nu_3(b) = 0, a \not\equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{9}$.

Here

$$\frac{\Delta}{3^3} = \frac{4a^3 - 27b^2}{3^3} = 4(a/3)^3 - b^2 \equiv (a/3) - 1 \not\equiv 0 \pmod{3},$$

so $s_3 = 3$. By Theorem 2.1.1, $(1 - b\theta + \theta^2)/3$ is a 3-integral element of K if and only if

$$3 + 2a \equiv 0 \pmod{3}, \quad (2.3.20)$$

$$3 + 4a - ab^2 + a^2 - 3b^2 \equiv 0 \pmod{3^2}, \quad (2.3.21)$$

$$1 + 2a - ab^2 - 3b^2 + a^2 + b^4 + b^2 - ab^2 \equiv 0 \pmod{3^3}. \quad (2.3.22)$$

The congruence (2.3.20) holds as $a \equiv 0 \pmod{3}$. Congruence (2.3.21) holds as

$$3 + 4a - ab^2 + a^2 - 3b^2 \equiv 3 + 4a - a + 0 - 3 \equiv 3a \equiv 0 \pmod{3^2},$$

which clearly holds. Thus, by Theorem 2.1.3, $\{1, \theta, (1 - b\theta + \theta^2)/3\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 3 - 2 = 1$.

Case B8 : $\nu_3(a) \geq 1, \nu_3(b) = 0, a \not\equiv 3 \pmod{9}, b^2 \not\equiv a + 1 \pmod{9}$.

By (2.3.1), we have

$$\begin{aligned} \Delta &= 4a^3 - 27b^2 \\ &= 4a^3 - 27(b^2 - (a + 1) + (a + 1)) \\ &= (4a^3 - 27(a + 1)) - 3^3(b^2 - (a + 1)). \end{aligned}$$

It is easy to see that

$$\nu_3(4a^3 - 27(a + 1)) = 3 \text{ and } \nu_3(3^3(b^2 - (a + 1))) = 4.$$

Hence $s_3 = \nu_3(\Delta) = 3$.

Now we show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/3$ of K is not a 3-integral element of K . Suppose $(x + y\theta + \theta^2)/3$ is a 3-integral element of K .

By Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3}, \quad (2.3.23)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}, \quad (2.3.24)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \quad (2.3.25)$$

As $a \equiv 0 \pmod{3}$ and $a \not\equiv 3 \pmod{9}$ we must have $a \equiv 0 \pmod{9}$ or $a \equiv 6 \pmod{9}$.

Assume first that $a \equiv 0 \pmod{9}$. Then it follows from (2.3.24) that

$$x^2 + by \equiv 0 \pmod{3}.$$

Hence we have the following possibilities:

$$x \equiv y \equiv 0 \pmod{3},$$

$$x \equiv y \equiv 1 \pmod{3}, \quad b \equiv 2 \pmod{3},$$

$$x \equiv 1 \pmod{3}, \quad y \equiv 2 \pmod{3}, \quad b \equiv 1 \pmod{3},$$

$$x \equiv 2 \pmod{3}, \quad y \equiv 1 \pmod{3}, \quad b \equiv 2 \pmod{3},$$

$$x \equiv y \equiv 2 \pmod{3}, \quad b \equiv 1 \pmod{3}.$$

If $x \equiv y \equiv 0 \pmod{3}$ then (2.3.25) gives $b^2 \equiv 0 \pmod{3^3}$, which is a contradiction.

If $x \equiv y \equiv 1 \pmod{3}$, $b \equiv 2 \pmod{3}$ then (2.3.25) gives after a short calculation $b \equiv -1 \pmod{9}$, so that $b^2 \equiv 1 \pmod{9}$, contradicting $b^2 \not\equiv a + 1 \pmod{9}$.

If $x \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{3}$, $b \equiv 1 \pmod{3}$ then (2.3.25) gives after a short calculation $b \equiv 1 \pmod{9}$, so that $b^2 \equiv 1 \pmod{9}$, contradicting $b^2 \not\equiv a + 1 \pmod{9}$.

If $x \equiv 2 \pmod{3}$, $y \equiv 1 \pmod{3}$, $b \equiv 2 \pmod{3}$ then (2.3.25) taken modulo 9 gives the contradiction $4 \equiv 0 \pmod{9}$.

If $x \equiv y \equiv 2 \pmod{3}$, $b \equiv 1 \pmod{3}$ then (2.3.25) taken modulo 9 gives the contradiction $4 \equiv 0 \pmod{9}$.

Now assume that $a \equiv 6 \pmod{9}$. It follows from (2.3.24) that

$$x(x + 2) + y(y + b) \equiv 0 \pmod{3}.$$

Hence we have the following possibilities:

$$\begin{aligned} x &\equiv y \equiv 0 \pmod{3}, \\ x &\equiv 0 \pmod{3}, y \equiv -b \pmod{3}, \\ x &\equiv 1 \pmod{3}, y \equiv 0 \pmod{3}, \\ x &\equiv 1 \pmod{3}, y \equiv -b \pmod{3}. \end{aligned}$$

If $x \equiv y \equiv 0 \pmod{3}$ then (2.3.25) taken modulo 3 gives $b^2 \equiv 0 \pmod{3}$ contradicting $b \not\equiv 0 \pmod{3}$.

If $x \equiv 0 \pmod{3}, y \equiv -b \pmod{3}$ then (2.3.25) taken modulo 3 gives $b^4 + b^2 \equiv 0 \pmod{3}$, that is $b^2 \equiv 2 \pmod{3}$, a contradiction.

If $x \equiv 1 \pmod{3}, y \equiv 0 \pmod{3}$ then (2.3.25) taken modulo 3 gives $b^2 \equiv 2 \pmod{3}$, a contradiction.

If $x \equiv 1 \pmod{3}, y \equiv -b \pmod{3}$ then (2.3.25) gives after a short calculation $b^4 + 4b^2 + 4 \equiv 0 \pmod{27}$, that is $b^2 \equiv 7 \pmod{9}$, contradicting $b^2 \not\equiv a + 1 \pmod{9}$.

Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 3$.

Case B9 : $a \equiv 3 \pmod{9}, \nu_3(b) = 0, b^2 \equiv 4 \pmod{9}, b^2 \not\equiv a + 1 \pmod{27}$.

By (2.3.1), we have

$$\begin{aligned} \Delta &= 4a^3 - 27b^2 \\ &= 4a^3 - 27(b^2 - (a + 1) + (a + 1)) \\ &= (4a^3 - 27(a + 1)) - 3^3(b^2 - (a + 1)). \end{aligned}$$

It is easy to see that

$$\nu_3(4a^3 - 27(a + 1)) \geq 6 \text{ and } \nu_3(3^3(b^2 - (a + 1))) = 5.$$

Hence $s_3 = \nu_3(\Delta) = 5$.

First we show that for every rational integer x the element $(x + \theta)/3$ of K is not a 3-integral element of K . Suppose $(x + \theta)/3$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{3}, \tag{2.3.30}$$

$$3x^2 - a \equiv 0 \pmod{3^2}, \quad (2.3.31)$$

$$x^3 - ax - b \equiv 0 \pmod{3^3}. \quad (2.3.32)$$

From (2.3.31) we see that $3x^2 \equiv 3 \pmod{9}$ so $x^2 \equiv 1 \pmod{3}$ that is $x \equiv \pm 1 \pmod{3}$. Then it follows from (2.3.32) that $b \equiv \pm(1 - a) \pmod{27}$. Thus $b^2 \equiv (1 - a)^2 \equiv 1 - 2a + a^2 \equiv 10 - 2a \equiv a + 1 \pmod{27}$, contradicting $b^2 \not\equiv a + 1 \pmod{27}$. Next, by Theorem 2.1.1, $(1 - b\theta + \theta^2)/3$ is a 3-integral element of K if and only if

$$3 + 2a \equiv 0 \pmod{3}, \quad (2.3.33)$$

$$3 + 4a - ab^2 + a^2 - 3b^2 \equiv 0 \pmod{3^2}, \quad (2.3.34)$$

$$1 + 2a - ab^2 - 3b^2 + a^2 + b^4 + b^2 - ab^2 \equiv 0 \pmod{3^3}. \quad (2.3.35)$$

Congruence (2.3.33) holds as $a \equiv 0 \pmod{3}$. Congruence (2.3.34) follows as $a \equiv 0 \pmod{3}$ and $b^2 \equiv 1 \pmod{3}$. Congruence (2.3.35) can be expressed as $(b^2 - (a + 1))^2 \equiv 0 \pmod{3^3}$, which holds as $b^2 - (a + 1) \equiv b^2 - 4 \equiv 0 \pmod{3^2}$.

Now we show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/3^2$ of K is not a 3-integral element of K . Suppose $(x + y\theta + \theta^2)/3^2$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3^2}, \quad (2.3.36)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^4}, \quad (2.3.37)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^6}. \quad (2.3.38)$$

Congruence (2.3.36) gives $x \equiv 1 \pmod{3}$. As $3x \equiv 3x^2 \equiv 3 \pmod{9}$ and $a \equiv 3 \pmod{9}$, (2.3.37) taken modulo 9, gives $y \equiv -b \pmod{3}$. Hence we have the following three possibilities:

- 1) $a \equiv 3 \pmod{27}$, $x \equiv 1 \pmod{3}$, $y \equiv -b \pmod{3}$,
- 2) $a \equiv 12 \pmod{27}$, $x \equiv 1 \pmod{3}$, $y \equiv -b \pmod{3}$,
- 3) $a \equiv 21 \pmod{27}$, $x \equiv 1 \pmod{3}$, $y \equiv -b \pmod{3}$,

1) $a \equiv 3 \pmod{27}$, $x \equiv 1 \pmod{3}$, $y \equiv -b \pmod{3}$.

Set $a = 27A + 3$, $x = 3X + 1$, $y = 3Y - b$.

Then (2.3.37) gives

$$9X^2 - 9Y^2 + 18X + 9bY + 2(4 - b^2) \equiv 0 \pmod{27}.$$

As $b^2 \equiv 4 \pmod{9}$ and $b^2 \not\equiv 4 \pmod{27}$ the above congruence implies

$$9X^2 - 9Y^2 + 18X + 9bY \not\equiv 0 \pmod{27}.$$

Hence

$$X^2 - Y^2 + 2X + bY \not\equiv 0 \pmod{3},$$

that is

$$X(X + 2) + Y(-Y + b) \not\equiv 0 \pmod{3}.$$

Then we have the following four cases:

$$X \equiv 0 \pmod{3} , Y \equiv -b \pmod{3},$$

$$X \equiv 1 \pmod{3} , Y \equiv -b \pmod{3},$$

$$X \equiv 2 \pmod{3} , Y \equiv 0 \pmod{3},$$

$$X \equiv 2 \pmod{3} , Y \equiv b \pmod{3},$$

We do the first case, the other cases can be treated similarly.

Set $x = 9X + 1$, $y = 9Y - 4b$, $a = 27A + 3$. Then (2.3.38) gives $32b^4 + 5b^2 + 8 \equiv (\text{mod } 3^4)$, which is a contradiction.

2) $a \equiv 12 \pmod{27}$, $x \equiv 1 \pmod{3}$, $y \equiv -b \pmod{3}$.

Set $a = 27A + 12$, $x = 3X + 1$, $y = 3Y - b$.

Then (2.3.37) gives

$$9X^2 - 36Y^2 - 5b^2 + 11 \equiv 0 \pmod{27}.$$

As $b^2 \equiv 4 \pmod{9}$ and $b^2 \not\equiv a+1 \pmod{27}$ the above congruence implies $X^2 - Y^2 \not\equiv 0 \pmod{3}$. Then we have the following four cases:

$$X \equiv 1 \pmod{3}, Y \equiv 0 \pmod{3},$$

$$X \equiv 2 \pmod{3}, Y \equiv 0 \pmod{3},$$

$$X \equiv 0 \pmod{3}, Y \equiv b \pmod{3},$$

$$X \equiv 0 \pmod{3}, Y \equiv -b \pmod{3}.$$

We just treat the third case, the other cases can be done similarly.

Set $x = 9X + 1$, $y = 9Y + 2b$, $a = 27A + 12$. Then (2.3.37) gives $b^2 \equiv 2 \pmod{9}$ which is a contradiction.

$$3) a \equiv -6 \pmod{27}, x \equiv 1 \pmod{3}, y \equiv -b \pmod{3}.$$

Set $a = 27A - 6$, $x = 3X + 1$, $y = 3Y - b$.

Then (2.3.37) gives

$$9X(X - 2) + 9Y(2Y - b) + b^2 + 5 \equiv 0 \pmod{27}.$$

As $b^2 \equiv 4 \pmod{9}$ and $b^2 \not\equiv 4 \pmod{27}$ the above congruence implies

$$X(X - 2) + Y(2Y - b) \not\equiv 0 \pmod{3}.$$

Hence we have the following four cases:

$$X \equiv 0 \pmod{3}, Y \equiv b \pmod{3},$$

$$X \equiv 1 \pmod{3}, Y \equiv 0 \pmod{3},$$

$$X \equiv 1 \pmod{3}, Y \equiv -b \pmod{3},$$

$$X \equiv 2 \pmod{3}, Y \equiv b \pmod{3}.$$

We do the first case, the other cases can be treated similarly.

Set $x = 9X + 1$, $y = 9Y + 2b$, $a = 27A - 6$. Then (2.3.38) gives $b^2 \equiv 2 \pmod{3}$, a contradiction.

Thus, by Theorem 2.1.3,

$$\{1, \theta, \frac{1 - b\theta + \theta^2}{3}\}$$

is a 3-integral basis of K and $\nu_3(d(K)) = 3$.

Case B10 : $a \equiv 3 \pmod{9}$, $b^2 \not\equiv 4 \pmod{9}$, $\nu_3(b) = 0$.

By (2.3.1), we have

$$\begin{aligned} \Delta &= 4a^3 - 27b^2 \\ &= 4a^3 - 27(b^2 - (a+1) + (a+1)) \\ &= (4a^3 - 27(a+1)) - 3^3(b^2 - (a+1)). \end{aligned}$$

It is easy to see that

$$\nu_3(4a^3 - 27(a+1)) \geq 6 \text{ and } \nu_3(3^3(b^2 - (a+1))) = 4.$$

Hence $s_3 = \nu_3(\Delta) = 4$.

Now we show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/3$ of K is not a 3-integral element of K . Suppose $(x + y\theta + \theta^2)/3$ is a 3-integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{3}, \tag{2.3.45}$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{3^2}, \tag{2.3.46}$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{3^3}. \tag{2.3.47}$$

It follows from (2.3.46) that

$$x(x+1) - y(y-b) \equiv 0 \pmod{3}.$$

Hence we have the following possibilities:

$$\begin{aligned}x &\equiv y \equiv 0 \pmod{3}, \\x &\equiv 0 \pmod{3}, y \equiv b \pmod{3}, \\x &\equiv 1 \pmod{3}, y \equiv -b \pmod{3}, \\x &\equiv 2 \pmod{3}, y \equiv 0 \pmod{3}, \\x &\equiv 2 \pmod{3}, y \equiv b \pmod{3}.\end{aligned}$$

If $x \equiv y \equiv 0$ then it follows from (2.3.47) taken modulo 9 that $b^2 \equiv 0 \pmod{9}$, a contradiction.

If $x \equiv 0 \pmod{3}, y \equiv b \pmod{3}$ then it follows from (2.3.47) that $b^2 \equiv 4 \pmod{9}$, a contradiction.

If $x \equiv 2 \pmod{3}, y \equiv 0 \pmod{3}$ then it follows from (2.3.47) taken modulo 9 that $b^2 \equiv 4 \pmod{9}$, a contradiction.

If $x \equiv 2 \pmod{3}, y \equiv b \pmod{3}$ then (2.3.47) taken modulo 3 gives a contradiction.

If $x \equiv 1 \pmod{3}, y \equiv -b \pmod{3}$ then it follows from (2.3.47) taken modulo 9 that $(b^2 - 1)^2 + 6 \equiv 0 \pmod{9}$, which is a contradiction.

Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a 3-integral basis of K and $\nu_3(d(K)) = 4$.

Case B11 : $a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27}$.

By (2.3.1),

$$\Delta = 4a^3 - 27b^2 = (4a^3 - 3^3(a + 1)) - 3^3(b^2 - (a + 1)).$$

As $\nu_3(4a^3 - 3^3(a + 1)) \geq 6$ and $\nu_3(3^3(b^2 - (a + 1))) \geq 6$ we have $s_3 = \nu_3(\Delta) \geq 6$.

By Theorem 2.1.1, $(b + \theta)/3$ is a 3-integral element of K if and only if

$$3b \equiv 0 \pmod{3}, 3b^2 - a \equiv 0 \pmod{3^2}, b^3 - ab - b \equiv 0 \pmod{3^3},$$

which clearly holds.

Next we show that for every rational integer x the element $(x + \theta)/3^2$ of K is not a 3-integral element of K . Suppose $(x + \theta)/3^2$ is a 3-integral element of K . Then, by

Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{3^2}, \quad 3x^2 - a \equiv 0 \pmod{3^4}, \quad x^3 - ax - b \equiv 0 \pmod{3^6}.$$

The first two of these congruences give $x \equiv 0 \pmod{3}$, and $a \equiv 0 \pmod{3^3}$, which is a contradiction.

As $s_3 \geq 6$ we can define an integer $m \geq 2$ by

$$m = [s_2 - 2]/2. \quad (2.3.48)$$

Note that $3^{2m+2} | \Delta$. Define integers x, y, z by

$$x \equiv -2a/3 \pmod{3^m}, \quad 2ay \equiv 3b \pmod{3^{m+2}}, \quad z = 1. \quad (2.3.49)$$

Then, in the notation of Theorem 2.1.2, we have

$$X = 3x + 2az = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{3^{m+1}}. \quad (2.3.50)$$

Also

$$\begin{aligned} 3bU &= 3b(9by - 2a^2z) \\ &= 27b^2y - 6a^2b \\ &= (4a^3 - \Delta)y - 6a^2b \\ &\equiv 4a^3y - 6a^2b \pmod{3^{2m+2}} \\ &\equiv 4a^3y - 6a^2b \pmod{3^{m+4}} \\ &\equiv (2a^2)(3b) - 6a^2b \pmod{3^{m+4}} \\ &\equiv 0 \pmod{3^{m+4}}, \end{aligned}$$

so that

$$U \equiv 0 \pmod{3^{m+3}}.$$

Further

$$V = 2ay - 3bz = 2ay - 3b \equiv 0 \pmod{3^{m+2}}.$$

It follows from (2.1.13) and (2.1.14) that

$$Y \equiv 0 \pmod{3^{2m}} \text{ and } Z \equiv 0 \pmod{3^{3m}}. \quad (2.3.51)$$

Thus it follows from (2.3.50), (2.3.51) and Theorem 2.1.1 that $(x + y\theta + \theta^2)/3^m$ is a 3-integral element of K where x and y are given by (2.3.49) and m is given by (2.3.48).

Thus, by Theorem 2.1.3,

$$\left\{1, \frac{b + \theta}{3}, \frac{x + y\theta + \theta^2}{3^m}\right\}$$

is a 3-integral basis of K , and $\nu_3(d(K)) = s_3 - 2[s_3/2]$.

Hence all the cases are complete. ■

Corollary 2.3.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b; \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2).

Define integers R_3, S_3, T_3 , by

$$\begin{cases} R_3 \equiv -2a/3 \pmod{3^{[s_3/2]-1}} & , \text{ if } a \equiv 3 \pmod{9}, b^2 \equiv a+1 \pmod{27}, \\ R_3 = 1 & , \text{ if } \nu_3(a) \geq 1, a \not\equiv 3 \pmod{9}, b^2 \equiv a+1 \pmod{9} \text{ or} \\ & a \equiv 3 \pmod{9}, b^2 \equiv 4 \pmod{9}, b^2 \not\equiv a+1 \pmod{27} \\ R_3 = 0 & , \text{ otherwise ;} \end{cases}$$

$$\begin{cases} (2a/3)S_3 \equiv b \pmod{3^{[s_3/2]}} & , \text{ if } a \equiv 3 \pmod{9}, b^2 \equiv a+1 \pmod{27}, \\ S_3 = -b & , \text{ if } \nu_3(a) \geq 1, a \not\equiv 3 \pmod{9}, b^2 \equiv a+1 \pmod{9} \text{ or} \\ & a \equiv 3 \pmod{9}, b^2 \equiv 4 \pmod{9}, b^2 \not\equiv a+1 \pmod{27}, \\ S_3 = 0 & , \text{ otherwise ;} \end{cases}$$

$$T_3 = \begin{cases} [s_3/2] - 1 & , \text{ if } a \equiv 3 \pmod{9} , \nu_3(b) = 0 , b^2 \equiv a + 1 \pmod{27}, \\ 1 & , \text{ if } 2 = \nu_3(b) = \nu_3(a) \text{ or} \\ & 2 = \nu_3(b) < \nu_3(a) \text{ or} \\ & 1 = \nu_3(a) < \nu_3(b) \text{ or} \\ & \nu_3(b) = 0 , \nu_3(a) \geq 1 , a \not\equiv 3 \pmod{9} , b^2 \equiv a + 1 \pmod{9} \text{ or} \\ & \nu_3(b) = 0 , a \equiv 3 \pmod{9} , b^2 \equiv 4 \pmod{9} , b^2 \not\equiv a + 1 \pmod{27}, \\ 0 & , \text{ otherwise.} \end{cases}$$

Then, except in the case

$$a \equiv 3 \pmod{9} , b^2 \equiv a + 1 \pmod{27}$$

a 3-integral basis of K is

$$\left\{ 1, \theta, \frac{R_3 + S_3\theta + \theta^2}{3T_3} \right\}.$$

In the excluded case, $a \equiv 3 \pmod{9} , b^2 \equiv a + 1 \pmod{27}$, a 3-integral basis of K is

$$\left\{ 1, \frac{b + \theta}{3}, \frac{R_3 + S_3\theta + \theta^2}{3T_3} \right\}.$$

Proof: This corollary follows immediately from Table B of Theorem 2.3.1. ■

2.4 $p(> 3)$ -Integral Basis of a Cubic Field

In this section we determine a p -integral basis of a cubic field.

Theorem 2.4.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b , a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Let p be a prime with $p > 3$.

Then a p -integral basis of K is given in the following table.

Case	Condition	$p(> 3)$ -integral basis	s_p	$\nu_p(d(K))$
C1	$\nu_p(a) = 0, \nu_p(b) \geq 1$ or $\nu_p(a) \geq 1, \nu_p(b) = 0$	$\{1, \theta, \theta^2\}$	0	0
C2	$1 = \nu_p(b) \leq \nu_p(a)$	$\{1, \theta, \theta^2\}$	2	2
C3	$2 = \nu_p(b) \leq \nu_p(a)$	$\{1, \theta, \theta^2/p\}$	4	2
C4	$1 = \nu_p(a) < \nu_p(b)$	$\{1, \theta, \theta^2/p\}$	3	1
C5	$\nu_p(a) = \nu_p(b) = 0$	$\{1, \theta, (x + y\theta + \theta^2)/p^m\}$ $m = \lfloor s_p/2 \rfloor,$ $3x \equiv -2a \pmod{p^m},$ $2ay \equiv 3b \pmod{p^m}$	$s_p \geq 0$	$s_p - 2\lfloor s_p/2 \rfloor$

Table C

Proof: The following flowchart shows that C1-C5 comprise all cases.

Recall that

$$\Delta = 2^2 a^3 - 3^3 b^2 \quad , \quad s_p = \nu_p(\Delta) \quad , \quad \text{and} \quad \Delta_p = \Delta/p^{s_p}. \quad (2.4.1)$$

Case C1 : $\nu_p(a) = 0, \nu_p(b) \geq 1$ or $\nu_p(a) \geq 1, \nu_p(b) = 0$.

By (2.4.1), $s_p = 0$. Then, by Theorem 2.1.3, $\nu_p(d(K)) = 0$ and $\{1, \theta, \theta^2\}$ is a p -integral basis of K .

Case C2 : $1 = \nu_p(b) \leq \nu_p(a)$.

By (2.4.1), $s_p = 2$. Now we show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/p$ of K is not a p -integral element of K . Suppose $(x + y\theta + \theta^2)/p$ is a p -integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{p}, \quad (2.4.2)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{p^2}, \quad (2.4.3)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{p^3}. \quad (2.4.4)$$

It follows from (2.4.2) that $x \equiv 0 \pmod{p}$. Then it follows from (2.4.4) modulo p^2 that $y \equiv 0 \pmod{p}$. Finally from (2.4.4) we get $b^2 \equiv 0 \pmod{p^3}$, a contradiction.

Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2\}$ is a p -integral basis of K and $\nu_p(d(K)) = 2$.

Case C3 : $2 = \nu_p(b) \leq \nu_p(a)$.

By (2.4.1), $s_p = 4$. By Theorem 2.1.1, θ^2/p is a p -integral element of K if and only if

$$2a \equiv 0 \pmod{p}, \quad a^2 \equiv 0 \pmod{p^2}, \quad b^2 \equiv 0 \pmod{p^3},$$

which clearly holds.

Now we show that for every rational integer x , the element $(x + \theta)/p$ of K is not a p -integral element of K . Suppose $(x + \theta)/p$ is a p -integral element of K . Then, by Theorem 2.1.1, we have

$$3x \equiv 0 \pmod{p}, \quad (2.4.5)$$

$$3x^2 - a \equiv 0 \pmod{p^2}, \quad (2.4.6)$$

$$x^3 - ax - b \equiv 0 \pmod{p^3}. \quad (2.4.7)$$

It follows from (2.4.5) that $x \equiv 0 \pmod{p}$. Then (2.4.7) implies that $b \equiv 0 \pmod{p^3}$, which is a contradiction.

Next we show that for every pair of integers x, y , the element $(x + y\theta + \theta^2)/p^2$ of K is not a p -integral element of K . Suppose $(x + y\theta + \theta^2)/p^2$ is a p -integral element of K . Then, by Theorem 2.1.1, we have

$$3x + 2a \equiv 0 \pmod{p^2}, \quad (2.4.8)$$

$$3x^2 + 4ax - ay^2 + a^2 + 3by \equiv 0 \pmod{p^4}, \quad (2.4.9)$$

$$x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + b^2 + aby \equiv 0 \pmod{p^6}. \quad (2.4.10)$$

It follows from (2.4.8) that $x \equiv 0 \pmod{p^2}$. Then (2.4.9) becomes

$$-ay^2 + 3by \equiv 0 \pmod{p^4} \quad (2.4.11)$$

and (2.4.10) becomes

$$-axy^2 + 3bxy - by^3 + b^2 + aby \equiv 0 \pmod{p^6}. \quad (2.4.12)$$

If $y \equiv 0 \pmod{p}$ (2.4.12) gives $b^2 \equiv 0 \pmod{p^5}$, which is impossible. Hence $y \not\equiv 0 \pmod{p}$ and (2.4.11) gives $ay \equiv 3b \pmod{p^4}$. Then (2.4.10) becomes $-by^3 + b^2 + aby \equiv 0 \pmod{p^6}$. As $p^2 \nmid b$ this is just $b + ay - y^3 \equiv 0 \pmod{p^4}$, which implies $y \equiv 0 \pmod{p}$, a contradiction.

Hence, by Theorem 2.1.3, $\{1, \theta, \theta^2/p\}$ is a p -integral basis for K , and $\nu_p(d(K)) = 4 - 2 = 2$.

Case C4 : $1 = \nu_p(a) < \nu_p(b)$.

By (2.4.1), $s_p = 3$. By Theorem 2.1.1, θ^2/p is a p -integral element of K if and only if

$$2a \equiv 0 \pmod{p}, \quad a^2 \equiv 0 \pmod{p^2}, \quad b^2 \equiv 0 \pmod{p^3},$$

which clearly holds. Thus, by Theorem 2.1.3, $\{1, \theta, \theta^2/p\}$ is a p -integral basis for K , and $\nu_p(d(K)) = 3 - 2 = 1$.

Case C5 : $\nu_p(a) = \nu_p(b) = 0$.

We define a nonnegative integer m by

$$m = [s_p/2]. \quad (2.4.13)$$

Note that $p^{2m} | \Delta$. Define integers x, y, z by

$$3x \equiv -2a \pmod{p^m}, \quad 2ay \equiv 3b \pmod{p^m}, \quad z = 1. \quad (2.4.14)$$

Then, in the notation of Theorem 2.1.2, we have

$$X = 3x + 2az = 3x + 2a \equiv -2a + 2a \equiv 0 \pmod{p^m}. \quad (2.4.15)$$

Also

$$\begin{aligned} 3bU &= 3b(9by - 2a^2z) \\ &= 27b^2y - 6a^2b \\ &= (4a^3 - \Delta)y - 6a^2b \\ &\equiv (2a^2)(3b) - 6a^2b \pmod{p^m} \\ &\equiv 0 \pmod{p^m}. \end{aligned}$$

As $p \nmid 3b$, we deduce $U \equiv 0 \pmod{p^m}$. Thus, by Theorem 2.1.3, $\{1, \theta, (x + y\theta + \theta^2)/p^m\}$ is a p -integral basis of K , and $\nu_p(d(K)) = s_p - 2[s_p/2]$.

Hence all the cases are treated. ■

Corollary 2.4.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Let p be a prime with $p > 3$.

Define integers R_p, S_p, T_p , by

$$\begin{cases} 3R_p \equiv -2a \pmod{p^{[s_p/2]}} & , \text{ if } \nu_p(a) = \nu_p(b) = 0, \\ R_p = 0 & , \text{ otherwise ;} \end{cases}$$

$$\begin{cases} 2aS_p \equiv 3b \pmod{p^{[s_p/2]}} & , \text{ if } \nu_p(a) = \nu_p(b) = 0, \\ S_p = 0 & , \text{ otherwise ;} \end{cases}$$

$$T_p = \begin{cases} [s_p/2] & , \text{ if } \nu_p(a) = \nu_p(b) = 0, \\ 1 & , \text{ if } \nu_p(a) \geq 1, \nu_p(b) \geq 2, \\ 0 & , \text{ otherwise.} \end{cases}$$

Then

$$\left\{ 1, \theta, \frac{R_p + S_p\theta + \theta^2}{p^{T_p}} \right\}$$

is a p -integral basis of K .

Proof: This corollary follows immediately from Table C of Theorem 2.4.1. ■

2.5 Evaluation of the Discriminant $d(K)$ of a Cubic Field K

In this section we use the results of Theorems 2.2.1, 2.3.1 and 2.4.1 to determine an explicit formula for the discriminant of the cubic field K . As a consequence of this formula, we obtain an explicit formula for the index of θ in terms of a and b .

Theorem 2.5.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Then the discriminant $d(K)$ of K is

$$d(K) = \text{sgn}(4a^3 - 27b^2) 2^{\alpha} 3^{\beta} \prod_{\substack{p > 3 \\ s_p \text{ odd}}} p \prod_{\substack{p > 3 \\ 1 \leq \nu_p(b) \leq \nu_p(a)}} p^2, \quad (2.5.1)$$

where

$$\alpha = \begin{cases} 0, & \text{if } b \equiv 1 \pmod{2} \\ & \text{or } a \equiv 1 \pmod{4}, b \equiv 0 \pmod{4} \\ & \text{or } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}, \Delta_2 \equiv 1 \pmod{4}, \\ 2, & \text{if } a \equiv 0 \pmod{2}, b \equiv 2 \pmod{4} \\ & \text{or } a \equiv 0 \pmod{2}, b \equiv 4 \pmod{8} \\ & \text{or } a \equiv 3 \pmod{4}, b \equiv 0 \pmod{4} \\ & \text{or } a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}, s_2 \equiv 0 \pmod{2}, \Delta_2 \equiv 3 \pmod{4}, \\ 3, & \text{if } s_2 \equiv 1 \pmod{2}, \end{cases} \quad (2.5.2)$$

and

$$\beta = \begin{cases} 0, & \text{if } \nu_3(a) = 0 \\ & \text{or } \nu_3(b) = 0, a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27}, s_3 \equiv 0 \pmod{2}, \\ 1, & \text{if } 1 = \nu_3(a) < \nu_3(b) \\ & \text{or } \nu_3(b) = 0, \nu_3(a) \geq 1, a \not\equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{9} \\ & \text{or } \nu_3(b) = 0, a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27}, s_3 \equiv 1 \pmod{2}, \\ 3, & \text{if } 1 = \nu_3(a) = \nu_3(b) \\ & \text{or } \nu_3(b) = 0, \nu_3(a) \geq 1, a \not\equiv 3 \pmod{9}, b^2 \not\equiv a + 1 \pmod{9} \\ & \text{or } \nu_3(b) = 0, a \equiv 3 \pmod{9}, b^2 \equiv 4 \pmod{9}, b^2 \not\equiv a + 1 \pmod{27}, \\ 4, & \text{if } 2 = \nu_3(b) = \nu_3(a) \\ & \text{or } \nu_3(b) = 0, a \equiv 3 \pmod{9}, b^2 \not\equiv 4 \pmod{9}, \\ 5, & \text{if } 1 \leq \nu_3(b) < \nu_3(a). \end{cases} \quad (2.5.3)$$

Proof: Recall from (2.1.3) and (2.1.4) that

$$4a^3 - 27b^2 = \{i(\theta)\}^2 d(K). \quad (2.5.4)$$

Hence $\text{sgn}(d(K)) = \text{sgn}(4a^3 - 27b^2)$.

The exponents of the prime powers in $d(K)$ follow from Tables A, B, C. ■

Theorem 2.5.2 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Then the index of θ is given by

$$i(\theta) = 2^r 3^s \prod_{\substack{2=\nu_p(b) \leq \nu_p(a) \text{ OR} \\ 1=\nu_p(a) < \nu_p(b)}} p, \quad (2.5.5)$$

where $r = (s_2 - \alpha)/2$, $s = (s_3 - \beta)/2$.

Proof: This follows from Tables A, B, C and Theorem 2.5.1. ■

Theorem 2.5.3 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Then $\{1, \theta, \theta^2\}$ is an integral basis of K if and only if $s_2 = \alpha$, $s_3 = \beta$ and the following two inequalities are not satisfied for any rational prime $p(> 3)$,

$$2 = \nu_p(b) \leq \nu_p(a) \text{ and } 1 = \nu_p(a) < \nu_p(b).$$

Proof: It is clear that $\{1, \theta, \theta^2\}$ is an integral basis of K if and only if $i(\theta) = 1$. The rest follows from Tables A, B, C and Theorem 2.5.2. ■

2.6 Integral Basis of a Cubic Field

In this section we construct an integral basis for K by using the p -integral basis for K constructed in Theorems 2.2.1, 2.3.1 and 2.4.1.

Theorem 2.6.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2).

Define the integers

R_2, S_2, T_2 as in Corollary 2.2.1 ,

R_3, S_3, T_3 as in Corollary 2.3.1 ,

and for a prime $p > 3$

R_p, S_p, T_p as in Corollary 2.4.1.

Let R and S be integers such that for all primes p

$$R \equiv R_p \pmod{p^{T_p}},$$

$$S \equiv S_p \pmod{p^{T_p}}.$$

Let T be the positive integer $T = \prod_p p^{T_p}$. Then

$$\left\{ 1, \theta, \frac{R + S\theta + \theta^2}{T} \right\}$$

is an integral basis of K except in the case

$$\nu_3(b) = 0, \quad a \equiv 3 \pmod{9}, \quad b^2 \equiv a + 1 \pmod{27}$$

when an integral basis is

$$\left\{ 1, \frac{b + \theta}{3}, \frac{R + S\theta + \theta^2}{T} \right\}.$$

Proof: This theorem follows from Theorem 1.3.5, Corollary 2.2.1, Corollary 2.3.1 and Corollary 2.4.1. ■

2.7 Numerical Examples

In this section we give some numerical examples illustrating Theorem 2.6.1.

$$K = Q(\theta), \theta^3 - a\theta + b = 0$$

a	b	nonzero values of s_p	nonzero values of R_p, S_p, T_p	R	S	T	integral basis	$d(K)$
6	36	$s_2 = 4, s_3 = 3,$ $s_{79} = 1$	$T_2 = T_3 = 1$	0	0	6	$1, \theta, \theta^2/6$	$-2^2 \cdot 3 \cdot 79$
6	32	$s_2 = 5, s_3 = 3,$ $s_{31} = 1$	$T_2 = T_3 = R_3 = 1$ $S_3 = -32$	4	4	6	$1, \theta,$ $(4 + 4\theta + \theta^2)/6$	$-2^3 \cdot 3 \cdot 31$
30	52	$s_2 = 4, s_3 = 7$	$T_2 = 1, T_3 = 2$ $R_3 = -20,$ $S_3 = 8.$	-2	8	18	$1, (1 + \theta)/3,$ $(-2 + 8\theta + \theta^2)/18$	$2^2 \cdot 3$
2	8	$s_2 = 5, s_{53} = 1$	$T_2 = 1$	0	0	2	$1, \theta, \theta^2/2$	$-2^3 \cdot 53$
21	72	$s_2 = 2, s_3 = 3,$ $s_{953} = 1$	$S_2 = T_2 = T_3 = 1$	0	3	2	$1, \theta$ $(3\theta + \theta^2)/6$	$-3 \cdot 953$
57	16	$s_2 = 2, s_3 = 5,$ $s_5 = s_{151} = 1$	$S_2 = T_2 = 1,$ $R_3 = T_3 = 1$ $S_3 = -16$	4	-1	6	$1, \theta,$ $(4 - \theta + \theta^2)/6$	$3^3 \cdot 5 \cdot 151$
57	272	$s_2 = 2, s_3 = 6,$ $s_{43} = 1$	$S_2 = T_2 = 1$ $R_3 = -38$ $S_3 = 10, T_3 = 2$	-2	1	18	$1, (272 + \theta)/3,$ $(-2 + \theta + \theta^2)/18$	-43
1	4	$s_2 = 2, s_{107} = 1$	$S_2 = T_2 = 1$	0	1	2	$1, \theta,$ $(\theta + \theta^2)/2$	-107
3	54	$s_2 = 5, s_3 = 3,$ $s_7 = s_{13} = 1$	$R_2 = 2, S_2 = 1,$ $T_2 = T_3 = 1$	0	3	6	$1, \theta,$ $(3\theta + \theta^2)/6$	$-2^3 \cdot 3 \cdot 7 \cdot 13$
39	34	$s_2 = 4, s_3 = 5,$ $s_{53} = 1$	$R_2 = 2, S_2 = -1,$ $T_2 = R_3 = T_3 = 1$ $S_3 = -34$	4	-1	6	$1, \theta,$ $(4 - \theta + \theta^2)/6$	$2^2 \cdot 3^3 \cdot 53$

TABLE D

a	b	nonzero values of s_p	nonzero values of R_p, S_p, T_p	R	S	T	integral basis	$d(K)$
255	3850	$s_2 = 4,$ $s_3 = 6$ $s_5 = 3$ $s_{229} = 1$	$R_2 = 2,$ $S_2 = -1,$ $T_2 = R_3 = 1$ $S_3 = 2, T_3 = 2$ $T_5 = 1$	10	-25	90	$1, (3850 + \theta)/3,$ $(10 - 25\theta + \theta^2)/90$	$-2^2 \cdot 5 \cdot 229$
7	2	$s_2 = 4$ $s_{79} = 1$	$R_2 = 2, S_2 = 3,$ $T_2 = 1$	0	1	2	$1, \theta,$ $(\theta + \theta^2)/2$	$2^2 \cdot 79$
3	9	$s_3 = 3,$ $s_7 = s_{11} = 1$	$T_3 = 1$	0	0	3	$1, \theta, \theta^2/3$	$-3 \cdot 7 \cdot 11$
3	7	$s_3 = 5$ $s_5 = 1$	$R_3 = T_3 = 1$ $S_3 = -7$	1	-1	3	$1, \theta,$ $(1 - \theta + \theta^2)/3$	$-3^3 \cdot 5$
3	56	$s_2 = 2,$ $s_3 = 6$ $s_{29} = 1$	$R_3 = -2$ $S_3 = 1, T_3 = 2$	-2	1	9	$1, (56 + \theta)/3,$ $(-2 + \theta + \theta^2)/9$	$-2^2 \cdot 29$
1	1	$s_{23} = 1$		0	0	1	$1, \theta, \theta^2$	-23
21	-236	$s_2 = 2,$ $s_3 = 6$ $s_{503} = 1$	$S_2 = T_2 = 1,$ $R_3 = 4,$ $T_3 = 2$ $S_3 = 14$	4	5	18	$1, (-236 + \theta)/3,$ $(4 + 5\theta + \theta^2)/18$	-503
-11	4	$s_2 = 2,$ $s_{1439} = 1$	$S_2 = T_2 = 1$	0	1	2	$1, \theta,$ $(\theta + \theta^2)/2$	-1439
27	9	$s_3 = 7,$ $s_5 = s_7 = 1$	$T_3 = 1$	0	0	3	$1, \theta, \theta^2/3$	$3^5 \cdot 5 \cdot 7$
9	-6	$s_2 = 3,$ $s_3 = 5$		0	0	1	$1, \theta, \theta^2$	$2^3 \cdot 3^5$

TABLE D continued

2.8 Integral Basis of a Pure Cubic Field

Let t be a cubefree integer. We express t in the form

$$t = hk^2, \quad (2.8.1)$$

where h is squarefree. Clearly k is squarefree and $GCD(h, k) = 1$. Let $\theta = t^{1/3}$ and let K be the pure cubic field $Q(\theta)$. We use Theorems 2.2.1, 2.3.1 and 2.4.1 to determine an integral basis of K . As $x^3 - t$ is the irreducible polynomial of θ , we have $a = 0$, $b = -t$, and

$$\Delta = 4a^3 - 27b^2 = -27(-t)^2 = -27t^2.$$

Since $a = 0$, only the cases A1-A3, B3, B5, B7, B8, C1-C3 can arise.

It follows from A1-A3 that a 2-integral basis of K is

$$\begin{cases} \{1, \theta, \theta^2\} & , \text{ if } t \not\equiv 0 \pmod{4} \Leftrightarrow 2 \nmid k, \\ \{1, \theta, \theta^2/2\} & , \text{ if } t \equiv 0 \pmod{4} \Leftrightarrow 2 \mid k. \end{cases}$$

Hence a 2-integral basis of K is

$$\{1, \theta, \theta^2/k\}.$$

It follows from B3, B5, B7 and B8 that a 3-integral basis of K is

$$\begin{cases} \{1, \theta, \theta^2/3\} & , \text{ if } t \equiv 0 \pmod{9} \Leftrightarrow 3 \mid k, \\ \{1, \theta, \theta^2\} & , \text{ if } t \not\equiv 0 \pmod{9} \text{ and } t^2 \not\equiv 1 \pmod{9}, \\ \{1, \theta, (1 + t\theta + \theta^2)/3\} & , \text{ if } t^2 \equiv 1 \pmod{9}. \end{cases} \quad (2.8.2)$$

It follows from C1-C3 that a $p(> 3)$ -integral basis of K is

$$\begin{cases} \{1, \theta, \theta^2\} & , \text{ if } t \not\equiv 0 \pmod{p^2} \Leftrightarrow p \nmid k, \\ \{1, \theta, \theta^2/p\} & , \text{ if } t \equiv 0 \pmod{p^2} \Leftrightarrow p \mid k. \end{cases}$$

Hence a $p(> 3)$ -integral basis of K is

$$\{1, \theta, \theta^2/p\}. \quad (2.8.3)$$

If $3|k$ then it follows from (2.8.2), (2.8.3), (2.8.4) that

$$\{1, \theta, \theta^2/k\} \quad (2.8.4)$$

is an integral basis of K .

Now assume $3 \nmid k$. If $t^2 \not\equiv 1 \pmod{9}$ then it follows from (2.8.2), (2.8.3), (2.8.4) that

$$\{1, \theta, \theta^2/k\} \quad (2.8.5)$$

is an integral basis of K .

If $t^2 \equiv 1 \pmod{9}$, equivalently $t \equiv \pm 1 \pmod{9}$, then it follows from (2.8.2), (2.8.3), (2.8.4) that

$$\left\{1, \theta, \frac{k^2 \pm k^2\theta + \theta^2}{3k}\right\} \quad (2.8.6)$$

is an integral basis of K . To justify (2.8.7), we must show that $k^2 \equiv 1 \pmod{3}$, and

$$t \equiv \pm k^2 \pmod{3} \text{ if } t \equiv \pm 1 \pmod{9}.$$

As $k \equiv 1, 2 \pmod{3}$ then $k^2 \equiv 1 \pmod{3}$, and so

$$t \equiv \pm k^2 \pmod{3} \text{ if } t \equiv \pm 1 \pmod{9}.$$

Thus from (2.8.5), (2.8.6), (2.8.7) we have the following result.

Theorem 2.8.1 *Let t be a cubefree integer. Set $t = hk^2$, where h is squarefree, $\theta = t^{1/3}$, $K = Q(\theta)$. Then an integral basis of K is*

$$\begin{cases} \{1, \theta, \theta^2/k\} & , \text{ if } t^2 \not\equiv 1 \pmod{9}, \\ \{1, \theta, (k^2 \pm k^2\theta + \theta^2)/3k\} & , \text{ if } t \equiv \pm 1 \pmod{9}. \end{cases} \quad (2.8.7)$$

The discriminant of K is

$$\Delta(K) = \begin{cases} -27h^2k^2 & , \text{ if } t^2 \not\equiv 1 \pmod{9}, \\ -3h^2k^2 & , \text{ if } t \equiv \pm 1 \pmod{9}. \end{cases} \quad (2.8.8)$$

2.9 Alternative Form of an Integral Basis of a Cubic Field

In this section we give a new compact form of an integral basis of K and illustrate it with some examples.

Theorem 2.9.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in \mathbb{Z},$$

where a and b satisfy the simplifying assumption (2.1.2). Let n^2 be the largest square dividing $4a^3 - 27b^2$ for which the pair of congruences

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{n^2}, \\ 3t^2 - a \equiv 0 \pmod{n}, \end{cases} \quad (2.9.1)$$

is simultaneously solvable for t . Then, except in the case

$$a \equiv 3 \pmod{9}, \quad b^2 \equiv a + 1 \pmod{27}, \quad (2.9.2)$$

an integral basis of K is

$$\left\{ 1, \theta, \frac{(-a + t^2) + t\theta + \theta^2}{n} \right\} \quad (2.9.3)$$

and

$$d(K) = \frac{4a^3 - 27b^2}{n^2}. \quad (2.9.4)$$

In the excluded case $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$, let n^2 be the largest square dividing $(4a^3 - 27b^2)/729$ for which the pair of congruences

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{27n^2}, \\ 3t^2 - a \equiv 0 \pmod{9n}, \end{cases} \quad (2.9.5)$$

is simultaneously solvable for t . Then an integral basis of K is

$$\left\{ 1, \frac{-t + \theta}{3}, \frac{(t^2 - a) + t\theta + \theta^2}{9n} \right\} \quad (2.9.6)$$

and

$$d(K) = \frac{4a^3 - 27b^2}{729n^2}. \quad (2.9.7)$$

Proof: Let the notation be as in Theorem 2.6.1. We break up the proof into three lemmas. First let us exclude the case $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$.

Lemma 2.9.1

$$T^2 | 4a^3 - 27b^2. \quad (2.9.8)$$

Proof : The proof follows from Theorem 2.6.1. ■

Lemma 2.9.2

$$S^3 - aS + b \equiv 0 \pmod{T^2}, \quad (2.9.9)$$

$$3S^2 - a \equiv 0 \pmod{T}, \quad (2.9.10)$$

$$R \equiv -a + S^2 \pmod{T}. \quad (2.9.11)$$

Proof : It is enough to show that for every prime p

$$S^3 - aS + b \equiv 0 \pmod{p^{2T_p}}, \quad (2.9.12)$$

$$3S^2 - a \equiv 0 \pmod{p^{T_p}}, \quad (2.9.13)$$

$$R \equiv -a + S^2 \pmod{p^{T_p}}. \quad (2.9.14)$$

(2.9.13) is equivalent to

$$9S^4 - 6aS^2 + a^2 \equiv 0 \pmod{p^{2T_p}}. \quad (2.9.15)$$

Recall that

$$R \equiv R_p \pmod{p^{T_p}}, \quad (2.9.16)$$

$$S \equiv S_p \pmod{p^{T_p}}. \quad (2.9.17)$$

Let $p = 2$. We need to treat the cases A1-A10 in Theorem 2.2.1. We do the case A9, the other cases can be done similarly.

Case A9 : $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ and $\Delta_2 \equiv 3 \pmod{4}$.

By Corollary 2.2.1,

$$3R_2 \equiv -2a \pmod{2^{T_2+1}}, \quad (2.9.18)$$

$$aS_2 \equiv 3(b/2) + 2^{T_2} \pmod{2^{T_2+1}}, \quad (2.9.19)$$

$$T_2 = (s_2 - 2)/2. \quad (2.9.20)$$

(2.9.13) is satisfied if and only if, by (2.9.17),

$$3S_2^2 - a \equiv 0 \pmod{2^{T_2}}$$

if and only if

$$3(2aS_2)^2 - 4a^3 \equiv 0 \pmod{2^{T_2+2}}$$

if and only if, by (2.9.19),

$$2^{T_2+2} | \Delta$$

which is satisfied.

(2.9.12) is satisfied if and only if

$$9S^4 - 9aS^2 + 9bS \equiv 0 \pmod{2^{2T_2}}$$

if and only if, by (2.9.15),

$$3aS^2 - 9bS + a^2 \equiv 0 \pmod{2^{2T_2}}$$

if and only if

$$aS \equiv 3(b/2) \pmod{2^{T_2}}$$

which is true by (2.9.19).

(2.9.14) is satisfied if and only if, by (2.9.16)–(2.9.17),

$$R_2 \equiv -a + S_2^2 \pmod{2^{T_2}}$$

if and only if

$$3a^2 R_2 \equiv -3a^3 + 3a^2 S_2^2 \pmod{2^{T_2}}$$

if and only if, by (2.9.18)–(2.9.19),

$$2^{T_2+2} | \Delta$$

which is satisfied.

Let $p = 3$. We need to treat the cases B1–B10 in Theorem 2.3.1. We just do the case B9, the other cases can be done similarly.

Case B9 : $\nu_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ and $b^2 \not\equiv a+1 \pmod{27}$.
By Corollary 2.3.1,

$$R_3 = 1, S_3 = -b \text{ and } T_3 = 1. \quad (2.9.21)$$

Then it is easy to see that (2.9.12)–(2.9.14) are satisfied.

Let $p(> 3)$ be a prime. We need to do the cases C1–C5 in Theorem 2.4.1. We do the case C5, the other cases can be done similarly.

Case C5 : $\nu_p(ab) = 0$. By Corollary 2.4.1, we have

$$3R_p \equiv -2a \pmod{p^{T_p}}, \quad (2.9.22)$$

$$2aS_p \equiv 3b \pmod{p^{T_p}}, \quad (2.9.23)$$

$$T_p = \lfloor s_p/2 \rfloor. \quad (2.9.24)$$

(2.9.13) is satisfied if and only if, by (2.9.17),

$$3S_p^2 - a \equiv 0 \pmod{p^{T_p}}$$

if and only if

$$3(2aS_p)^2 - 4a^3 \equiv 0 \pmod{p^{T_p}}$$

if and only if, by (2.9.23),

$$p^{T_p} | \Delta$$

which is true.

(2.9.12) is satisfied if and only if

$$9S^4 - 9aS^2 + 9bS \equiv 0 \pmod{p^{2T_p}}$$

if and only if, by (2.9.15)

$$3aS^2 - 9bS + a^2 \equiv 0 \pmod{p^{2T_p}}$$

if and only if

$$(6aS - 9b)^2 + 3\Delta \equiv 0 \pmod{p^{2T_p}}$$

if and only if

$$2aS \equiv 3b \pmod{p^{T_p}}$$

which is true by (2.9.23). Hence, the proof of Lemma 2.9.2 is complete. ■

Corollary 2.9.1 *The pair of congruences*

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{T^2}, \\ 3t^2 - a \equiv 0 \pmod{T}, \end{cases} \quad (2.9.25)$$

is simultaneously solvable with $t = S$.

Lemma 2.9.3 *If p is a prime such that*

$$(pT)^2 | 4a^3 - 27b^2 \quad (2.9.26)$$

then the pair of congruences

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{p^2T^2}, \\ 3t^2 - a \equiv 0 \pmod{pT}, \end{cases} \quad (2.9.27)$$

is not simultaneously solvable.

Proof : We state the Lemma in the following equivalent way:

If p is a prime such that

$$p^{2(T_p+1)} | 4a^3 - 27b^2 \quad (2.9.28)$$

then the pair of congruences

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{p^{2(T_p+1)}}, \\ 3t^2 - a \equiv 0 \pmod{p^{T_p+1}}, \end{cases} \quad (2.9.29)$$

is not simultaneously solvable. (2.9.29) is equivalent to the pair

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{p^{2(T_p+1)}}, \\ 9t^4 - 6at^2 + a^2 \equiv 0 \pmod{p^{2(T_p+1)}}. \end{cases} \quad (2.9.30)$$

Let $p = 2$. We need to treat the cases A1-A10 in Theorem 2.2.1. We do the case A9, the other cases can be done similarly.

Case A9 : $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{2}$ and $\Delta_2 \equiv 3 \pmod{4}$.

Note that (2.9.28) is satisfied. (2.9.30) is satisfied if and only if

$$\begin{cases} 9t^4 - 9at^2 + 9bt \equiv 0 \pmod{2^{2(T_2+1)}}, \\ 9t^4 - 6at^2 + a^2 \equiv 0 \pmod{2^{2(T_2+1)}}, \end{cases} \quad (2.9.31)$$

which implies

$$3at^2 - 9bt + a^2 \equiv 0 \pmod{2^{2(T_2+1)}}.$$

The above equation gives

$$(6at - 9b)^2 + 3\Delta \equiv 0 \pmod{2^{(s_2+2)}},$$

which is not satisfied as $\Delta_2 \equiv 3 \pmod{4}$.

Let $p = 3$. We need to treat the cases B1-B10 in Theorem 2.3.1. We do the case B9, the other cases can be done similarly.

Case B9 : $\nu_3(b) = 0$, $a \equiv 3 \pmod{9}$, $b^2 \equiv 4 \pmod{9}$ and $b^2 \not\equiv a+1 \pmod{27}$.
By Corollary 2.3.1, $T_3 = 1$. Note that (2.9.28) is satisfied. (2.9.29) is satisfied if and only if

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{3^4}, \\ 3t^2 - a \equiv 0 \pmod{3^2}. \end{cases}$$

The first equation taken modulo 3 gives $t \equiv -b \pmod{3}$. Substituting $t = -b+3X$ into the first equation taken modulo 27 gives $b^2 \equiv a+1 \pmod{27}$ which is a contradiction.

Let $p(> 3)$ be a prime. We need to treat the cases C1–C5 in Theorem 2.4.1. As in the previous Lemma we do the case C5. Since, by (2.9.24), $T_p = [s_p/2]$ then

$$(p^{T_p+1})^2 = p^{2T_p+2} = p^{2[s_p/2]+2} \not\equiv \Delta.$$

So (2.9.28) is not satisfied. Hence the proof of Lemma 2.9.3 is complete. ■

Corollary 2.9.2 *If n is the largest integer for which $n^2 | 4a^3 - 27b^2$ and the pair of congruences*

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{n^2}, \\ 3t^2 - a \equiv 0 \pmod{n}, \end{cases} \quad (2.9.32)$$

is simultaneously solvable for t then $n = T$.

To complete the proof of the first part of Theorem 2.9.1, we show that if t is a solution of the pair of the congruences (2.9.1), then $t \equiv S \pmod{T}$. It is enough to show that for every prime p , $t \equiv S \pmod{p^{T_p}}$.

Let $p = 2$. We do the case A9. If t is a solution of the pair of congruences (2.9.1), we see after a short calculation, that

$$2at \equiv 3b \pmod{2^{T_2+1}}. \quad (2.9.33)$$

It follows from (2.9.19) that

$$2aS_2 \equiv 3b \pmod{2^{T_2+1}}. \quad (2.9.34)$$

By (2.9.33)–(2.9.34),

$$2at \equiv 2aS_2 \pmod{2^{T_2+1}},$$

which gives $t \equiv S_2 \pmod{2^{T_2}}$.

Let $p = 3$. We do the case B9. Recall that

$$R_3 = 1, S_3 = -b \text{ and } T_3 = 1.$$

We know that

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{3^2}, \\ 3t^2 - a \equiv 0 \pmod{3}. \end{cases} \quad (2.9.35)$$

It follows from the first equation taken modulo 3 that $t \equiv -b \equiv S_3 \pmod{3}$.

Let $p(> 3)$ be a prime. We do the case C5. If t is a solution of the pair of congruences (2.9.1), we see, after a short calculation, that

$$2at \equiv 3b \pmod{p^{T_p}}. \quad (2.9.36)$$

It follows from (2.9.23) and (2.9.36) that

$$2at \equiv 2aS_p \pmod{p^{T_p}},$$

which gives $t \equiv S_p \pmod{p^{T_p}}$. Hence, $t \equiv S \pmod{T}$.

Thus, it follows from the above lemmas and corollaries that an integral basis of K is

$$\begin{aligned} \left\{ 1, \theta, \frac{K + S\theta + \theta^2}{T} \right\} &= \left\{ 1, \theta, \frac{(-a + S^2) + S\theta + \theta^2}{T} \right\} \\ &= \left\{ 1, \theta, \frac{(-a + t^2) + t\theta + \theta^2}{n} \right\} \end{aligned}$$

which proves the first part of Theorem 2.9.1.

Now we treat the excluded case $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$. We again break up the proof into three lemmas which are analogous to Lemmas 2.9.1–2.9.3.

Lemma 2.9.4

$$(T/3^2)^2 | (4a^3 - 27b^2)/3^6.$$

Proof : The proof follows from Table B. ■

Lemma 2.9.5

$$S^3 - aS + b \equiv 0 \pmod{3^3(T/3^2)^2}, \quad (2.9.37)$$

$$3S^2 - a \equiv 0 \pmod{3^2(T/3^2)}, \quad (2.9.38)$$

$$R \equiv -a + S^2 \pmod{3^2(T/3^2)}. \quad (2.9.39)$$

Proof : It is enough to show that

$$S^3 - aS + b \equiv 0 \pmod{3^{2T_3-1}}, \quad (2.9.40)$$

$$3S^2 - a \equiv 0 \pmod{3^{T_3}}, \quad (2.9.41)$$

$$R \equiv -a + S^2 \pmod{3^{T_3}}. \quad (2.9.42)$$

(2.9.41) is equivalent to

$$9S^4 - 6aS^2 + a^2 \equiv 0 \pmod{3^{2T_3}}. \quad (2.9.43)$$

Recall that

$$R \equiv R_3 \pmod{3^{T_3}}, \quad (2.9.44)$$

$$S \equiv S_3 \pmod{3^{T_3}}. \quad (2.9.45)$$

By Corollary 2.3.1, we have

$$R_3 \equiv -2(a/3) \pmod{3^{T_3}}, \quad (2.9.46)$$

$$2(a/3)S_3 \equiv b \pmod{3^{T_3+1}}, \quad (2.9.47)$$

$$T_3 = [s_3/2] - 1. \quad (2.9.48)$$

(2.9.41) is satisfied if and only if

$$S^2 \equiv (a/3) \pmod{3^{T_3-1}} \text{ if and only if, by (2.9.45), } S_3^2 \equiv (a/3) \pmod{3^{T_3-1}}$$

if and only if, by (2.9.47),

$$3^{\lfloor s_3/2 \rfloor + 1} | \Delta,$$

which is true.

(2.9.40) is satisfied if and only if

$$9S^4 - 9aS^2 + 9bS \equiv 0 \pmod{3^{2T_3+1}}$$

if and only if, by (2.9.43),

$$3aS^2 - 9bS + a^2 \equiv 0 \pmod{3^{2T_3+1}}$$

if and only if

$$2aS \equiv 3b \pmod{3^{T_3+1}},$$

which is true by (2.9.45) and (2.9.47).

(2.9.42) is satisfied if and only if, by (2.9.44)–(2.9.45)

$$R_3 \equiv -a + S_3^2 \pmod{3^{T_3}}$$

if and only if, by (2.9.46)–(2.9.47),

$$4a^3 - 27b^3 \equiv 0 \pmod{3^{T_3+3}},$$

which is satisfied. Hence the proof of Lemma 2.9.5 is complete. ■

Corollary 2.9.3 *The pair of congruences*

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{3^3(T/3^2)^2}, \\ 3t^2 - a \equiv 0 \pmod{3^2(T/3^2)}. \end{cases} \quad (2.9.49)$$

is simultaneously solvable with $t = S$.

Lemma 2.9.6 *If p is a prime such that*

$$(p(T/3^2))^2 | (4a^3 - 27b^2)/3^6 \quad (2.9.50)$$

then the pair of the congruences

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{3^3 p^2 (T/3^2)^2}, \\ 3t^2 - a \equiv 0 \pmod{3^3 p (T/3^2)}. \end{cases} \quad (2.9.51)$$

is not simultaneously solvable.

Proof : Since $3^2(T/3^2)^2 \nmid (4a^3 - 27b^2)/3^6$ the assertion of the lemma is obvious for $p = 3$. The rest goes the same as in lemma 2.9.3. ■

Corollary 2.9.4 *The largest integer n with $n^2 | \Delta/3^6$ and*

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{3^3 n^2}, \\ 3t^2 - a \equiv 0 \pmod{3^2 n}. \end{cases} \quad (2.9.52)$$

solvable is $n = T/9$.

To complete the proof of the second part of Theorem 2.9.1, we show that if t is a solution of the pair of congruences (2.9.5) then $t \equiv S \pmod{T}$ and $-t \equiv b \pmod{3}$. It is enough to show that $t \equiv S_3 \pmod{3^{T_3}}$ and $-t \equiv b \pmod{3}$.

It follows from the first equation of (2.9.5) that $b \equiv -t \pmod{3}$. If t is a solution of the pair of the congruences (2.9.5), we see, after a short calculation, that

$$2at \equiv 3b \pmod{3^{T_3+1}}. \quad (2.9.53)$$

It follows from (2.9.47) and (2.9.53) that

$$2at \equiv 2aS_3 \pmod{3^{T_3+1}}.$$

which gives $t \equiv S_3 \pmod{3^{T_3}}$.

Thus, it follows from the above Lemmas and Corollaries that an integral basis of K is

$$\left\{1, \frac{b+\theta}{3}, \frac{R+S\theta+\theta^2}{T}\right\} = \left\{1, \frac{-t+\theta}{3}, \frac{(-a+S^2)+S\theta+\theta^2}{T}\right\}$$

$$= \left\{1, \frac{-t+\theta}{3}, \frac{(-a+t^2)+t\theta+\theta^2}{9n}\right\}$$

which completes the proof of the second part of Theorem 2.9.1. ■

$$K = Q(\theta), \theta^3 - a\theta + b = 0$$

a	b	n	t	integral basis	$d(K)$
6	36	6	0	$\{1, \theta, (-6 + \theta^2)/6\}$	$-2^2 \cdot 3 \cdot 79$
6	32	6	4	$\{1, \theta, (10 + 4\theta + \theta^2)/6\}$	$-2^3 \cdot 3 \cdot 31$
30	52	2	2	$\{1, (-2 + \theta)/3, (-26 + 2\theta + \theta^2)/18\}$	$2^2 \cdot 3$
2	8	2	0	$\{1, \theta, (-2 + \theta^2)/2\}$	$-2^3 \cdot 53$
21	72	6	3	$\{1, \theta, (-12 + 3\theta + \theta^2)/6\}$	$-3 \cdot 953$
57	16	6	5	$\{1, \theta, (-32 + 5\theta + \theta^2)/6\}$	$3^3 \cdot 5 \cdot 151$
57	272	2	1	$\{1, (-1 + \theta)/3, (-56 + \theta + \theta^2)/18\}$	-43
1	4	2	1	$\{1, \theta, (\theta + \theta^2)/2\}$	-107
3	54	6	3	$\{1, \theta, (6 + 3\theta + \theta^2)/6\}$	$-2^3 \cdot 3 \cdot 7 \cdot 13$
39	34	6	5	$\{1, \theta, (-14 + 5\theta + \theta^2)/6\}$	$2^2 \cdot 3^3 \cdot 53$
255	3850	10	5	$\{1, (-5 + \theta)/3, (-230 + 5\theta + \theta^2)/90\}$	$-2^2 \cdot 5 \cdot 229$
7	2	2	1	$\{1, \theta, (-6 + \theta + \theta^2)/2\}$	$2^2 \cdot 79$
3	9	3	0	$\{1, \theta, (-3 + \theta^2)/3\}$	$-3 \cdot 7 \cdot 11$
3	7	3	2	$\{1, \theta, (1 + 2\theta + \theta^2)/3\}$	$-3^3 \cdot 5$
3	56	1	1	$\{1, (-1 + \theta)/3, (-2 + \theta + \theta^2)/9\}$	$-2^2 \cdot 29$
1	1	1	0	$\{1, \theta, -1 + \theta^2\}$	-23
21	-236	2	-25	$\{1, (25 + \theta)/3, (604 - 25\theta + \theta^2)/18\}$	-503
-11	4	2	1	$\{1, \theta, (12 + \theta + \theta^2)/2\}$	-1439
27	9	3	0	$\{1, \theta, (-27 + \theta^2)/3\}$	$3^5 \cdot 5 \cdot 7$
9	-6	1	0	$\{1, \theta, -9 + \theta^2\}$	$2^3 \cdot 3^5$

TABLE E

2.10 Alternative Form of a p -Integral Basis of a Cubic Field

In this section we give an alternative form of a p -integral basis which is analogous to Theorem 2.9.1.

Theorem 2.10.1 *Let α be the largest integer such that*

$$0 \leq 6\alpha \leq s_p \quad (2.10.1)$$

and

$$\begin{cases} 3t \equiv 0 \pmod{p^\alpha} \\ 3t^2 - a \equiv 0 \pmod{p^{2\alpha}} \\ t^3 - at + b \equiv 0 \pmod{p^{3\alpha}} \end{cases} \quad (2.10.2)$$

are simultaneously solvable for t . Let β be the largest integer such that

$$0 \leq 2\beta \leq s_p - 6\alpha \quad (2.10.3)$$

and

$$\begin{cases} 3t \equiv 0 \pmod{p^\alpha} \\ 3t^2 - a \equiv 0 \pmod{p^{2\alpha+\beta}} \\ t^3 - at + b \equiv 0 \pmod{p^{3\alpha+2\beta}} \end{cases} \quad (2.10.4)$$

are simultaneously solvable for t . Then

$$\left\{ 1, \frac{-t + \theta}{p^\alpha}, \frac{(t^2 - a) + t\theta + \theta^2}{p^{2\alpha+\beta}} \right\} \quad (2.10.5)$$

is a p -integral basis of K and

$$\nu_p(d(K)) = s_p - (6\alpha + 2\beta), \quad (2.10.6)$$

where t satisfies (2.10.4).

Proof: Let $p = 2$. We just treat the case A8, the other cases can be done similarly.

Case A8 : $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$ and $s_2 \equiv 1 \pmod{2}$.

It is easy to see that $\alpha = 0$. Let $\beta = (s_2 - 3)/2$. Set

$$2at \equiv 3b \pmod{2^{(s_2-1)/2}}. \quad (2.10.7)$$

(2.10.4) is equivalent to

$$\begin{cases} 3t^2 - a \equiv 0 \pmod{2^{(s_2-3)/2}}, \\ t^3 - at + b \equiv 0 \pmod{2^{s_2-3}}, \end{cases} \quad (2.10.8)$$

which is equivalent to

$$\begin{cases} 3(2at)^2 - 4a^3 \equiv 0 \pmod{2^{(s_2+1)/2}}, \\ (2at)^3 - 2^2 a^3 (2at) + 2^3 a^3 b \equiv 0 \pmod{2^{s_2}}. \end{cases} \quad (2.10.9)$$

Substituting $2at = 3b + A2^{(s_2-1)/2}$ into the previous system implies that (2.10.4) is solvable.

Let $\beta = (s_2 - 1)/2$. If (2.10.4) is solvable then we obtain

$$2at \equiv 3b \pmod{2^{(s_2-1)/2}}.$$

Substituting $2at = 3b + A2^{(s_2-1)/2}$ into the second equation of (2.10.4), we get

$$3^2 A^2 2^{(s_2-1)} - \Delta \equiv 0 \pmod{2^{s_2+1}},$$

which is a contradiction.

Let $p = 3$. We do the Case B11, the other cases can be done similarly.

Case B11 : $a \equiv 3 \pmod{9}$, $b^2 \equiv a + 1 \pmod{27}$.

It is easy to see that $\alpha = 1$. Let $\beta = (s_3 - 6)/2$. Suppose $s_2 \equiv 0 \pmod{2}$. Then (2.10.4) is equivalent to

$$\begin{cases} 3t^2 - a \equiv 0 \pmod{3^{(s_3-2)/2}}, \\ t^3 - at + b \equiv 0 \pmod{2^{s_3-3}}. \end{cases} \quad (2.10.10)$$

2 of/de 2

PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

PRECISIONSM RESOLUTION TARGETS

Taking $2at \equiv 3b \pmod{3^{s_3/2}}$ and substituting it into the previous system we obtain that (2.10.4) is solvable and β is the maximum.

Suppose $s_3 \equiv 1 \pmod{2}$. Let $\beta = (s_3 - 7)/2$. Then (2.10.4) is equivalent to

$$\begin{cases} 3t^2 - a \equiv 0 \pmod{3^{(s_3-3)/2}}, \\ t^3 - at + b \equiv 0 \pmod{2^{s_3-4}}, \end{cases} \quad (2.10.11)$$

Taking $2at \equiv 3b \pmod{3^{(s_3-1)/2}}$ and substituting it into the previous system we obtain that (2.10.4) is solvable and β is maximum.

Let $p > 3$. We give the details for the case C5, the other cases can be done similarly.

Case C5 : $\nu_p(a) = \nu_p(b) = 0$.

It is easy to see that $\alpha = 0$. Let $\beta = [s_p/2]$. (2.10.4) is equivalent to

$$\begin{cases} 3t^2 - a \equiv 0 \pmod{p^{[s_p/2]}}, \\ t^3 - at + b \equiv 0 \pmod{p^{2[s_p]}}. \end{cases} \quad (2.10.12)$$

Taking $2at \equiv 3b \pmod{p^{[s_p/2]}}$ and substituting it into the previous system we obtain that (2.10.4) is solvable and β is the maximum. ■

2.11 The Conductor of an Abelian Cubic Field

In this section we rederive the formula of Hasse [26] for the conductor $f(K)$ of an abelian cubic field in a form equivalent to that given by Huard, Spearman and Williams [30].

Theorem 2.11.1 *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^3 - ax + b, \quad a, b \in \mathbb{Z},$$

where a and b satisfy the simplifying assumption (2.1.2). Then K is an abelian field if and only if

$$4a^3 - 27b^2 = c^2$$

for some nonzero integer c .

Proof: Since K is an abelian cubic field, and $f(x)$ is a polynomial of degree 3 then the Galois group of $f(x)$ is A_3 , the alternating group of degree 3. Let $\theta = \theta^{(1)}, \theta^{(2)}, \theta^{(3)}$ be the roots of $f(x)$. As $4a^3 - 27b^2$ is the discriminant of $f(x)$, we have

$$4a^3 - 27b^2 = (\theta^{(1)} - \theta^{(2)})^2(\theta^{(1)} - \theta^{(3)})^2(\theta^{(2)} - \theta^{(3)})^2.$$

It is also easy to show that $(\theta^{(1)} - \theta^{(2)})(\theta^{(1)} - \theta^{(3)})(\theta^{(2)} - \theta^{(3)})$ is fixed under the Galois group A_3 of $f(x)$. Hence $(\theta^{(1)} - \theta^{(2)})(\theta^{(1)} - \theta^{(3)})(\theta^{(2)} - \theta^{(3)})$ is in Q . On the other hand, $(\theta^{(1)} - \theta^{(2)})(\theta^{(1)} - \theta^{(3)})(\theta^{(2)} - \theta^{(3)})$ is an algebraic integer, and so it must be in Z . Thus,

$$4a^3 - 27b^2 = c^2$$

for some nonzero integer c .

Conversely let

$$4a^3 - 27b^2 = (\theta^{(1)} - \theta^{(2)})^2(\theta^{(1)} - \theta^{(3)})^2(\theta^{(2)} - \theta^{(3)})^2 = c^2$$

for some nonzero integer c . Since $(\theta^{(1)} - \theta^{(2)})(\theta^{(1)} - \theta^{(3)})(\theta^{(2)} - \theta^{(3)})$ is not invariant under the symmetric group S_3 then the Galois group of $f(x)$ is A_3 . ■

Definition 2.11.1 Let K be an abelian extension of Q . Then the smallest positive integer f which satisfies $K \subseteq Q(e^{2\pi i/f})$ is called the conductor of K , and denoted by $f(K)$. (Such integers f exist by the Kronecker-Weber theorem.)

Theorem 2.11.2 Let $K = Q(\theta)$ be an abelian cubic field, where θ is a root of the irreducible polynomial

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). Then

$$d(K) = f(K)^2.$$

Proof: See [10, p. 219]

Theorem 2.11.3 Let $K = Q(\theta)$ be an abelian cubic field, where θ is a root of the irreducible polynomial

$$f(x) = x^3 - ax + b, \quad a, b \in Z,$$

where a and b satisfy the simplifying assumption (2.1.2). By Theorem 2.11.1,

$$4a^3 - 27b^2 = c^2 \quad (2.11.1)$$

for some nonzero integer c . Then the conductor $f(K)$ of K is given by

$$f(K) = 3^\alpha \prod_{\substack{p > 3 \\ 1 \leq \nu_p(b) \leq \nu_p(a)}} p,$$

where

$$\alpha = \begin{cases} 0 & , \text{if } 3 \nmid a \text{ or} \\ & 3 \parallel a, 3 \nmid b, 3^3 \mid c, \\ 2 & , \text{if } 3^2 \parallel a, 3^2 \parallel b \text{ or} \\ & 3 \parallel a, 3 \nmid b, 3^2 \parallel c. \end{cases}$$

Proof: First we show that $\nu_2(f(K)) = 0$. It follows from Table A that we need to treat only the cases A2-A3, A6 and A9.

Suppose $2 \mid a$, $2 \mid b$. Then $a = 2x$, $b = 2y$, $c = 2z$. It follows from (2.11.1) that $z^2 + 27y^2 \equiv 0 \pmod{8}$. Since $z^2, y^2 \equiv 0, 1, 4 \pmod{8}$, we have the following possibilities.

i) $z^2 \equiv y^2 \equiv 0 \pmod{8}$,

ii) $z^2 \equiv y^2 \equiv 4 \pmod{8}$.

I. $z^2 \equiv y^2 \equiv 0 \pmod{8}$ then $z \equiv y \equiv 0 \pmod{4}$. Then $x \equiv 0 \pmod{2}$. So, we obtain $a \equiv 0 \pmod{4}$ and $b \equiv 0 \pmod{8}$, a contradiction.

If $z^2 \equiv y^2 \equiv 4 \pmod{8}$ then $z \equiv y \equiv 2 \pmod{4}$. Then we obtain $8x^3 \equiv 16 \pmod{32}$ which gives $x^3 \equiv 2 \pmod{4}$, a contradiction. Hence cases A2-A3 cannot occur.

If $a \equiv 3 \pmod{4}$, $b \equiv 0 \pmod{4}$ then $c \equiv 0 \pmod{2}$. Then we obtain $(c/2)^2 \equiv a^3 \equiv -1 \pmod{4}$, a contradiction. Hence case A6 cannot occur.

If $a \equiv 3 \pmod{4}$, $b \equiv 2 \pmod{4}$, $s_2 \equiv 0 \pmod{4}$, $\Delta_2 \equiv 3 \pmod{4}$ then $c^2 = 4a^3 - 27b^2 = 2^{s_2}\Delta_2 = 2^{2t}\Delta_2$. Then $(c/2^t)^2 = \Delta_2 \equiv 3 \pmod{4}$, a contradiction, so case A9 cannot occur. Thus $\nu_2(f(K)) = 0$.

Now we determine $\nu_3(f(K))$. It follows from Table B that we need only treat cases B1, B4, B10-B11.

If $3 \nmid a$ then $\nu_3(f(K)) = 0$ which is the case B1.

If $3 \parallel a$, $3 \nmid b$, $3^3 \mid c$ then $\nu_3(f(K)) = 0$ which is the case B11.

If $3^2 \mid a$, $3^2 \mid b$ then $\nu_3(f(K)) = 2$ which is the case B4.

If $3 \mid a$, $3 \nmid b$, $3^2 \parallel c$ then $\nu_3(f(K)) = 2$ which is the case B10.

Finally we determine $\nu_p(f(K))$ for $p > 3$. It follows from Table C that only cases C2-C3 can contribute to $\nu_p(f(K))$ in which cases $\nu_p(f(K)) = 1$. ■

Chapter 3

p -INTEGRAL BASIS OF A QUARTIC FIELD

Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial

$$f(x) = x^4 + ax + b ; a, b \in Z.$$

Let p denote a rational prime. In Section 3.1 we develop the properties of p -integral elements of the quartic field K . In Sections 3.2 and 3.3 we determine a 2-integral basis and a 3-integral basis of K , respectively. In Section 3.4 we determine a p -integral basis of K for every rational prime $p > 3$. Using these results in Section 3.5 we give the discriminant $d(K)$ and an integral basis of K in one case.

3.1 Properties of p -Integral Elements of a Quartic Field

Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible quartic polynomial

$$f(x) = x^4 + ax + b ; a, b \in Z. \tag{3.1.1}$$

If for any rational prime p we have $\nu_p(a) \geq 3$ and $\nu_p(b) \geq 4$ then θ/p is an algebraic integer whose irreducible polynomial is

$$x^4 + (a/p^3)x + b/p^4.$$

Therefore we can assume that for every rational prime p

$$\nu_p(u) < 3 \quad \text{or} \quad \nu_p(b) < 4. \quad (3.1.2)$$

The discriminant of $f(x)$ (or θ) is the nonzero integer

$$\Delta = d(\theta) = 2^8 b^3 - 3^3 a^4, \quad (3.1.3)$$

and

$$\Delta = i(\theta)^2 d(K), \quad (3.1.4)$$

where $d(K)$ is the discriminant of K and the positive integer $i(\theta)$ is the index of θ .

For each prime p , we set

$$s_p = \nu_p(\Delta) \quad \text{and} \quad \Delta_p = \Delta / p^{s_p}. \quad (3.1.5)$$

Theorem 3.1.1 *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial (3.1.1) which is assumed to satisfy the simplifying assumption (3.1.2). Let*

$$\alpha = \frac{x + y\theta + z\theta^2 + w\theta^3}{p^m}, \quad (3.1.6)$$

where $x, y, z, w, m \in Z$, $m \geq 0$, and p is a rational prime. Set

$$\left. \begin{aligned} X &= 4x - 3aw, \\ Y &= 6x^2 - 9axw + 3ayz + 4byw + 2bz^2 + 3a^2w^2, \\ Z &= 4x^3 - 9ax^2w + 4bxz^2 + 8bxyw + 6axyz + 6a^2xw^2 - ay^3 \\ &\quad - 4by^2z - 3a^2yzw + a^2z^3 - 5abyw^2 + abz^2w + 4b^2zw^2 - a^3w^3, \\ W &= x^4 + 3ax^2yz + 2bx^2z^2 - axy^3 - 4bxy^2z - 3ax^3w + by^4 \\ &\quad + b^2z^4 + b^3w^4 + 3a^2x^2w^2 - 3a^2xyzw + a^2xz^3 - 5abxyw^2 \\ &\quad + abxz^2w + 4b^2xz^2w^2 - a^3xw^3 + 4bx^2yw + 3aby^2zw \\ &\quad + 2b^2y^2w^2 - abyz^3 - 4b^2yz^2w + a^2byw^3 - ab^2zw^3. \end{aligned} \right\} \quad (3.1.7)$$

Then α is p -integral if and only if

$$\begin{aligned} X &\equiv 0 \pmod{p^m}, \quad Y \equiv 0 \pmod{p^{2m}}, \\ Z &\equiv 0 \pmod{p^{3m}}, \quad W \equiv 0 \pmod{p^{4m}}. \end{aligned} \quad (3.1.8)$$

Proof: Let $\alpha^{(1)} = \alpha, \alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}$ denote the conjugates of α with respect to K . By Theorem 1.2.2, we know that α is p -integral if and only if the four quantities $\alpha + \alpha^{(2)} + \alpha^{(3)} + \alpha^{(4)}$, $\alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(4)} + \alpha^{(3)}\alpha^{(4)}$, $\alpha\alpha^{(2)}\alpha^{(3)} + \alpha\alpha^{(2)}\alpha^{(4)} + \alpha\alpha^{(3)}\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)}\alpha^{(4)}$, and $\alpha\alpha^{(2)}\alpha^{(3)}\alpha^{(4)}$ are p -integral in Q . To prove the theorem it is enough to show that

$$\alpha + \alpha^{(2)} + \alpha^{(3)} + \alpha^{(4)} = X/p^m,$$

$$\alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(4)} + \alpha^{(3)}\alpha^{(4)} = Y/p^{2m},$$

$$\alpha\alpha^{(2)}\alpha^{(3)} + \alpha\alpha^{(2)}\alpha^{(4)} + \alpha\alpha^{(3)}\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)}\alpha^{(4)} = Z/p^{3m},$$

$$\alpha\alpha^{(2)}\alpha^{(3)}\alpha^{(4)} = W/p^{4m}.$$

Let $\theta, \theta^{(2)}, \theta^{(3)}, \theta^{(4)}$ be the four roots of $f(x) = x^4 + ax + b$, so that

$$\left. \begin{aligned} \theta + \theta^{(2)} + \theta^{(3)} + \theta^{(4)} &= 0, \\ \theta\theta^{(2)} + \theta\theta^{(3)} + \theta\theta^{(4)} + \theta^{(2)}\theta^{(3)} + \theta^{(2)}\theta^{(4)} + \theta^{(3)}\theta^{(4)} &= 0, \\ \theta\theta^{(2)}\theta^{(3)} + \theta\theta^{(2)}\theta^{(4)} + \theta\theta^{(3)}\theta^{(4)} + \theta^{(2)}\theta^{(3)}\theta^{(4)} &= -a, \\ \theta\theta^{(2)}\theta^{(3)}\theta^{(4)} &= b \end{aligned} \right\} \quad (3.1.9)$$

We now use (3.1.9) to verify the following sixteen equalities :

$$\theta^2 + \theta^{(2)2} + \theta^{(3)2} + \theta^{(4)2} = 0, \quad (3.1.10)$$

$$\begin{aligned} &\theta^2\theta^{(2)} + \theta\theta^{(2)2} + \theta^2\theta^{(3)} + \theta\theta^{(3)2} + \theta^2\theta^{(4)} + \theta\theta^{(4)2} + \theta^{(2)2}\theta^{(3)} \\ &+ \theta^{(2)}\theta^{(3)2} + \theta^{(2)2}\theta^{(4)} + \theta^{(2)}\theta^{(4)2} + \theta^{(3)2}\theta^{(4)} + \theta^{(3)}\theta^{(4)2} = 3a, \end{aligned} \quad (3.1.11)$$

$$\theta^2\theta^{(2)2} + \theta^2\theta^{(3)2} + \theta^2\theta^{(4)2} + \theta^{(2)2}\theta^{(3)2} + \theta^{(2)2}\theta^{(4)2} + \theta^{(3)2}\theta^{(4)2} = 2b, \quad (3.1.12)$$

$$\begin{aligned} &\theta^2\theta^{(2)}\theta^{(3)} + \theta^2\theta^{(2)}\theta^{(4)} + \theta^2\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)2}\theta^{(3)} \\ &+ \theta\theta^{(2)2}\theta^{(4)} + \theta^{(2)2}\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)}\theta^{(3)2} + \theta\theta^{(3)2}\theta^{(4)} \\ &+ \theta^{(2)}\theta^{(3)2}\theta^{(4)} + \theta\theta^{(2)}\theta^{(4)2} + \theta\theta^{(3)}\theta^{(4)2} + \theta^{(2)}\theta^{(3)}\theta^{(4)2} = -4b, \end{aligned} \quad (3.1.13)$$

$$\begin{aligned}
& \theta^2 \theta^{(2)^2} \theta^{(3)} + \theta^2 \theta^{(2)^2} \theta^{(4)} + \theta^2 \theta^{(2)} \theta^{(3)^2} + \theta^2 \theta^{(3)^2} \theta^{(4)} \\
& + \theta^2 \theta^{(2)} \theta^{(4)^2} + \theta^2 \theta^{(3)} \theta^{(4)^2} + \theta \theta^{(2)^2} \theta^{(3)^2} + \theta^{(2)^2} \theta^{(3)^2} \theta^{(4)} \\
& + \theta \theta^{(2)^2} \theta^{(4)^2} + \theta^{(2)^2} \theta^{(3)} \theta^{(4)^2} + \theta \theta^{(3)^2} \theta^{(4)^2} + \theta^{(2)} \theta^{(3)^2} \theta^{(4)^2} = 0, \quad (3.1.14)
\end{aligned}$$

$$\theta^2 \theta^{(2)^2} \theta^{(3)^2} + \theta^2 \theta^{(2)^2} \theta^{(4)^2} + \theta^2 \theta^{(3)^2} \theta^{(4)^2} + \theta^{(2)^2} \theta^{(3)^2} \theta^{(4)^2} = a^2, \quad (3.1.15)$$

$$\theta^3 + \theta^{(2)^3} + \theta^{(3)^3} + \theta^{(4)^3} = -3a, \quad (3.1.16)$$

$$\begin{aligned}
& \theta^3 \theta^{(2)} + \theta \theta^{(2)^3} + \theta^3 \theta^{(3)} + \theta \theta^{(3)^3} + \theta^3 \theta^{(4)} + \theta \theta^{(4)^3} + \theta^{(2)^3} \theta^{(3)} \\
& + \theta^{(2)} \theta^{(3)^3} + \theta^{(2)^3} \theta^{(4)} + \theta^{(2)} \theta^{(4)^3} + \theta^{(3)^3} \theta^{(4)} + \theta^{(3)} \theta^{(4)^3} = 4b, \quad (3.1.17)
\end{aligned}$$

$$\begin{aligned}
& \theta^3 \theta^{(2)^2} + \theta^2 \theta^{(2)^3} + \theta^3 \theta^{(3)^2} + \theta^2 \theta^{(3)^3} + \theta^3 \theta^{(4)^2} + \theta^2 \theta^{(4)^3} + \theta^{(2)^3} \theta^{(3)^2} \\
& + \theta^{(2)^2} \theta^{(3)^3} + \theta^{(2)^3} \theta^{(4)^2} + \theta^{(2)^2} \theta^{(4)^3} + \theta^{(3)^3} \theta^{(4)^2} + \theta^{(3)^2} \theta^{(4)^3} = 0, \quad (3.1.18)
\end{aligned}$$

$$\theta^3 \theta^{(2)^3} + \theta^3 \theta^{(3)^3} + \theta^3 \theta^{(4)^3} + \theta^{(2)^3} \theta^{(3)^3} + \theta^{(2)^3} \theta^{(4)^3} + \theta^{(3)^3} \theta^{(4)^3} = 3a^2, \quad (3.1.19)$$

$$\begin{aligned}
& \theta^3 \theta^{(2)} \theta^{(3)} + \theta^3 \theta^{(2)} \theta^{(4)} + \theta^3 \theta^{(3)} \theta^{(4)} + \theta \theta^{(2)^3} \theta^{(3)} \\
& + \theta \theta^{(2)^3} \theta^{(4)} + \theta^{(2)^3} \theta^{(3)} \theta^{(4)} + \theta \theta^{(2)} \theta^{(3)^3} + \theta \theta^{(3)^3} \theta^{(4)} \\
& + \theta^{(2)} \theta^{(3)^3} \theta^{(4)} + \theta \theta^{(2)} \theta^{(4)^3} + \theta \theta^{(3)} \theta^{(4)^3} + \theta^{(2)} \theta^{(3)} \theta^{(4)^3} = 0, \quad (3.1.20)
\end{aligned}$$

$$\begin{aligned}
& \theta^3 \theta^{(2)^2} \theta^{(3)} + \theta^3 \theta^{(2)^2} \theta^{(4)} + \theta^3 \theta^{(2)} \theta^{(3)^2} + \theta^3 \theta^{(3)^2} \theta^{(4)} + \theta^3 \theta^{(2)} \theta^{(4)^2} \\
& + \theta^3 \theta^{(3)} \theta^{(4)^2} + \theta^2 \theta^{(2)^3} \theta^{(3)} + \theta^2 \theta^{(2)^3} \theta^{(4)} + \theta \theta^{(2)^3} \theta^{(3)^2} + \theta^{(2)^3} \theta^{(3)^2} \theta^{(4)} \\
& + \theta \theta^{(2)^3} \theta^{(4)^2} + \theta^{(2)^3} \theta^{(3)} \theta^{(4)^2} + \theta^2 \theta^{(2)} \theta^{(3)^3} + \theta^2 \theta^{(3)^3} \theta^{(4)} + \theta \theta^{(2)^2} \theta^{(3)^3} \\
& + \theta^{(2)^2} \theta^{(3)^3} \theta^{(4)} + \theta \theta^{(3)^3} \theta^{(4)^2} + \theta^{(2)} \theta^{(3)^3} \theta^{(4)^2} + \theta^2 \theta^{(2)} \theta^{(4)^3} + \theta^2 \theta^{(3)} \theta^{(4)^3} \\
& + \theta \theta^{(2)^2} \theta^{(4)^3} + \theta^{(2)^2} \theta^{(3)} \theta^{(4)^3} + \theta \theta^{(3)^2} \theta^{(4)^3} + \theta^{(2)} \theta^{(3)^2} \theta^{(4)^3} = -3a^2, \quad (3.1.21)
\end{aligned}$$

$$\begin{aligned}
& \theta^3 \theta^{(2)^3} \theta^{(3)} + \theta^3 \theta^{(2)^3} \theta^{(4)} + \theta^3 \theta^{(2)} \theta^{(3)^3} + \theta^3 \theta^{(3)^3} \theta^{(4)} \\
& + \theta^3 \theta^{(2)} \theta^{(4)^3} + \theta^3 \theta^{(3)} \theta^{(4)^3} + \theta \theta^{(2)^3} \theta^{(3)^3} + \theta^{(2)^3} \theta^{(3)^3} \theta^{(4)}
\end{aligned}$$

$$+\theta\theta^{(2)^3}\theta^{(4)^3} + \theta^{(2)^3}\theta^{(3)}\theta^{(4)^3} + \theta\theta^{(3)^3}\theta^{(4)^3} + \theta^{(2)}\theta^{(3)^3}\theta^{(4)^3} = -5ab, \quad (3.1.22)$$

$$\begin{aligned} &\theta^3\theta^{(2)^2}\theta^{(3)^2} + \theta^3\theta^{(2)^2}\theta^{(4)^2} + \theta^3\theta^{(3)^2}\theta^{(4)^2} + \theta^2\theta^{(2)^3}\theta^{(3)^2} \\ &+ \theta^2\theta^{(2)^3}\theta^{(4)^2} + \theta^{(2)^3}\theta^{(3)^2}\theta^{(4)^2} + \theta^2\theta^{(2)^2}\theta^{(3)^3} + \theta^2\theta^{(3)^3}\theta^{(4)^2} \\ &+ \theta^{(2)^2}\theta^{(3)^3}\theta^{(4)^2} + \theta^2\theta^{(2)^2}\theta^{(4)^3} + \theta^2\theta^{(3)^2}\theta^{(4)^3} + \theta^{(2)^2}\theta^{(3)^2}\theta^{(4)^3} = ab, \end{aligned} \quad (3.1.23)$$

$$\begin{aligned} &\theta^3\theta^{(2)^3}\theta^{(3)^2} + \theta^3\theta^{(2)^3}\theta^{(4)^2} + \theta^3\theta^{(2)^2}\theta^{(3)^3} + \theta^3\theta^{(3)^3}\theta^{(4)^2} \\ &+ \theta^3\theta^{(2)^2}\theta^{(4)^3} + \theta^3\theta^{(3)^2}\theta^{(4)^3} + \theta^2\theta^{(2)^3}\theta^{(3)^3} + \theta^{(2)^3}\theta^{(3)^3}\theta^{(4)^2} \\ &+ \theta^2\theta^{(2)^3}\theta^{(4)^3} + \theta^{(2)^3}\theta^{(3)^2}\theta^{(4)^3} + \theta^2\theta^{(3)^3}\theta^{(4)^3} + \theta^{(2)^2}\theta^{(3)^3}\theta^{(4)^3} = 4b^2, \end{aligned} \quad (3.1.24)$$

$$\theta^3\theta^{(2)^3}\theta^{(3)^3} + \theta^3\theta^{(2)^3}\theta^{(4)^3} + \theta^3\theta^{(3)^3}\theta^{(4)^3} + \theta^{(2)^3}\theta^{(3)^3}\theta^{(4)^3} = -a^3. \quad (3.1.25)$$

We now make use of (3.1.9)–(3.1.25) to determine

$$\alpha + \alpha^{(2)} + \alpha^{(3)} + \alpha^{(4)}, \alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(4)} + \alpha^{(3)}\alpha^{(4)}$$

$$\alpha\alpha^{(2)}\alpha^{(3)} + \alpha\alpha^{(2)}\alpha^{(4)} + \alpha\alpha^{(3)}\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)}\alpha^{(4)} \text{ and } \alpha\alpha^{(2)}\alpha^{(3)}\alpha^{(4)}.$$

First

$$\begin{aligned} \alpha + \alpha^{(2)} + \alpha^{(3)} + \alpha^{(4)} &= \frac{1}{p^m} [4x + y(\theta + \theta^{(2)} + \theta^{(3)} + \theta^{(4)}) \\ &\quad + z(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2} + \theta^{(4)^2}) + w(\theta^3 + \theta^{(2)^3} + \theta^{(3)^2} + \theta^{(4)^3})] \\ &= \frac{1}{p^m} (4x - 3aw) = X/p^m. \end{aligned}$$

Secondly

$$\begin{aligned} &\alpha\alpha^{(2)} + \alpha\alpha^{(3)} + \alpha\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(2)}\alpha^{(4)} + \alpha^{(3)}\alpha^{(4)} \\ &= (\alpha^{(2)} + \alpha^{(3)})\alpha + (\alpha^{(3)} + \alpha^{(4)})\alpha^{(2)} + (\alpha + \alpha^{(3)})\alpha^{(4)} \\ &= \frac{1}{p^{2m}} [(2x + y(\theta^{(2)} + \theta^{(3)}) + z(\theta^{(2)^2} + \theta^{(3)^2}) + w(\theta^{(2)^3} + \theta^{(3)^3}))(x + y\theta + z\theta^2 + w\theta^3) \\ &\quad + (2x + y(\theta^{(3)} + \theta^{(4)}) + z(\theta^{(3)^2} + \theta^{(4)^2}) + w(\theta^{(3)^3} + \theta^{(4)^3}))(x + y\theta^{(2)} + z\theta^{(2)^2} + w\theta^{(2)^3})] \end{aligned}$$

$$\begin{aligned}
& + (2x + y(\theta + \theta^{(3)}) + z(\theta^2 + \theta^{(3)^2}) + w(\theta^3 + \theta^{(3)^3}))(x + y\theta^{(4)} + z\theta^{(4)^2} + w\theta^{(4)^3})] \\
& = \frac{1}{p^{2m}} [6x^2 + 3xy(\theta + \theta^{(2)} + \theta^{(3)} + \theta^{(4)}) + 3xz(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2} + \theta^{(4)^2}) \\
& + 3xw(\theta^3 + \theta^{(2)^3} + \theta^{(3)^3} + \theta^{(4)^3}) + y^2(\theta\theta^{(2)} + \theta\theta^{(3)} + \theta^{(2)}\theta^{(3)} + \theta^{(2)}\theta^{(4)} + \theta\theta^{(4)} + \theta^{(3)}\theta^{(4)}) \\
& + yz(\theta^2\theta^{(2)} + \theta^2\theta^{(3)} + \theta\theta^{(2)^2} + \theta\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)} + \theta^{(2)^2}\theta^{(4)} + \theta^{(2)}\theta^{(3)^2} + \theta^{(2)}\theta^{(4)^2} \\
& + \theta\theta^{(4)^2} + \theta^{(3)}\theta^{(4)^2} + \theta^2\theta^{(4)} + \theta^{(3)^2}\theta^{(4)}) \\
& + yw(\theta^3\theta^{(2)} + \theta^3\theta^{(3)} + \theta\theta^{(2)^3} + \theta\theta^{(3)^3} + \theta^{(2)^3}\theta^{(3)} + \theta^{(2)^3}\theta^{(4)} + \theta^{(2)}\theta^{(3)^3} + \theta^{(2)}\theta^{(4)^3} \\
& + \theta\theta^{(4)^3} + \theta^{(3)}\theta^{(4)^3} + \theta^3\theta^{(4)} + \theta^{(3)^3}\theta^{(4)}) \\
& + z^2(\theta^2\theta^{(2)^2} + \theta^2\theta^{(3)^2} + \theta^{(2)^2}\theta^{(3)^2} + \theta^{(2)^2}\theta^{(4)^2} + \theta^2\theta^{(4)^2} + \theta^{(3)^2}\theta^{(4)^2}) \\
& + zw(\theta^3\theta^{(2)^2} + \theta^3\theta^{(3)^2} + \theta^2\theta^{(2)^3} + \theta^2\theta^{(3)^3} + \theta^{(2)^3}\theta^{(3)^2} + \theta^{(2)^3}\theta^{(4)^2} + \theta^{(2)^2}\theta^{(3)^3} + \theta^{(2)^2}\theta^{(4)^3} \\
& + \theta^2\theta^{(4)^3} + \theta^{(3)^2}\theta^{(4)^3} + \theta^3\theta^{(4)^2} + \theta^{(3)^3}\theta^{(4)^2}) \\
& + w^2(\theta^3\theta^{(2)^3} + \theta^3\theta^{(3)^3} + \theta^{(2)^3}\theta^{(3)^3} + \theta^{(2)^3}\theta^{(4)^3} + \theta^3\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)^3})] \\
& = \frac{1}{p^{2m}} [6x^2 - 9axw + 3ayz + 4byw + 2bz^2 + 3a^2w^2] \\
& = Y/p^{2m}.
\end{aligned}$$

Thirdly

$$\begin{aligned}
& \alpha\alpha^{(2)}\alpha^{(3)} + \alpha\alpha^{(2)}\alpha^{(4)} + \alpha\alpha^{(3)}\alpha^{(4)} + \alpha^{(2)}\alpha^{(3)}\alpha^{(4)} = (\alpha^{(3)} + \alpha^{(4)})\alpha\alpha^{(2)} + (\alpha + \alpha^{(2)})\alpha^{(3)}\alpha^{(4)} \\
& = \frac{1}{p^{3m}} [(2x + y(\theta^{(3)} + \theta^{(4)}) + z(\theta^{(3)^2} + \theta^{(4)^2}) + w(\theta^{(3)^3} + \theta^{(4)^3})) \\
& \quad (x + y\theta + z\theta^2 + w\theta^3)(x + y\theta^{(2)} + z\theta^{(2)^2} + w\theta^{(2)^3}) \\
& + (2x + y(\theta + \theta^{(2)}) + z(\theta^2 + \theta^{(2)^2}) + w(\theta^3 + \theta^{(2)^3})) \\
& \quad (x + y\theta^{(3)} + z\theta^{(3)^2} + w\theta^{(3)^3})(x + y\theta^{(4)} + z\theta^{(4)^2} + w\theta^{(4)^3})] \\
& = \frac{1}{p^{3m}} [4x^3 + 3x^2w(\theta^3 + \theta^{(2)^3} + \theta^{(3)^3} + \theta^{(4)^3})
\end{aligned}$$

$$\begin{aligned}
& +2xyz(\theta\theta^{(2)^2} + \theta^2\theta^{(2)} + \theta\theta^{(3)^2} + \theta^2\theta^{(3)} + \dots + \theta^{(3)}\theta^{(4)^2} + \theta^{(3)^2}\theta^{(4)}) \\
& +2xyw(\theta\theta^{(2)^3} + \theta^3\theta^{(2)} + \theta\theta^{(3)^3} + \theta^3\theta^{(3)} + \dots + \theta^{(3)}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)}) \\
& +xz^2(2\theta^2\theta^{(2)^2} + (\theta^2 + \theta^{(2)^2})(\theta^{(3)^2} + \theta^{(4)^2}) + 2\theta^{(3)^2}\theta^{(4)^2} + (\theta^2 + \theta^{(2)^2})(\theta^{(3)^2} + \theta^{(4)^2})) \\
& +2xzw(\theta^2\theta^{(2)^3} + \theta^3\theta^{(2)^2} + \theta^2\theta^{(3)^3} + \theta^3\theta^{(3)^2} + \dots + \theta^{(3)^2}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)^2}) \\
& +xw^2(2\theta^3\theta^{(2)^3} + (\theta^3 + \theta^{(2)^3})(\theta^{(3)^3} + \theta^{(4)^3}) + 2\theta^{(3)^3}\theta^{(4)^3} + (\theta^3 + \theta^{(2)^3})(\theta^{(3)^3} + \theta^{(4)^3})) \\
& +y^3(\theta\theta^{(2)}\theta^{(3)} + \theta\theta^{(2)}\theta^{(4)} + \theta\theta^{(3)}\theta^{(4)} + \theta^{(2)}\theta^{(3)}\theta^{(4)}) \\
& +y^2z(\theta^2\theta^{(2)}\theta^{(3)} + \theta^2\theta^{(2)}\theta^{(4)} + \theta^2\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)^2}\theta^{(3)} + \theta\theta^{(2)^2}\theta^{(4)} + \theta^{(2)^2}\theta^{(3)}\theta^{(4)} \\
& +\theta\theta^{(2)}\theta^{(3)^2} + \theta\theta^{(3)^2}\theta^{(4)} + \theta^{(2)}\theta^{(3)^2}\theta^{(4)} + \theta\theta^{(2)}\theta^{(4)^2} + \theta\theta^{(3)}\theta^{(4)^2} + \theta^{(2)}\theta^{(3)}\theta^{(4)^2}) \\
& y^2w((\theta\theta^{(2)^3} + \theta^3\theta^{(2)})(\theta^{(3)} + \theta^{(4)}) + \theta\theta^{(2)}(\theta^{(3)^3} + \theta^{(4)^3}) \\
& +(\theta + \theta^{(2)})(\theta^{(3)}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)}) + (\theta^3 + \theta^{(2)^3})\theta^{(3)}\theta^{(4)}) \\
& yz^2(\theta^2\theta^{(2)^2}(\theta^{(3)} + \theta^{(4)}) + (\theta\theta^{(2)^2} + \theta^2\theta^{(2)})(\theta^{(3)^2} + \theta^{(4)^2}) \\
& +(\theta + \theta^{(2)})\theta^{(3)^2}\theta^{(4)^2} + (\theta^2 + \theta^{(2)^2})(\theta^{(3)}\theta^{(4)^2} + \theta^{(3)^2}\theta^{(4)})) \\
& +yzw(\theta^2\theta^{(2)^3}\theta^{(3)} + \theta^2\theta^{(2)^3}\theta^{(4)} + \theta^3\theta^{(2)^2}\theta^{(3)} + \theta^3\theta^{(2)^2}\theta^{(4)} + \dots + \theta\theta^{(3)^2}\theta^{(4)^3} \\
& +\theta^{(2)}\theta^{(3)^2}\theta^{(4)^3} + \theta\theta^{(3)^3}\theta^{(4)^2} + \theta^{(2)}\theta^{(3)^3}\theta^{(4)^2}) \\
& +yw^2(\theta^3\theta^{(2)^3}\theta^{(3)} + \theta^3\theta^{(2)^3}\theta^{(4)} + \dots + \theta\theta^{(3)^3}\theta^{(4)^3} + \theta^{(2)}\theta^{(3)^3}\theta^{(4)^3}) \\
& +z^3(\theta^2\theta^{(2)^2}(\theta^{(3)^2} + \theta^{(4)^2}) + \theta^{(3)^2}\theta^{(4)^2}(\theta^2 + \theta^{(2)^2})) \\
& +z^2w(\theta^2\theta^{(2)^2}\theta^{(3)^3} + \theta^2\theta^{(2)^2}\theta^{(4)^3} + \dots + \theta^3\theta^{(3)^2}\theta^{(4)^2} + \theta^{(2)^3}\theta^{(3)^2}\theta^{(4)^2}) \\
& +zw^2(\theta^3\theta^{(2)^3}\theta^{(3)^2} + \theta^3\theta^{(2)^3}\theta^{(4)^2} + \dots + \theta^2\theta^{(3)^3}\theta^{(4)^3} + \theta^{(2)^2}\theta^{(3)^3}\theta^{(4)^3}) \\
& +w^3(\theta^3\theta^{(2)^3}(\theta^{(3)^3} + \theta^{(4)^3}) + (\theta^3 + \theta^{(2)^3})\theta^{(3)^3}\theta^{(4)^3})] \\
& = \frac{1}{p^{3m}}(4x^3 - 9ax^2w + 4bxz^2 + 8bxyw + 6axyz + 6a^2xw^2 - ay^3
\end{aligned}$$

$$\begin{aligned}
& -4by^2z - 3a^2yzw + a^2z^3 - 5abyw^2 + abz^2w + 4b^2zw^2 - a^3w^3) \\
& = Z/p^{3m}.
\end{aligned}$$

Finally

$$\begin{aligned}
\alpha^{(1)}\alpha^{(2)}\alpha^{(3)}\alpha^{(4)} &= \frac{1}{p^{4m}}[(x + y\theta + z\theta^2 + w\theta^3)(x + y\theta^{(2)} + z\theta^{(2)^2} + w\theta^{(2)^3}) \\
&\quad (x + y\theta^{(3)} + z\theta^{(3)^2} + w\theta^{(3)^3})(x + y\theta^{(4)} + z\theta^{(4)^2} + w\theta^{(4)^3})] \\
&= \frac{1}{p^{4m}}[x^4 + x^3y(\theta + \theta^{(2)} + \theta^{(3)} + \theta^{(4)}) + x^3z(\theta^2 + \theta^{(2)^2} + \theta^{(3)^2} + \theta^{(4)^2}) \\
&\quad + x^3w(\theta^3 + \theta^{(2)^3} + \theta^{(3)^3} + \theta^{(4)^3}) + x^2y^2(\theta\theta^{(2)} + \theta\theta^{(3)} + \theta\theta^{(4)} + \theta^{(2)}\theta^{(3)} + \theta^{(2)}\theta^{(4)} + \theta^{(3)}\theta^{(4)}) \\
&\quad + x^2yz(\theta\theta^{(2)^2} + \theta^2\theta^{(2)} + \theta\theta^{(3)^2} + \theta^2\theta^{(3)} + \dots + \theta^{(3)}\theta^{(4)^2} + \theta^{(3)^2}\theta^{(4)}) \\
&\quad + x^2yw(\theta\theta^{(2)^3} + \theta^3\theta^{(2)} + \theta\theta^{(3)^3} + \theta^3\theta^{(3)} + \dots + \theta^{(3)}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)}) \\
&\quad + x^2z^2(\theta^2\theta^{(2)^2} + \theta^2\theta^{(3)^2} + \theta^2\theta^{(4)^2} + \theta^{(2)^2}\theta^{(3)^2} + \theta^{(2)^2}\theta^{(4)^2} + \theta^{(3)^2}\theta^{(4)^2}) \\
&\quad + x^2zw(\theta^{(3)^2}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)^2} + \theta^2\theta^{(3)^3} + \theta^2\theta^{(4)^3} + \theta^{(2)^2}\theta^{(3)^3} + \theta^{(2)^2}\theta^{(4)^3} + \theta^3\theta^{(3)^2} + \theta^3\theta^{(4)^2} \\
&\quad + \theta^{(2)^3}\theta^{(3)^2} + \theta^{(2)^3}\theta^{(4)^2} + \theta^2\theta^{(2)^3} + \theta^3\theta^{(2)^2}) \\
&\quad + x^2w^2(\theta^3\theta^{(2)^3} + \theta^3\theta^{(3)^3} + \theta^3\theta^{(4)^3} + \theta^{(2)^3}\theta^{(3)^3} + \theta^{(2)^3}\theta^{(4)^3} + \theta^{(3)^3}\theta^{(4)^3}) \\
&\quad + xy^3(\theta\theta^{(3)}\theta^{(4)} + \theta^{(2)}\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)}\theta^{(3)} + \theta\theta^{(2)}\theta^{(4)}) \\
&\quad + xy^2z(\theta\theta^{(3)}\theta^{(4)^2} + \theta^{(2)}\theta^{(3)}\theta^{(4)^2} + \theta\theta^{(3)^2}\theta^{(4)} + \theta^{(2)}\theta^{(3)^2}\theta^{(4)} + \theta\theta^{(2)}\theta^{(3)^2} + \theta\theta^{(2)}\theta^{(4)^2} \\
&\quad + \theta\theta^{(2)^2}\theta^{(3)} + \theta\theta^{(2)^2}\theta^{(4)} + \theta^2\theta^{(2)}\theta^{(3)} + \theta^2\theta^{(2)}\theta^{(4)} + \theta^2\theta^{(3)}\theta^{(4)} + \theta^{(2)^2}\theta^{(3)}\theta^{(4)}) \\
&\quad + xy^2w(\theta\theta^{(3)}\theta^{(4)^3} + \theta^{(2)}\theta^{(3)}\theta^{(4)^3} + \theta\theta^{(3)^3}\theta^{(4)} + \theta^{(2)}\theta^{(3)^3}\theta^{(4)} + \theta^3\theta^{(3)}\theta^{(4)} + \theta^{(2)^3}\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)}\theta^{(3)^3} \\
&\quad + \theta\theta^{(2)}\theta^{(4)^3} + \theta\theta^{(2)^3}\theta^{(3)} + \theta\theta^{(2)^3}\theta^{(4)} + \theta^3\theta^{(2)}\theta^{(3)} + \theta^3\theta^{(2)}\theta^{(4)}) \\
&\quad + xyz^2(\theta\theta^{(3)^2}\theta^{(4)^2} + \theta^{(2)}\theta^{(3)^2}\theta^{(4)^2} + \theta^2\theta^{(3)}\theta^{(4)^2} + \theta^2\theta^{(3)^2}\theta^{(4)} + \theta^{(2)^2}\theta^{(3)}\theta^{(4)^2} + \theta^{(2)^2}\theta^{(3)^2}\theta^{(4)} \\
&\quad + \theta\theta^{(2)^2}\theta^{(3)^2} + \theta\theta^{(2)^2}\theta^{(4)^2} + \theta^2\theta^{(2)}\theta^{(3)^2} + \theta^2\theta^{(2)}\theta^{(4)^2} + \theta^2\theta^{(2)^2}\theta^{(3)} + \theta^2\theta^{(2)^2}\theta^{(4)})]
\end{aligned}$$

$$\begin{aligned}
& +xyzw(\theta\theta(3)^2\theta(4)^3 + \theta(2)\theta(3)^2\theta(4)^3 + \theta\theta(3)^3\theta(4)^2 + \theta(2)\theta(3)^3\theta(4)^2 + \theta^2\theta(3)\theta(4)^3 + \theta(2)^2\theta(3)\theta(4)^3 \\
& + \theta^2\theta(3)^3\theta(4) + \theta(2)^2\theta(3)^3\theta(4) + \theta^3\theta(3)\theta(4)^2 + \theta(2)^3\theta(3)\theta(4)^2 + \theta^3\theta(3)^2\theta(4) + \theta(2)^3\theta(3)^2\theta(4) \\
& + \theta\theta(2)^2\theta(3)^3 + \theta\theta(2)^2\theta(4)^3 + \theta^2\theta(2)\theta(3)^3 + \theta^2\theta(2)\theta(4)^3 + \theta\theta(2)^3\theta(3)^2 + \theta\theta(2)^3\theta(4)^2 \\
& + \theta^3\theta(2)\theta(3)^2 + \theta^3\theta(2)\theta(4)^2 + \theta^2\theta(2)^3\theta(3) + \theta^2\theta(2)^3\theta(4) + \theta^3\theta(2)^2\theta(3) + \theta^3\theta(2)^2\theta(4)) \\
& +xyzw^2(\theta\theta(3)^3\theta(4)^3 + \theta(2)\theta(3)^3\theta(4)^3 + \theta^3\theta(3)\theta(4)^3 + \theta^3\theta(3)^3\theta(4) + \theta(2)^3\theta(3)\theta(4)^3 + \theta(2)^3\theta(3)^3\theta(4) \\
& + \theta\theta(2)^3\theta(3)^3 + \theta\theta(2)^3\theta(4)^3 + \theta^3\theta(2)\theta(3)^3 + \theta^3\theta(2)\theta(4)^3 + \theta^3\theta(2)^3\theta(3) + \theta^3\theta(2)^3\theta(4)) \\
& +xz^3(\theta^2\theta(3)^2\theta(4)^2 + \theta(2)^2\theta(3)^2\theta(4)^2 + \theta^2\theta(2)^2\theta(3)^2 + \theta^2\theta(2)^2\theta(4)^2) \\
& +xz^2w(\theta^2\theta(3)^2\theta(4)^3 + \theta(2)^2\theta(3)^2\theta(4)^3 + \theta^2\theta(3)^3\theta(4)^2 + \theta(2)^2\theta(3)^3\theta(4)^2 + \theta^3\theta(3)^2\theta(4)^2 + \theta(2)^3\theta(3)^2\theta(4)^2 \\
& + \theta^2\theta(2)^2\theta(3)^3 + \theta^2\theta(2)^2\theta(4)^3 + \theta^2\theta(2)^3\theta(3)^2 + \theta^2\theta(2)^3\theta(4)^2 + \theta^3\theta(2)^2\theta(3)^2 + \theta^3\theta(2)^2\theta(4)^2) \\
& +xzw^2(\theta^2\theta(3)^3\theta(4)^3 + \theta(2)^2\theta(3)^3\theta(4)^3 + \theta^3\theta(3)^2\theta(4)^3 + \theta^3\theta(3)^3\theta(4)^2 + \theta(2)^3\theta(3)^2\theta(4)^3 + \theta(2)^3\theta(3)^3\theta(4)^2 \\
& + \theta^2\theta(2)^3\theta(3)^3 + \theta^2\theta(2)^3\theta(4)^3 + \theta^3\theta(2)^2\theta(3)^3 + \theta^3\theta(2)^2\theta(4)^3 + \theta^3\theta(2)^3\theta(3)^2 + \theta^3\theta(2)^3\theta(4)^2) \\
& +xw^3(\theta^3\theta(3)^3\theta(4)^3 + \theta(2)^3\theta(3)^3\theta(4)^3 + \theta^3\theta(2)^3\theta(3)^3 + \theta^3\theta(2)^3\theta(4)^3) + by^4 \\
& +y^3zb(\theta(4) + \theta(3) + \theta(2) + \theta) + y^3wb(\theta(4)^2 + \theta(3)^2 + \theta(2)^2 + \theta^2) \\
& +y^2z^2b(\theta(3)\theta(4) + \theta(2)\theta(4) + \theta(2)\theta(3) + \theta\theta(4) + \theta\theta(3) + \theta\theta(2)) \\
& +y^2zwb(\theta(3)\theta(4)^2 + \theta(3)^2\theta(4) + \theta(2)\theta(4)^2 + \theta(2)\theta(3)^2 + \theta\theta(4)^2 + \theta\theta(3)^2 + \theta(2)^2\theta(4) \\
& + \theta(2)^2\theta(3) + \theta^2\theta(4) + \theta^2\theta(3) + \theta\theta(2)^2 + \theta^2\theta(2)) \\
& +yz^3b(\theta(2)\theta(3)\theta(4) + \theta\theta(3)\theta(4) + \theta\theta(2)\theta(4) + \theta\theta(2)\theta(3)) \\
& +yz^2wb(\theta(2)\theta(3)\theta(4)^2 + \theta\theta(3)\theta(4)^2 + \theta(2)\theta(3)^2\theta(4) + \theta\theta(3)^2\theta(4) + \theta(2)^2\theta(3)\theta(4) + \theta^2\theta(3)\theta(4) + \theta\theta(2)\theta(4) \\
& + \theta\theta(2)\theta(3)^2 + \theta\theta(2)^2\theta(4) + \theta\theta(2)^2\theta(3) + \theta^2\theta(2)\theta(4) + \theta^2\theta(2)\theta(3)) \\
& +y^2w^2b(\theta(3)^2\theta(4)^2 + \theta(2)^2\theta(4)^2 + \theta(2)^2\theta(3)^2 + \theta^2\theta(4)^2 + \theta^2\theta(3)^2 + \theta^2\theta(2)^2)
\end{aligned}$$

$$\begin{aligned}
& + yzw^2b(\theta^{(2)}\theta^{(3)^2}\theta^{(4)^2} + \theta\theta^{(3)^2}\theta^{(4)^2} + \theta^{(2)^2}\theta^{(3)}\theta^{(4)^2} + \theta^{(2)^2}\theta^{(3)^2}\theta^{(4)} + \theta^2\theta^{(3)}\theta^{(4)^2} + \theta^2\theta^{(3)^2}\theta^{(4)} \\
& + \theta\theta^{(2)^2}\theta^{(4)^2} + \theta\theta^{(2)^2}\theta^{(3)^2} + \theta^2\theta^{(2)}\theta^{(4)^2} + \theta^2\theta^{(2)}\theta^{(3)^2} + \theta^2\theta^{(2)^2}\theta^{(4)} + \theta^2\theta^{(2)^2}\theta^{(3)}) \\
& + yw^3b(\theta^{(2)^2}\theta^{(3)^2}\theta^{(4)^2} + \theta^2\theta^{(3)^2}\theta^{(4)^2} + \theta^2\theta^{(2)^2}\theta^{(4)^2} + \theta^2\theta^{(2)^2}\theta^{(3)^2}) + b^2z^4 \\
& + z^3wb^3(\theta^{(4)} + \theta^{(3)} + \theta^{(2)} + \theta) \\
& + z^2w^2b^2(\theta^{(3)}\theta^{(4)} + \theta^{(2)}\theta^{(4)} + \theta^{(2)}\theta^{(3)} + \theta\theta^{(4)} + \theta\theta^{(3)} + \theta\theta^{(2)}) \\
& + zw^3b^2(\theta^{(2)}\theta^{(3)}\theta^{(4)} + \theta\theta^{(3)}\theta^{(4)} + \theta\theta^{(2)}\theta^{(4)} + \theta\theta^{(2)}\theta^{(3)}) + b^3w^4] \\
& = \frac{1}{p^{4m}}(x^4 + 3ax^2yz + 2bx^2z^2 - axy^3 - 4bxy^2z - 3ax^3w + by^4 \\
& + b^2z^4 + b^3w^4 + 3a^2x^2w^2 - 3a^2xyzw + a^2xz^3 - 5abxyw^2 \\
& + abxz^2w + 4b^2xzw^2 - a^3xw^3 + 4bx^2yw + 3aby^2zw \\
& + 2b^2y^2w^2 - aby^3z - 4b^2yz^2w + a^2byw^3 - ab^2zw^3) \\
& = W/p^{4m}.
\end{aligned}$$

This completes the proof. ■

Theorem 3.1.2 *With the same notation as in Theorem 3.1.1 and with $w = 1$, set*

$$\begin{aligned}
X &= 4x - 3a \\
U &= 3^2a^2y - 2^4b^2, \\
V &= 3az + 4b,
\end{aligned}$$

Then,

$$\begin{aligned}
Y &= \frac{1}{2^33^2a^2}[3^3a^2X^2 + 2^3(U + 2bV)V + \Delta], \\
Z &= \frac{1}{2^43^6a^5}[3^6a^5X^3 - 2^4U^3 + 2^43^3a^4V^3 + 2^43^4a^3bV^2X \\
&\quad - 2^63bU^2V + 2^33^4a^3UVX - 2^33\Delta UV + 3^4a^3\Delta X]
\end{aligned} \tag{3.1.26}$$

$$+2^4 3 b \Delta U - 2^6 3 b^2 \Delta V + 2 \Delta^2], \quad (3.1.27)$$

$$\begin{aligned} W = & \frac{1}{2^8 3^8 a^8} [3^8 a^8 X^4 + 2^5 3^6 a^6 b V^2 X^2 + 2^4 3^6 a^6 U V X^2 + 2^6 3^5 a^7 V^3 X \\ & - 2^8 3^3 a^3 b U^2 V X - 2^6 3^2 a^3 U^3 X + 2^8 3^4 a^4 b^2 V^4 - 2^8 3^3 a^4 b U V^3 \\ & + 2^8 b U^4 - 2^5 3^3 a^3 \Delta U V X - 2^6 3^3 a^4 \Delta V^3 + 2^6 \Delta U^3 \\ & + 2 \cdot 3^6 a^6 \Delta X^2 - 2^8 3^3 a^3 b^2 \Delta V X + 2^6 3^3 a^3 b \Delta U X + 2^5 3^5 a^4 b \Delta V^2 \\ & + 2^4 3^4 a^4 \Delta U V + 2^9 3 b^2 \Delta U^2 + 2^3 3^2 a^3 \Delta^2 X + 2^6 b \Delta^2 U + \Delta^3] \quad (3.1.28) \end{aligned}$$

Proof: Substituting the expressions for U, V and X in terms of x, y, z, a and b into the expressions on the right sides of (3.1.26), (3.1.27) and (3.1.28), we obtain the respective left sides on appealing to (3.1.7). ■

We end this section with the following theorem which plays an important role in the calculation of an integral basis of a quartic field. This theorem is the special case $n = 4$ of Theorem 1.3.4.

Theorem 3.1.3 *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial (3.1.1), which is assumed to satisfy the simplifying assumption (3.1.2). Let p be a rational prime. Let*

$$\begin{aligned} & \frac{u + \theta}{p^i} \quad (u \in Z), \\ & \frac{r + s\theta + \theta^2}{p^j} \quad (r, s \in Z) \text{ and} \\ & \frac{x + y\theta + z\theta^2 + \theta^3}{p^k} \quad (x, y, z \in Z) \end{aligned}$$

be p -integral elements of K having the integers i, j and k as large as possible. Then

$$\left\{ 1, \frac{u + \theta}{p^i}, \frac{r + s\theta + \theta^2}{p^j}, \frac{x + y\theta + z\theta^2 + \theta^3}{p^k} \right\} \quad (3.1.29)$$

is a p -integral basis of K , and

$$\nu_p(d(K)) = s_p - 2(i + j + k). \quad (3.1.30)$$

As $\nu_p(d(K)) \geq 0$ for every prime p , we see from (3.1.30) that

$$i + j + k \leq s_p/2.$$

Hence if $s_p = 0$ or 1 we have $i = j = k = 0$, and if $s_p = 2$ or 3 we have $(i, j, k) = (0, 0, 0), (1, 0, 0), (0, 1, 0)$ or $(0, 0, 1)$. Use will be made of these simple remarks in Sections 3.2, 3.3 and 3.4.

3.2 2-Integral Basis of a Quartic Field

In this section we calculate a 2-integral basis for the quartic field K except in the case $a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$ where some partial results are obtained.

Theorem 3.2.1 *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^4 + ax + b ; a, b \in Z,$$

where a and b satisfy the simplifying assumption (3.1.2). Then a 2-integral basis of K is given in the following table. (Note that the notation $a \equiv b \pmod{m}$ has been shortened to $a \equiv b(m)$ in the table.)

Case	Condition	2-integral basis	s_2	$\nu_2(d(K))$
F1	$\nu_2(a) = 0$	$\{1, \theta, \theta^2, \theta^3\}$	0	0
F2	$\nu_2(a) = 1$ and $b \equiv 3(4)$	$\{1, \theta, \theta^2, \theta^3\}$	4	4
F3	$\nu_2(a) = 1$ and $b \equiv 1(4)$	$\{1, \theta, \theta^2, (1 + \theta + \theta^2 + \theta^3)/2\}$	4	2
F4	$\nu_2(a) = 1$ and $\nu_2(b) = 1$	$\{1, \theta, \theta^2, \theta^3\}$	4	4
F5	$\nu_2(a) = 1$ and $\nu_2(b) \geq 2$	$\{1, \theta, \theta^2, \theta^3/2\}$	4	2
F6	$\nu_2(a) = 2$ and $\nu_2(b) = 1$	$\{1, \theta, \theta^2, \theta^3\}$	8	8
F7	$\nu_2(a) = 2$ and $\nu_2(b) = 2$	$\{1, \theta, \theta^2/2, \theta^3/2\}$	8	4
F8	$\nu_2(a) = 2$ and $\nu_2(b) \geq 3$	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	8	2
F9	$\nu_2(a) \geq 3$ and $b \equiv 1(4)$	$\{1, \theta, \theta^2, \theta^3\}$	8	8
F10	$\nu_2(a) \geq 3$ and $b \equiv 3(4)$	$\{1, \theta, \theta^2, (\theta + \theta^2)/2\}$	8	6
F11	$\nu_2(a) \geq 3$ and $\nu_2(b) = 1$	$\{1, \theta, \theta^2, \theta^3\}$	11	11
F12	$\nu_2(a) = 3$ and $\nu_2(b) = 2$	$\{1, \theta, \theta^2/2, (2\theta + \theta^3)/2^2\}$	12	6
F13	$\nu_2(a) \geq 4$ and $b \equiv 4(16)$	$\{1, \theta, (2 + 2\theta + \theta^2)/2^2, (2\theta + \theta^3)/2^2\}$	14	6
F14	$\nu_2(a) \geq 4$ and $b \equiv 12(16)$	$\{1, \theta, (2 + \theta^2)/2^2, (2\theta + \theta^3)/2^2\}$	14	6
F15	$\nu_2(a) = 3$ and $\nu_2(b) = 3$	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	12	6
F16	$\nu_2(a) = 4$ and $\nu_2(b) = 3$	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	16	10
F17	$\nu_2(a) \geq 5$ and $\nu_2(b) = 3$	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	17	11
F18	$\nu_2(a) = 2$ and $b \equiv 1(4)$	$\{1, \theta, \theta^2, \theta^3\}$	9	9
F19	$\nu_2(a) = 2$ and $b \equiv 7(8)$	$\{1, \theta, (1 + \theta^2)/2, (\theta + \theta^3)/2\}$	10	6
F20	$a \equiv 4(8)$, $b \equiv 3(8)$ and $s_2 \equiv 1(2)$	First three basis elements are $\{1, \theta, (1 + \theta^2)/2\}$	≥ 11	3 or 5
F21	$a \equiv 4(8)$, $b \equiv 3(8)$ and $s_2 \equiv 0(2)$	First three basis elements are $\{1, \theta, (1 + \theta^2)/2\}$	≥ 12	≤ 6

Table F

Proof: The following flowchart shows that F1–F21 comprise all cases.

Recall that

$$\Delta = 2^8 b^3 - 3^3 a^4, \quad s_2 = \nu_2(\Delta), \quad \Delta/2^{s_2}. \quad (3.2.1)$$

Case F1 : $a \equiv 1 \pmod{2}$.

By (3.2.1), $s_2 = 0$. Then, by Theorem 3.1.3, we have $\nu_2(d(K)) = 0$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F2 : $\nu_2(a) = 1$ and $b \equiv 3 \pmod{4}$.

By (3.2.1), $s_2 = 4$. We show that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . Without loss of generality we may assume that each of x, y, z is 0 or 1. By Theorem 3.1.1, it is 2-integral if and only if

$$X \equiv 0 \pmod{2}, \quad Y \equiv 0 \pmod{2^2}, \quad Z \equiv 0 \pmod{2^3}, \quad W \equiv 0 \pmod{2^4}.$$

Taking W modulo 2 gives

$$x^4 + by^4 + b^2z^4 + b^3 \equiv 0 \pmod{2}. \quad (3.2.2)$$

If $x = y = 0$ then (3.2.2) gives $z = 1$. Then $Y \equiv 0 \pmod{2^2}$ gives $b \equiv 0 \pmod{2}$, a contradiction.

If $x = 0, y = 1$ then (3.2.2) gives $z = 0$. $Z \equiv 0 \pmod{2^3}$ implies $b + 1 \equiv 0 \pmod{4}$. Then $W \equiv 0 \pmod{2^4}$ implies that $a \equiv 0 \pmod{4}$, a contradiction.

If $x = 1, y = 0$ then (3.2.2) gives that $z = 0$. Then $Z \equiv 0 \pmod{2^3}$ implies that $a \equiv 0 \pmod{4}$, a contradiction.

Note that so far we have not used $b \equiv 3 \pmod{4}$. We have only used $\nu_2(b) = 0$.

If $x = y = 1$ then (3.2.2) gives $z = 1$. Then $W \equiv 0 \pmod{2^4}$ implies that $b \equiv 1 \pmod{4}$, a contradiction. Note that $W \equiv 0 \pmod{2^4}$ is satisfied for $b \equiv 1 \pmod{4}$.

By Theorem 3.1.3 we have $\nu_2(d(K)) = 4$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F3 : $\nu_2(a) = 1$ and $b \equiv 1 \pmod{4}$.

By (3.2.1), $s_2 = 4$. As noted in Case F2, $(1 + \theta + \theta^2 + \theta^3)/2$ is 2-integral. We show that $(x + y\theta + z\theta^2 + \theta^3)/2^2$ is not 2-integral for any triple of integers x, y, z . If it is 2-integral then $X \equiv 0 \pmod{2^2}$ implies that $a \equiv 0 \pmod{4}$, a contradiction. Similarly it can

be shown that $(x + y\theta + \theta^2)/2$ is not 2-integral for any pair of integers x, y . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 2$ and $\{1, \theta, \theta^2, (1 + \theta + \theta^2 + \theta^3)/2\}$ is a 2-integral basis of K .

Case F4 : $\nu_2(a) = 1$ and $\nu_2(b) = 1$.

By (3.2.1), $s_2 = 4$. We show that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . If it is 2-integral then taking W modulo 2 gives that $x = 0$. Taking Z modulo 2^2 gives that $y = 0$. Finally $W \equiv 0 \pmod{2^4}$ implies

$$b^2 z^4 + b^3 - ab^2 z \equiv 0 \pmod{2^4},$$

a contradiction. Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 4$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F5 : $\nu_2(a) = 1$ and $\nu_2(b) \geq 2$.

By (3.2.1), $s_2 = 4$. First let us show that $(x + y\theta + \theta^2)/2$ is not 2-integral for any pair of integers x, y . If it is 2-integral without loss of generality we may assume that $x = 0, 1$ and $y = 0, 1$. Then, by Theorem 3.1.1, we have $6x^2 + 3ay \equiv 0 \pmod{4}$, which implies that $x = 0$ if and only if $y = 0$.

If $x = y = 0$ then $a^2 \equiv 0 \pmod{8}$, a contradiction.

If $x = y = 1$ then $x = 0$, a contradiction.

Secondly, it is easy to show that $\theta^3/2$ is 2-integral, and $(x + y\theta + z\theta^2 + \theta^3)/2^2$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 2$ and $\{1, \theta, \theta^2, \theta^3/2\}$ is a 2-integral basis of K .

Case F6 : $\nu_2(a) = 2$ and $\nu_2(b) = 1$.

By (3.2.1), $s_2 = 8$. We show that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . If it is 2-integral then, by Theorem 3.1.1, we have

$$4x - 3a \equiv 0 \pmod{2},$$

$$6x^2 \equiv 0 \pmod{2^2},$$

$$-ay^3 \equiv 0 \pmod{2^3},$$

$$b^2 z^4 + b^3 \equiv 0 \pmod{2^4},$$

which implies that $x = y = z = 0$ and $2^4 | b^3$, a contradiction. Hence $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis and $\nu_2(d(K)) = 8$.

Case F7 : $\nu_2(a) = 2$ and $\nu_2(b) = 2$.

By (3.2.1), $s_2 = 8$. It is easy to see that $\theta^2/2$ and $\theta^3/2$ are 2-integral. After some calculation we find that $(x + y\theta + z\theta^2 + \theta^3)/2^2$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 4$ and $\{1, \theta, \theta^2/2, \theta^3/2\}$ is a 2-integral basis of K .

Case F8 : $\nu_2(a) = 2$ and $\nu_2(b) \geq 3$.

By (3.2.1), $s_2 = 8$. It is easy to see that $\theta^2/2$ and $\theta^3/2^2$ are 2-integral, and $(x + \theta)/2$ is not 2-integral for any integer x .

Now we show that $(x + y\theta + z\theta^2 + \theta^3)/2^3$ is not 2-integral for any triple of integers x, y, z . If it is 2-integral then in the notation of Theorem 3.1.1, we have $X \equiv 0 \pmod{2^3}$ which implies $x \equiv 1 \pmod{2}$, and $W \equiv 0 \pmod{2^6}$ which implies $x \equiv 0 \pmod{2}$, a contradiction.

Similarly it can be shown that $(x + y\theta + \theta^2)/2^2$ is not 2-integral for any pair of integers x, y . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 2$ and $\{1, \theta, \theta^2/2, \theta^3/2^2\}$ is a 2-integral basis of K .

Case F9 : $\nu_2(a) \geq 3$ and $b \equiv 1 \pmod{4}$. By (3.2.1), $s_2 = 8$. We show that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 2-integral if and only if

$$X \equiv 0 \pmod{2}, Y \equiv 0 \pmod{2^2}, Z \equiv 0 \pmod{2^3}, W \equiv 0 \pmod{2^4}.$$

Then $Y \equiv 0 \pmod{2^2}$ implies that $x \equiv z \pmod{2}$. Without loss of generality we have the following two possibilities:

- i) $x = z = 0$. Then $W \equiv 0 \pmod{2^4}$ gives that $b \equiv 3 \pmod{4}$, a contradiction.
- ii) $x = z = 1$. Then $Z \equiv 0 \pmod{2^3}$ implies that $y = 1$, and $W \equiv 0 \pmod{2^4}$ implies

that $b \equiv 3 \pmod{4}$, a contradiction.

Hence, by Theorem 3.1.3 we have $\nu_2(d(K)) = 8$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F10 : $\nu_2(a) \geq 3$ and $b \equiv 3 \pmod{4}$. By (3.2.1), $s_2 = 8$. It is easy to see that $(\theta + \theta^3)/2$ is 2-integral. After some calculation it can be shown that $(x + y\theta + z\theta^2 + \theta^3)/2^2$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3 we have $\nu_2(d(K)) = 6$ and $\{1, \theta, \theta^2, (\theta + \theta^3)/2\}$ is a 2-integral basis of K .

Case F11 : $\nu_2(a) \geq 3$ and $\nu_2(b) = 1$. By (3.2.1), $s_2 = 11$. It is easy to see that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 11$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F12 : $\nu_2(a) = 3$ and $\nu_2(b) = 2$. By (3.2.1), $s_2 = 12$. It is easy to see that $\theta^2/2$ and $(2\theta + \theta^3)/2^2$ are 2-integral. After a lengthy calculation we find that $(x + y\theta + z\theta^2 + \theta^3)/2^3$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3 we have $\nu_2(d(K)) = 6$ and $\{1, \theta, \theta^2/2, (2\theta + \theta^3)/2^2\}$ is a 2-integral basis of K .

Case F13 : $\nu_2(a) \geq 4$ and $b \equiv 4 \pmod{16}$.

By (3.2.1), $s_2 = 14$. It is easy to see that $(2 + 2\theta + \theta^2)/2^2$ and $(2\theta + \theta^3)/2^2$ are 2-integral. We show that $(x + y\theta + z\theta^2 + \theta^3)/2^3$ is not 2-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 2-integral if and only if

$$X \equiv 0 \pmod{2^3}, Y \equiv 0 \pmod{2^6}, Z \equiv 0 \pmod{2^9}, W \equiv 0 \pmod{2^{12}}.$$

Then $X \equiv 0 \pmod{2^3}$ gives that $x \equiv 0 \pmod{2}$. $W \equiv 0 \pmod{2^{12}}$ implies that $y \equiv 0 \pmod{2}$. So without loss of generality we may assume that $x, y = 0, 2, 4, 6$. We just treat the case $x = y = 0$. The other cases can be done similarly.

If $x = y = 0$ then $Y \equiv 0 \pmod{2^6}$ implies that $z \equiv 0 \pmod{4}$. Then $W \equiv 0 \pmod{2^7}$ gives that $b^3 \equiv 0 \pmod{2^7}$, a contradiction. Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 6$ and $\{1, \theta, (2 + 2\theta + \theta^2)/2^2, (2\theta + \theta^3)/2^2\}$ is a 2-integral basis of K .

Case F14 : $\nu_2(a) \geq 4$ and $b \equiv 12 \pmod{16}$.

By (3.2.1), $s_2 = 14$. It is easy to see that $(2 + \theta^2)/2^2$ and $(2\theta + \theta^3)/2^2$ are 2-integral. As in Case F13 we can show that $(x + y\theta + z\theta^2 + \theta^3)/2^3$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 6$ and $\{1, \theta, (2 + \theta^2)/2^2, (2\theta + \theta^3)/2^2\}$ is a 2-integral basis of K .

Case F15 : $\nu_2(a) = 3$ and $\nu_2(b) = 3$.

By (3.2.1), $s_2 = 12$. It is easy to see that $\theta^2/2$ and $\theta^3/2^2$ are 2-integral. Also after some calculation it can be shown that $(x + y\theta + z\theta^2 + \theta^3)/2^3$ is not 2-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 6$ and $\{1, \theta, \theta^2/2, \theta^3/2^2\}$ is a 2-integral basis of K .

Case F16 : $\nu_2(a) = 4$ and $\nu_2(b) = 3$.

By (3.2.1), $s_2 = 16$. As in Case F15, it can be shown that $\{1, \theta, \theta^2/2, \theta^3/2^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 10$.

Case F17 : $\nu_2(a) \geq 5$ and $\nu_2(b) = 3$.

By (3.2.1), $s_2 = 17$. As in the previous case, it can be shown that $\{1, \theta, \theta^2/2, \theta^3/2^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = 11$.

Case F18 : $\nu_2(a) = 2$ and $b \equiv 1 \pmod{4}$.

By (3.2.1), $s_2 = 9$. We show that $(x + y\theta + z\theta^2 + \theta^3)/2$ is not 2-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 2-integral if and only if

$$X \equiv 0 \pmod{2}, Y \equiv 0 \pmod{2^2}, Z \equiv 0 \pmod{2^3}, W \equiv 0 \pmod{2^4}.$$

Then $Y \equiv 0 \pmod{2^2}$ implies that $x \equiv z \pmod{2}$. $W \equiv 0 \pmod{2}$ implies that $y \equiv 1 \pmod{2}$. Without loss of generality we have the following two possibilities:

- 1) $x = z = 0, y = 1$. Then $W \equiv 0 \pmod{2^4}$ gives $b \equiv 3 \pmod{4}$, a contradiction.
- 2) $x = y = z = 1$. Then $W \equiv 0 \pmod{2^4}$ gives $(b + 1)^3 - a(b + 1)^2 \equiv 0 \pmod{2^4}$, a contradiction.

Hence, by Theorem 3.1.3, we have $\nu_2(d(K)) = 9$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 2-integral basis of K .

Case F19 : $\nu_2(a) = 2$ and $b \equiv 7 \pmod{8}$.

By (3.2.1), $s_2 = 10$. It is easy to see that $(1 + \theta^2)/2$ and $(\theta + \theta^3)/2$ are 2-integral. Now we show that $(x + y\theta + z\theta^2 + \theta^3)/2^2$ is not 2-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 2-integral if and only if

$$X \equiv 0 \pmod{2^2}, Y \equiv 0 \pmod{2^4}, Z \equiv 0 \pmod{2^6}, W \equiv 0 \pmod{2^8}.$$

Then $W \equiv 0 \pmod{2}$ implies that we have the following possibilities:

- 1) $x, y \equiv 0 \pmod{2}$ and $z \equiv 1 \pmod{2}$,
- 2) $x, z \equiv 0 \pmod{2}$ and $y \equiv 1 \pmod{2}$,
- 3) $y, z \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{2}$,
- 4) $x, y, z \equiv 1 \pmod{2}$.

These are all inconsistent with $Y \equiv 0 \pmod{2^4}$. Hence, by Theorem 3.1.3 we have $\nu_2(d(K)) = 6$ and $\{1, \theta, (1 + \theta^2)/2, (\theta + \theta^3)/2\}$ is a 2-integral basis of K .

Case F20–F21 : $a \equiv 4 \pmod{8}$ and $b \equiv 3 \pmod{8}$.

First, by Theorem 3.1.1, it is easy to see that for any integer x the element $(x + \theta)/2$ is not 2-integral. Secondly, $(1 + \theta^2)/2$ is a 2-integral element of K .

Thirdly, we show that for any pair x, y of integers $(x + y\theta + \theta^2)/2^2$ is not a 2-integral element of K .

By Theorem 3.1.1 $(x + y\theta + \theta^2)/2^2$ is a 2-integral element of K if and only if

$$4x \equiv 0 \pmod{2^2},$$

$$6x^2 + 3ay + 2b \equiv 0 \pmod{2^4},$$

$$4x^3 + 4bx + 6axy - ay^3 - 4by^2 + a^2 \equiv 0 \pmod{2^6},$$

$$x^4 + 3ax^2y + 2bx^2 - axy^3 - 4bxy^2 + by^4 + b^2 + a^2x - aby \equiv 0 \pmod{2^8}.$$

The second congruence implies that $x \equiv 1 \pmod{2}$. The fourth congruence taken modulo 2 implies that $y \equiv 0 \pmod{2}$. Then the second congruence gives $b \equiv 1 \pmod{4}$, a contradiction.

Hence, a 2-integral basis of K is of the form

$$\left\{ 1, \theta, \frac{1 + \theta^2}{2}, \frac{x + y\theta + z\theta^2 + \theta^3}{2^n} \right\}$$

where

$$\nu_2(d(K)) = s_2 - 2(n + 1)$$

and

$$n = \frac{s_2 - \nu_2(d(K)) - 2}{2}.$$

We define a positive integer m by

$$m = [(s_2 - 8)/2] \quad (3.2.3)$$

Note that $2^{2m+8} | \Delta$. Define integers x , y and z by

$$4x \equiv 3a \pmod{2^{m+2}}, \quad (3.2.4)$$

$$9a^2y \equiv 16b^2 \pmod{2^{m+4}}, \quad (3.2.5)$$

$$3az \equiv -4b \pmod{2^{m+2}}. \quad (3.2.6)$$

Then, in the notation of Theorem 3.1.2, we have

$$X \equiv 0 \pmod{2^{m+2}}, \quad U \equiv 0 \pmod{2^{m+4}}, \quad V \equiv 0 \pmod{3^{m+2}}.$$

It follows from (3.1.26), (3.1.27) and (3.1.28) that

$$Y \equiv 0 \pmod{3^{2m}}, \quad Z \equiv 0 \pmod{3^{3m}}, \quad W \equiv 0 \pmod{3^{4m}}.$$

Hence, it follows from Theorem 3.1.1 that $(x + y\theta + z\theta^2 + \theta^3)/2^m$ is a 2-integral element of K . Thus, by Theorem 3.1.3,

$$\nu_2(d(K)) \leq 6.$$

Case F20 : $s_2 \equiv 1 \pmod{2}$.

We know that $\nu_2(d(K)) \leq 5$. Now we show that $\nu_2(d(K)) \geq 3$. Let m by $m = (s_2 - 3)/2$.

Note that $2^{2m+3} \parallel \Delta$. It follows from (3.1.26) that

$$2^{2m+7} | 3^3 a^2 X^2 + 2^3 (U + 2bV)V + \Delta. \quad (3.2.7)$$

It follows that

$$2^{2m} \parallel (U + 2bV)V \quad (3.2.8)$$

which implies $2^{m+1} \nmid U$. Let $2^k \parallel U$, where $k \leq m$.

If $2^{m-i} \parallel U$ then either $2^{m+i} \parallel V$ or $2^{m-(i+1)} \parallel V$. It follows from (3.1.27) that $2^{3m-3i+5} \parallel 2^4 U^3$, a contradiction. Hence $m \geq (s_2 - 5)/2$. Then by Theorem 3.1.3, $\nu_2(d(K)) \geq 3$. Thus

$$\nu_2(d(K)) = 3 \text{ or } 5 \quad (3.2.9)$$

Case F21 : $s_2 \equiv 0 \pmod{2}$. We know that $\nu_2(d(K)) \leq 6$.

This completes our consideration of cases F1–F21. ■

3.3 3-Integral Basis of a Quartic Field

In this section we determine a 3-integral basis of a quartic field.

Theorem 3.3.1 *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^4 + ax + b ; a, b \in Z,$$

where a and b satisfy the simplifying assumption (3.1.2). Then a 3-integral basis of K is given in the following table.

Case	Condition	3-integral basis	s_3	$\nu_3(d(K))$
G1	$\nu_3(b) = 0$	$\{1, \theta, \theta^2, \theta^3\}$	0	0
G2	$\nu_3(b) = 1$ and $\nu_3(a) \geq 1$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
G3	$\nu_3(b) = 2, \nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
G4	$\nu_3(b) = 2, \nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3/3\}$	3	1
G5	$\nu_3(b) = 2$ and $\nu_3(a) = 1$	$\{1, \theta, \theta^2, \theta^3/3\}$	6	4
G6	$\nu_3(b) = 2$ and $\nu_3(a) \geq 2$	$\{1, \theta, \theta^2/3, \theta^3/3\}$	6	2
G7	$\nu_3(b) = 3, \nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
G8	$\nu_3(b) = 3, \nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	3	1
G9	$\nu_3(b) = 3$ and $\nu_3(a) = 1$	$\{1, \theta, \theta^2, \theta^3/3\}$	7	5
G10	$\nu_3(b) = 3$ and $\nu_3(a) \geq 2$	$\{1, \theta, \theta^2/3, \theta^3/3^2\}$	9	3

Table G

Case	Condition	3-integral basis	s_3	$\nu_3(d(K))$
G11	$\nu_3(b) \geq 4, \nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
G12	$\nu_3(b) \geq 4, \nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	3	1
G13	$\nu_3(b) \geq 4$ and $\nu_3(a) = 1$	$\{1, \theta, \theta^2, \theta^3/3\}$	7	5
G14	$\nu_3(b) \geq 4$ and $\nu_3(a) = 2$	$\{1, \theta, \theta^2/3, \theta^3/3^2\}$	11	5
G15	$\nu_3(a) = 0$ and $b \equiv 6 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
G16	$\nu_3(a) = 0, b \equiv 3 \pmod{9}$ and $a^4 \not\equiv 4b + 1 \pmod{9}$	$\{1, \theta, \theta^2, \theta^3\}$	4	4
G17	$\nu_3(a) = 0, b \equiv 3 \pmod{9}$ $a^4 \equiv 4b + 1 \pmod{9}$ but $a^4 \not\equiv 4b + 1 \pmod{27}$	$\{1, \theta, \theta^2, \theta^3\}$	5	5
G18	$\nu_3(a) = 0, b \equiv 3 \pmod{9}$ and $a^4 \equiv 4b + 1 \pmod{27}$ $m = [(s_3 - 2)/2]$ $4x \equiv 3a \pmod{3^m}$ $9a^2y \equiv 16b^2 \pmod{3^{m+2}}$ $3az \equiv -4b \pmod{3^{m+1}}$	$\{1, \theta, (a\theta + \theta^2)/3,$ $(x + y\theta + z\theta^2 + \theta^3)/3^m\}$	s_3	$s_3 - 2[s_3/2]$

Table G continued

Proof: The following flowchart shows that G1–G18 comprise all cases.

Recall that

$$\Delta = 2^8 b^3 - 3^3 a^4, \quad s_3 = \Delta/3^{e_3}. \quad (3.3.1)$$

Case G1 : $\nu_3(b) = 0$.

By (3.3.1), $s_3 = 0$. Then, by Theorem 3.1.3, we have $\nu_3(d(K)) = 0$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G2 : $\nu_3(b) = 1$ and $\nu_3(a) \geq 1$.

By (3.3.1), $s_3 = 3$. We show that $(x + y\theta + z\theta^2 + \theta^3)/3$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3}, Y \equiv 0 \pmod{3^2}, Z \equiv 0 \pmod{3^3}, W \equiv 0 \pmod{3^4}.$$

Then $X \equiv 0 \pmod{3}$ gives that $x \equiv 0 \pmod{3}$. $Y \equiv 0 \pmod{3^2}$ implies that $y \equiv 0 \pmod{3}$ if and only if $z \equiv 0 \pmod{3}$. $W \equiv 0 \pmod{3^2}$ implies that $y \equiv z \equiv 0 \pmod{3}$. Using this information on $W \equiv 0 \pmod{3^4}$, we obtain a contradiction. Hence by Theorem 3.1.3, we have $\nu_3(d(K)) = 3$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G3 : $\nu_3(b) = 2$, $\nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. We show that $(x + y\theta + z\theta^2 + \theta^3)/3$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3}, Y \equiv 0 \pmod{3^2}, Z \equiv 0 \pmod{3^3}, W \equiv 0 \pmod{3^4}.$$

Then $X \equiv 0 \pmod{3}$ gives $x \equiv 0 \pmod{3}$. $Y \equiv 0 \pmod{3^2}$ implies that $yz \equiv -a \pmod{3}$. $Z \equiv 0 \pmod{3^2}$ implies that $y \equiv 1 \pmod{3}$, and so $z \equiv -a \pmod{3}$. Then, from $W \equiv 0 \pmod{3^4}$, we obtain $a^2 \equiv 1 \pmod{9}$, a contradiction. Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = 3$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G4 : $\nu_3(b) = 2$, $\nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. It is easy to see that $(\theta - a\theta^2 + \theta^3)/3$ is 3-integral. Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = 1$ and $\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$ is a 3-integral basis of K .

Case G5 : $\nu_3(b) = 2$ and $\nu_3(a) = 1$.

By (3.3.1), $s_3 = 6$. It is easy to see that $\theta^3/3$ is 3-integral. As in Case G9, we obtain $\nu_3(d(K)) = 4$ and $\{1, \theta, \theta^2, \theta^3/3\}$ is a 3-integral basis of K .

Case G6 : $\nu_3(b) = 2$ and $\nu_3(a) \geq 2$.

By (3.3.1), $s_3 = 6$. It is easy to see that $\theta^2/3$ and $\theta^3/3$ are 3-integral. We show that $(x + y\theta + z\theta^2 + \theta^3)/3^2$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3^2}, Y \equiv 0 \pmod{3^4}, Z \equiv 0 \pmod{3^6}, W \equiv 0 \pmod{3^8}$$

Then $X \equiv 0 \pmod{3^2}$ gives that $x \equiv 0 \pmod{9}$. $W \equiv 0 \pmod{3^4}$ gives $y \equiv 0 \pmod{3}$. $Y \equiv 0 \pmod{3^4}$ gives $z \equiv 0 \pmod{3}$ and $y \equiv 0 \pmod{9}$. $Z \equiv 0 \pmod{3^6}$ gives $z \equiv 0 \pmod{9}$. Finally $W \equiv 0 \pmod{3^8}$ gives $b \equiv 0 \pmod{27}$, a contradiction. Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = ?$ and $\{1, \theta, \theta^2/3, \theta^3/3\}$ is a 3-integral basis of K .

Case G7 : $\nu_3(b) = 3$, $\nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. As in Case G3, we have $\nu_3(d(K)) = 3$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G8 : $\nu_3(b) = 3$, $\nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. As in Case G4, we have $\nu_3(d(K)) = 1$ and $\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$ is a 3-integral basis of K .

Case G9 : $\nu_3(b) = 3$ and $\nu_3(a) = 1$.

By (3.3.1), $s_3 = 7$. It is easy to see that $\theta^3/3$ is 3-integral. We show that $(x + y\theta + z\theta^2 + \theta^3)/3^2$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3^2}, Y \equiv 0 \pmod{3^4}, Z \equiv 0 \pmod{3^6}, W \equiv 0 \pmod{3^8}.$$

Then $X \equiv 0 \pmod{3^2}$ gives $x \equiv 0 \pmod{9}$. $Z \equiv 0 \pmod{3^6}$ gives $y \equiv z \equiv 0 \pmod{3}$, and $Y \equiv 0 \pmod{3^4}$ gives $z \not\equiv 0 \pmod{3}$, which is a contradiction.

Similarly it is easy to show that $(x + y\theta + \theta^2)/3$ is not 3-integral for any pair of integers x, y . Hence by Theorem 3.1.3, we have $\nu_3(d(K)) = 5$ and $\{1, \theta, \theta^2, \theta^3/3\}$ is a 3-integral basis of K .

Case G10 : $\nu_3(b) = 3$ and $\nu_3(a) \geq 2$.

By (3.3.1), $s_3 = 9$. It is easy to see that $\theta^2/3$ and $\theta^3/3^2$ are 3-integral. After a lengthy calculation, we obtain $\nu_3(d(K)) = 3$, and $\{1, \theta, \theta^2/3, \theta^3/3^2\}$ is a 3-integral basis of K .

Case G11 : $\nu_3(b) \geq 4$, $\nu_3(a) = 0$ and $a^2 \not\equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. As in Case G3, we have $\nu_3(d(K)) = 3$, and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G12 : $\nu_3(b) \geq 4$, $\nu_3(a) = 0$ and $a^2 \equiv 1 \pmod{9}$.

By (3.3.1), $s_3 = 3$. As in Case G4, we have $\nu_3(d(K)) = 1$, and $\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$ is a 3-integral basis of K .

Case G13 : $\nu_3(b) \geq 4$ and $\nu_3(a) = 1$.

By (3.3.1), $s_3 = 7$. It is easy to see that $\theta^3/3$ is 3-integral. After a lengthy calculation we obtain $\nu_3(d(K)) = 5$, and $\{1, \theta, \theta^2, \theta^3/3\}$ is a 3-integral basis of K .

Case G14 : $\nu_3(b) \geq 4$ and $\nu_3(a) = 2$. By (3.3.1), $s_3 = 11$. It is easy to see that $\theta^2/3$ and $\theta^3/3^2$ are 3-integral. After a lengthy calculation we obtain $\nu_3(d(K)) = 5$, and $\{1, \theta, \theta^2/3, \theta^3/3^2\}$ is a 3-integral basis of K .

Case G15 : $\nu_3(a) = 0$ and $b \equiv 6 \pmod{9}$.

By (3.3.1), we have

$$\begin{aligned}\Delta &= 2^8 b^3 - 27a^4 \\ &= 2^8 b^3 - 27(a^4 - (4b + 1) + (4b + 1)) \\ &= 2^8 b^3 - 27(4b + 1) - 27(a^4 - (4b + 1)).\end{aligned}$$

It is easy to see that

$$\nu_3(2^8 b^3 - 27(4b + 1)) = 3 \text{ and } \nu_3(27(a^4 - (4b + 1))) \geq 4.$$

Hence $s_3 = \nu_3(\Delta) = 3$. We show that $(x + y\theta + z\theta^2 + \theta^3)/3$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3}, Y \equiv 0 \pmod{3^2}, Z \equiv 0 \pmod{3^3}, W \equiv 0 \pmod{3^4}.$$

Then $X \equiv 0 \pmod{3}$ gives that $x \equiv 0 \pmod{3}$. $Y \equiv 0 \pmod{3^2}$ and $W \equiv 0 \pmod{3^2}$ give

$$ayz + 2y + z^2 + a^2 \equiv 0 \pmod{3} \text{ and } 1 - ayz + y \equiv 0 \pmod{3},$$

respectively. Then it follows that $y \equiv 1 \pmod{3}$ and $z \equiv -a \pmod{3}$. So, without loss of generality, we can assume $x = 0, y = 1, z = -a$. Substituting x, y and z into $Z \equiv 0 \pmod{3^3}$ gives $-a(a^2 - 1)^2 + ab(a^2 - (4b + 1)) \equiv 0 \pmod{3^3}$, a contradiction. Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = 3$ and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G16 : $\nu_3(a) = 0$, $b \equiv 3 \pmod{9}$ and $a^4 \not\equiv 4b + 1 \pmod{9}$.

By (3.3.1), we have

$$\begin{aligned} \Delta &= 2^8 b^3 - 27a^4 \\ &= 2^8 b^3 - 27(a^4 - (4b + 1) + (4b + 1)) \\ &= 2^8 b^3 - 27(4b + 1) - 27(a^4 - (4b + 1)). \end{aligned}$$

It is easy to see that

$$\nu_3(2^8 b^3 - 27(4b + 1)) \geq 6 \text{ and } \nu_3(27(a^4 - (4b + 1))) = 4.$$

Hence $s_3 = \nu_3(\Delta) = 4$. Now we show that $(x + y\theta + z\theta^2 + \theta^3)/3$ is not 3-integral for any triple of integers x, y, z . By Theorem 3.1.1, it is 3-integral if and only if

$$X \equiv 0 \pmod{3}, Y \equiv 0 \pmod{3^2}, Z \equiv 0 \pmod{3^3}, W \equiv 0 \pmod{3^4}.$$

$X \equiv 0 \pmod{3}$ implies that $x \equiv 0 \pmod{3}$.

If $y \equiv 0 \pmod{3}$ then $Y \equiv 0 \pmod{3^2}$ gives $z \not\equiv 0 \pmod{3}$.

If $y \not\equiv 0 \pmod{3}$ then $W \equiv 0 \pmod{2^2}$ gives $y - az + 1 \equiv 0 \pmod{3}$. So, without

loss of generality, we have the following four possibilities:

- 1) $x = y = 0, z = a$. Then $W \equiv 0 \pmod{3^4}$ implies $a^2 \equiv 7 \pmod{9}$, which gives $a^4 \equiv 4 \pmod{9}$, a contradiction.
- 2) $x = y = 0, z = -a$. Then $W \equiv 0 \pmod{3^4}$ implies $a^2 \equiv 2 \pmod{3}$, a contradiction.
- 3) $x = 0, y = 1, z = -a$. Then $W \equiv 0 \pmod{3^4}$ implies $a^2 \equiv 4, 7 \pmod{9}$. Since, by hypothesis, $a^4 \equiv 4 \pmod{9}$ cannot occur we must have $a^2 \equiv 4 \pmod{9}$. Substituting it into $W \equiv 0 \pmod{3^4}$ gives a contradiction.
- 4) $x = 0, y = -1, z = 0$. We know that $a^2 \equiv 1, 4 \pmod{9}$. Substituting it into $W \equiv 0 \pmod{3^4}$ gives a contradiction.

Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = 4$, and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G17 : $\nu_3(a) = 0$, $b \equiv 3 \pmod{9}$, $a^4 \equiv 4b + 1 \pmod{9}$ but $a^4 \not\equiv 4b + 1 \pmod{27}$.

By (3.3.1), we have

$$\begin{aligned} \Delta &= 2^8 b^3 - 27a^4 \\ &= 2^8 b^3 - 27(a^4 - (4b + 1) + (4b + 1)) \\ &= 2^8 b^3 - 27(4b + 1) - 27(a^4 - (4b + 1)). \end{aligned}$$

It is easy to see that

$$\nu_3(2^8 b^3 - 27(4b + 1)) \geq 6 \text{ and } \nu_3(27(a^4 - (4b + 1))) = 5.$$

Hence $s_3 = \nu_3(\Delta) = 5$. As in Case G14, after a lengthy calculation it can be shown that $(x + y\theta + z\theta^2 + \theta^3)/3$ is not 3-integral for any triple of integers x, y, z . Hence, by Theorem 3.1.3, we have $\nu_3(d(K)) = 5$, and $\{1, \theta, \theta^2, \theta^3\}$ is a 3-integral basis of K .

Case G18 : $\nu_3(a) = 0$, $b \equiv 3 \pmod{9}$ and $a^4 \equiv 4b + 1 \pmod{27}$.

By (3.3.1), we have

$$\begin{aligned}\Delta &= 2^8 b^3 - 27a^4 \\ &= 2^8 b^3 - 27(a^4 - (4b + 1) + (4b + 1)) \\ &= 2^8 b^3 - 27(4b + 1) - 27(a^4 - (4b + 1)).\end{aligned}$$

It is easy to see that

$$\nu_3(2^8 b^3 - 27(4b + 1)) \geq 6 \text{ and } \nu_3(27(a^4 - (4b + 1))) \geq 6.$$

Hence $s_3 = \nu_3(\Delta) \geq 6$.

First we show that the $(a\theta + \theta^2)/3$ is a 3-integral element of K . By Theorem 3.1.1, the element $(a\theta + \theta^2)/3$ is 3-integral if and only if

$$3a^2 + 2b \equiv 0 \pmod{3^2}, \quad (3.3.2)$$

$$-a^4 - 4ba^2 + a^2 \equiv 0 \pmod{3^3}, \quad (3.3.3)$$

$$ba^4 + b^2 - a^2b \equiv 0 \pmod{3^4}. \quad (3.3.4)$$

The congruence (3.3.2) is obvious. It is easy to see that $a^4 \equiv 4b + 1 \pmod{27}$ if and only if $a^2 \equiv \pm(4b - 1) \pmod{3^3}$. Since $b \equiv 3 \pmod{9}$ then $a^2 \equiv 4b - 1 \pmod{3^3}$ cannot occur. Hence $a^2 \equiv -4b + 1 \pmod{3^3}$, which implies (3.3.3). Further $b \equiv 3 \pmod{9}$ implies (3.3.4). Thus $(a\theta + \theta^2)/3$ is a 3-integral element of K .

As $s_3 \geq 6$ we can define an integer $m \geq 2$ by

$$m = [(s_3 - 2)/2]. \quad (3.3.5)$$

Note that $3^{2m+2} | \Delta$. Define integers x, y, z by

$$4x \equiv 3a \pmod{3^m}, \quad (3.3.6)$$

$$9a^2y \equiv 16b^2 \pmod{3^{m+2}}, \quad (3.3.7)$$

$$3az \equiv -4b \pmod{3^{m+1}}. \quad (3.3.8)$$

Then, in the notation of Theorem 3.1.2, we have

$$X \equiv 0 \pmod{3^m}, U \equiv 0 \pmod{3^{m+2}}, V \equiv 0 \pmod{3^{m+1}}.$$

It follows from (3.1.26), (3.1.27) and (3.1.28) that

$$Y \equiv 0 \pmod{3^{2m}}, Z \equiv 0 \pmod{3^{3m}}, W \equiv 0 \pmod{3^{4m}}.$$

Hence, it follows from Theorem 3.1.1 that $(x + y\theta + z\theta^2 + \theta^3)/3^m$ is a 3-integral element of K . Thus, by Theorem 3.1.3,

$$\left\{1, \theta, \frac{a\theta + \theta^2}{3}, \frac{x + y\theta + z\theta^2 + \theta^3}{3^m}\right\}$$

is a 3-integral basis of K and $\nu_3(d(K)) = s_3 - 2[s_3/2]$.

This completes the proof. ■

3.4 $p(> 3)$ -Integral Basis of a Quartic Field

In this section we determine a $p(> 3)$ -integral basis of a quartic field.

Theorem 3.4.1 *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial*

$$f(x) = x^4 + ax + b ; a, b \in Z,$$

where a and b satisfy the simplifying assumption (3.1.2). Then a $p(> 3)$ -integral basis of K is given in the following table.

Case	Condition	$p(> 3)$ -integral basis	s_p	$\nu_p(d(K))$
H1	$\nu_p(b) = 0, \nu_p(a) \geq 1$ or $\nu_p(b) \geq 1, \nu_p(a) = 0$	$\{1, \theta, \theta^2, \theta^3\}$	0	0
H2	$\nu_p(b) = 1, \nu_p(a) \geq 1$	$\{1, \theta, \theta^2, \theta^3\}$	3	3
H3	$\nu_p(a) = 1, \nu_p(b) \geq 2$	$\{1, \theta, \theta^2, \theta^3/p\}$	4	2
H4	$\nu_p(a) \geq 2, \nu_p(b) = 2$	$\{1, \theta, \theta^2, \theta^3/p\}$	4	2
H5	$\nu_p(a) = 2, \nu_p(b) \geq 3$	$\{1, \theta, \theta^2/p, \theta^3/p^2\}$	8	2
H6	$\nu_p(a) \geq 3, \nu_p(b) = 3$	$\{1, \theta, \theta^2/p, \theta^3/p^2\}$	9	3
H7	$\nu_p(ab) = 0$	$\{1, \theta, \theta^2, (x + y\theta + z\theta^2 + \theta^3)/p^m\}$ $m = [s_p/2]$ $4x \equiv 3a \pmod{p^m}$ $3ay \equiv 16b^2 \pmod{p^m}$ $3az \equiv -4b \pmod{p^m}$	s_p	$s_p - 2[s_p/2]$

Table H

Proof: The following flowchart shows that H1–H7 comprise all cases.

Recall that

$$\Delta = 2^8 b^3 - 3^3 a^4, \quad s_p = \nu_p(\Delta), \quad \text{and} \quad \Delta_p = \Delta/p^{s_p}. \quad (3.4.1)$$

Case H1 : $\nu_p(b) = 0, \nu_p(a) \geq 1$ or $\nu_p(b) \geq 1, \nu_p(a) = 0$.

By (3.4.1), $s_p = 0$. Then, by (3.1.30) $\nu_p(d(K)) = 0$ and $\{1, \theta, \theta^2, \theta^3\}$ is a p -integral basis of K .

Case H2 : $\nu_p(b) = 1, \nu_p(a) \geq 1$.

By (3.4.1) $s_p = 3$. We show that $(x + y\theta + z\theta^2 + \theta^3)/p$ is not p -integral for any triple x, y, z of integers. By Theorem 3.1.1, it is p -integral if and only if

$$X \equiv 0 \pmod{p}, \quad Y \equiv 0 \pmod{p^2}, \quad Z \equiv 0 \pmod{p^3}, \quad W \equiv 0 \pmod{p^4}.$$

Then $X \equiv 0 \pmod{p}$ implies $x \equiv 0 \pmod{p}$. $W \equiv 0 \pmod{p^4}$ implies $y \equiv 0 \pmod{p}$. Then $Y \equiv 0 \pmod{p^2}$ gives $z \equiv 0 \pmod{p}$. Finally substituting x, y and z into $W \equiv 0 \pmod{p^4}$ gives $b^3 \equiv 0 \pmod{p^4}$, a contradiction. Then, by Theorem 3.1.3, $\nu_p(d(K)) = 3$ and $\{1, \theta, \theta^2, \theta^3\}$ is a p -integral basis of K .

Case H3 : $\nu_p(a) = 1, \nu_p(b) \geq 2$.

By (3.4.1) $s_p = 4$. It is easy to see that θ^3/p is p -integral. We show that $(x + y\theta + z\theta^2 + \theta^3)/p^2$ is not p -integral for any triple x, y, z of integers. By Theorem 3.1.1, it is p -integral if and only if

$$X \equiv 0 \pmod{p^2}, \quad Y \equiv 0 \pmod{p^4}, \quad Z \equiv 0 \pmod{p^6}, \quad W \equiv 0 \pmod{p^8}.$$

Then $X \equiv 0 \pmod{p^2}$ implies $\nu_p(x) = 1$. $Y \equiv 0 \pmod{p^4}$ implies that $yz \equiv 0 \pmod{p}$. Then $Z \equiv 0 \pmod{p^6}$ gives that $y \equiv z \equiv 0 \pmod{p}$. Substituting x, y, z into $W \equiv 0 \pmod{p^8}$ implies $x \equiv 0 \pmod{p^2}$, a contradiction. Similarly it can be shown that $(x + y\theta + \theta^2)/p$ is not p -integral for any pair x, y of integers either. Then, by Theorem 3.1.3, $\{1, \theta, \theta^2, \theta^3/p\}$ is a p -integral basis of K and $\nu_p(d(K)) = 2$.

Case H4 : $\nu_p(a) \geq 2, \nu_p(b) = 2$.

By (3.4.1) $s_p = 6$. It is easy to see that θ^2/p and θ^3/p are p -integral elements of K .

We show that $(x + y\theta + z\theta^2 + \theta^3)/p^2$ is not p -integral for any triple x, y, z of integers. By Theorem 3.1.1, it is p -integral if and only if

$$X \equiv 0 \pmod{p^2}, Y \equiv 0 \pmod{p^4}, Z \equiv 0 \pmod{p^6}, W \equiv 0 \pmod{p^8}.$$

Then $X \equiv 0 \pmod{p^2}$ implies that $x \equiv 0 \pmod{p^2}$. $W \equiv 0 \pmod{p^3}$ gives $y \equiv 0 \pmod{p}$. Then $Y \equiv 0 \pmod{p^3}$ gives $z \equiv 0 \pmod{p}$. Again $Y \equiv 0 \pmod{p^4}$ gives $y \equiv 0 \pmod{p^2}$. Then $Z \equiv 0 \pmod{p^6}$ gives $z \equiv 0 \pmod{p^2}$. Finally $W \equiv 0 \pmod{p^8}$ gives $b \equiv 0 \pmod{p^3}$, a contradiction. Similarly it can be shown that $(x + \theta)/p$ is not p -integral for any integer x . Then, by Theorem 3.1.3, $\{1, \theta, \theta^2/p, \theta^3/p\}$ is a p -integral basis of K and $\nu_p(d(K)) = 2$.

Case H5 : $\nu_p(a) = 2, \nu_p(b) \geq 3$.

By (3.4.1) $s_p = 8$. It is easy to see that θ^2/p and θ^3/p^2 are p -integral elements of K . We show that $(x + y\theta + z\theta^2 + \theta^3)/p^3$ is not p -integral for any triple of integers x, y, z . By Theorem 3.1.1, it is p -integral if and only if

$$X \equiv 0 \pmod{p^3}, Y \equiv 0 \pmod{p^6}, Z \equiv 0 \pmod{p^9}, W \equiv 0 \pmod{p^{12}}.$$

Then $X \equiv 0 \pmod{p^3}$ gives that $\nu_p(x) = 2$. $Y \equiv 0 \pmod{p^4}$ gives $yz \equiv 0 \pmod{p}$. Then $Z \equiv 0 \pmod{p^6}$ implies that $z \equiv 0 \pmod{p}$ and $y \equiv 0 \pmod{p^2}$. Using these congruences for x, y and z in $W \equiv 0 \pmod{p^9}$ gives $x \equiv 0 \pmod{p^3}$, a contradiction. Similarly it can be shown that $(x + y\theta + \theta^2)/p^2$ is not p -integral for any pair of integers x, y and $(x + \theta)/p$ is not p -integral for any integer x . Hence, by Theorem 3.1.3, $\{1, \theta, \theta^2/p, \theta^3/p^2\}$ is a p -integral basis of K and $\nu_p(d(K)) = 2$.

Case H6 : $\nu_p(a) \geq 3, \nu_p(b) = 3$.

By (3.4.1) $s_p = 9$. It is easy to see that θ^2/p and θ^3/p^2 are p -integral elements of K . We show that $(x + y\theta + z\theta^2 + \theta^3)/p^3$ is not p -integral for any triple of integers x, y, z . By Theorem 3.1.1, it is p -integral if and only if

$$X \equiv 0 \pmod{p^3}, Y \equiv 0 \pmod{p^6}, Z \equiv 0 \pmod{p^9}, W \equiv 0 \pmod{p^{12}}.$$

Then $X \equiv 0 \pmod{p^3}$ gives that $x \equiv 0 \pmod{p^3}$. $Y \equiv 0 \pmod{p^6}$ implies that $y \equiv 0 \pmod{p}$ if and only if $z \equiv 0 \pmod{p}$. Then $W \equiv 0 \pmod{p^4}$ gives $y \equiv z \equiv 0 \pmod{p}$. $Y \equiv 0 \pmod{p^5}$ gives $y \equiv 0 \pmod{p^2}$. It follows from $Z \equiv 0 \pmod{p^8}$ that $z \equiv 0 \pmod{p^2}$. Then $Y \equiv 0 \pmod{p^6}$ and $Z \equiv 0 \pmod{p^8}$ imply $y \equiv 0 \pmod{p^3}$ and $z \equiv 0 \pmod{p^3}$, respectively. Finally, using these congruences for x, y and z in $W \equiv 0 \pmod{p^{12}}$ gives $b^3 \equiv 0 \pmod{p^{12}}$, a contradiction. Similarly it can be shown that $(x+y\theta+\theta^2)/p^2$ is not p -integral for any pair of integers x, y and $(x+\theta)/p$ is not p -integral for any x . Hence, by Theorem 3.1.3, $\{1, \theta, \theta^2/p, \theta^3/p^2\}$ is a p -integral basis of K and $\nu_p(d(K)) = 3$.

Case H7 : $\nu_p(ab) = 0$.

We define a nonnegative integer m by

$$m = [s_p/2]. \quad (3.4.2)$$

Note that $p^{2m}|\Delta$. Define integers x, y, z by

$$\begin{aligned} 4x &\equiv 3a \pmod{p^m}, \\ 3^2 a^2 y &\equiv 2^4 b^2 \pmod{p^m}, \\ 3az &\equiv -4b \pmod{p^m}. \end{aligned} \quad (3.4.3)$$

Then, in the notation of Theorem 3.1.2, we have

$$\begin{aligned} X &= 4x - 3a \equiv 0 \pmod{p^m}, \\ U &= 3^2 a^2 y - 2^4 b^2 \equiv 0 \pmod{p^m}, \\ V &= 3az + 4b \equiv 0 \pmod{p^m}. \end{aligned}$$

Then it follows that

$$X \equiv 0 \pmod{p^m}, Y \equiv 0 \pmod{p^{2m}}, Z \equiv 0 \pmod{p^{3m}} \text{ and } W \equiv 0 \pmod{p^{4m}}.$$

Thus, by Theorem 3.1.3, $\{1, \theta, \theta^2, (x + y\theta + z\theta^2 + \theta^3)/p^m\}$ is a p -integral basis of K , and $\nu_p(d(K)) = s_p - 2[s_p/2]$.

This completes the treatment of all the cases. ■

3.5 Integral Basis and Discriminant of a Quartic Field

Integral bases for quartic fields can be constructed using Theorem 1.3.2 and Theorem 1.3.5 from the p -integral bases given in Theorem 3.2.1, Theorem 3.3.1 and Theorem 3.4.1 as was done in the case of cubic fields. Consequently the discriminant of K can be determined.

Example : Let $K = \mathbb{Q}(\theta)$ be a quartic field, where θ is a root of the irreducible polynomial

$$f(x) = x^4 + ax + b, \quad a, b \in \mathbb{Z}$$

which is assumed to satisfy the simplifying assumption (3.1.2).

Let us find an integral basis and determine the discriminant corresponding to the Cases F7, G18 and H7. The other cases can be treated similarly.

Case F7 : $\nu_2(a) = 2$ and $\nu_2(b) = 2$.

Case G18 : $\nu_3(a) = 0$, $b \equiv 3 \pmod{9}$ and $a^4 \equiv 4b + 1 \pmod{27}$.

Case H7 : $\nu_p(ab) = 0$.

Define integers x, y, z by

$$x, y, z \equiv 0 \pmod{2},$$

$$4x \equiv 3a \pmod{3^{[(s_3-2)/2]} \prod_{p>3} p^{[s_p/2]}},$$

$$9a^2y \equiv 16b^2 \pmod{3^{[(s_3+2)/2]} \prod_{p>3} p^{[s_p/2]}},$$

$$3az \equiv -4b \pmod{3^{[s_3/2]} \prod_{p>3} p^{[s_p/2]}}. \quad (3.5.1)$$

Let

$$T = 2 \cdot 3^{[(s_3-2)/2]} \prod_{p>3} p^{[s_p/2]}.$$

Then an integral basis of K is

$$\left\{1, \theta, \frac{a\theta + \theta^2}{6}, \frac{x + y\theta + z\theta^2 + \theta^3}{T}\right\},$$

and the discriminant of K is

$$d(K) = 2^4 \prod_{p \neq 2} p^{s_p-2[s_p/2]}.$$

Now let us illustrate this example with numerical values. Consider the quartic field $K = Q(\theta)$, $\theta^4 + 76\theta + 2748 = 0$. Then

$$a = 76, b = 2748, T = 2 \cdot 3^3 \cdot 5 \text{ and } \Delta = 2^8 \cdot 3^8 \cdot 5^2 \cdot 126493.$$

It is easy to see that the conditions of the cases F7, G18 and H7 are satisfied. By solving the system of congruences (3.5.1) we obtain that

$$\left\{1, \theta, \frac{4\theta + \theta^2}{6}, \frac{-78 + 76\theta - 34\theta^2 + \theta^3}{2 \cdot 3^3 \cdot 5}\right\} \quad (3.5.2)$$

is an integral basis of K and $d(K) = 2^4 \cdot 126493$. One can also verify by Theorem 3.1.1 that (3.5.2) is an integral basis of K .

Conclusion

In this thesis the theory of p -integral elements of an algebraic number field was developed. This theory was applied to find explicit p -integral bases, integral bases, and discriminants in the case of cubic and quartic fields. Complete results were obtained except in one subcase in the case of quartic fields. Future work will focus on treating this incomplete case, and on applying the theory to quintic fields given by trinomials.

Bibliography

- [1] A. A. Albert, *The integers of normal quartic fields*, Annals of Math. **31**(1930), 381-418.
- [2] A. A. Albert, *A determination of the integers of all cubic fields*, Annals of Math. **31**(1930), 550-566.
- [3] E. J. Amberg, *Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen*, Diss., Zurich 1897.
- [4] I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. **5**(1973), 37-38.
- [5] I. O. Angell, *A table of totally real cubic fields*, Math. Comp. **30**(1976), 184-187.
- [6] M. Arai, *On Voronoi's theory of cubic fields. I*, Proc. Japan Acad. Ser. A Math. Sci **57**(1981), 226-229.
- [7] H. Bergstrom, *Über die Methode von Woronoj zur Berechnung einer Basis eines kubischen Zahlkörpers*, Arkiv Mat., Astr. Fys., **25B**(1937), 1-8.
- [8] W. E. H. Berwick, *Integral Bases*, Cambridge Tracts in Mathematics and Mathematical Physics No. 22, Cambridge University Press (1927).
- [9] A. Châtelet, *Arithmétique des corps abéliens du troisième degré*, Ann. Sci. École Norm. Sup. (3) **63**(1946), 109-160.

- [10] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag New York Inc., 1978.
- [11] H. Cohn, *Advanced Number Theory*, Dover Publications, Inc., 1980.
- [12] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen*, XI Suppl. to Dirichlet's "Vorlesungen über Zahlentheorie" 2nd ed. (1871), 3rd ed. (1879), 4th ed. (1894). [Gesammelte mathematische Werke, vol. III, 1-314, Vieweg, 1932.]
- [13] R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. **121**(1900), 40-123. [Gesammelte mathematische Werke, vol. II, 148-235, Vieweg, 1931.]
- [14] B. N. Delone, K. K. Billevich, and I. S. Sominskii, *Table of totally real fields of degree 4*, Izv. Akad. Nauk SSSR Ser. Mat. **10**(1935), 1267-1310. (Russian)
- [15] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs, Vol. 10, Amer. Math. Soc., Providence, Rhode Island, U.S.A. (1964).
- [16] H. Edgar and B. Peterson, *Some contributions to the theory of cyclic quartic extensions of the rationals*, J. Number Theory **12**(1980), 77-83.
- [17] K. Girstmair, *Elementare Berechnung von kubischen Diskriminanten*, Arch. Math. (Basel) **32**(1979), no. 4, 341-343.
- [18] H. J. Godwin, *Real quartic fields with small discriminant*, J. London Math. Soc. **31**(1956), 478-485.
- [19] H. J. Godwin, *On totally complex quartic fields with small discriminants*, Proc. Cambridge Philos. Soc. **53**(1957), 1-4.
- [20] H. J. Godwin, *On quartic fields of signature one with small discriminant*, Quart. J. Math. (Oxford), (2) **8**(1957), 214-222.

- [21] H. J. Godwin, *On relations between cubic and quartic fields*, Quart. J. Math. (Oxford), (2) **13**(1962), 206–212. (Corrigendum, Quart. J. Math. (2) **26**(1975), 511–512.)
- [22] H. J. Godwin and P. A. Samet, *A table of real cubic fields*, J. London Math. Soc. **34**(1959), 108–110. (Corrigendum, J. London Math. Soc. (2) **9**(1974/5), 624.)
- [23] D. G. Grebenyuk, *On algebraic numbers depending on a root of an irreducible equation of fourth degree*, Bulletin of University of Central Asia (Tashkent) **2**(1925), 18–43.
- [24] D. G. Grebenyuk, *On the theory of algebraic integers depending on a root of an irreducible equation of fourth degree*, Izv. Akad. Nauk. UzSSR. Ser. Fiz-Mat. (1958), no. 6, 27–47. (Russian, Uzbek summary)
- [25] K. Hardy, R. H. Hudson, D. Richman, K. S. Williams and N. M. Holtz, *Calculation of class numbers of imaginary cyclic quartic fields*, Carleton-Ottawa Mathematical Lecture Note Series No. 7, July 1986, 201pp.
- [26] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsch. Akad. Wiss., **2**(1948), 3–95.
- [27] H. Hasse, *Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York (1980).
- [28] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag New York Inc., 1981.
- [29] J. G. Huard, B. K. Spearman and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory (to appear).
- [30] J. G. Huard, B. K. Spearman and K. S. Williams, *A short proof of the formula for the conductor of a cyclic cubic field*, Preprint 1994.

- [31] R. H. Hudson and K. S. Williams, *The integers of a cyclic quartic field*, Rocky Mountain J. Math. **20**(1990), 145-150.
- [32] G. Kientega and P. Barrucand, *On quartic fields with the symmetric group*, Number Theory, Proc. First Conf. Canad. Number Theory Assoc. Banff Centre, Banff, Alberta, Canada, April 17-27, (1988), pp. 287-295.
- [33] K. Komatsu, *Integral bases in algebraic number fields*, J. Reine Angew. Math. **278/279**(1975), 137-144.
- [34] S. H. Kwon, *Corps de nombres de degré 4 de type alterne*, C. R. Acad. Sci. Paris Ser. A-B, **299**(1984), 41-43.
- [35] S. Lang, *Algebraic Number Theory*, Springer-Verlag New York Inc., 1986.
- [36] Walter Ledermann and Carol Van Der Ploeg, *Integral bases of dihedral number fields*, Bull. Austral. Math. Soc. (Series A) **38**(1985), 351-371.
- [37] E. L. Litver, *A fundamental basis of a composite of quadratic fields*, Rostov Gos. Univ. Uč. Zap. Fiz.-Mat. Fak. **32**(1955), 29-36. (Russian)
- [38] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87**(1983), 579-585.
- [39] P. Llorente, E. Nart and N. Vila, *Discriminant of number fields defined by trinomials*, Acta Arith. **43**(1984), 367-373.
- [40] P. Llorente and A. V. Oneto, *On the real cubic field*, Math. Comp. **39**(1982), 689-692.
- [41] R.L. Long, *Algebraic Number Theory*, Marcel Dekker, Inc., 1977.
- [42] H.B. Mann, *Introduction to Algebraic Number Theory*, Ohio State University Press, Columbus, Ohio (1955).

- [43] D.A. Marcus , *Number Fields*, Springer-Verlag New York Inc., 1977.
- [44] J. Martinet and J. Payan, *Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne*, J. Reine Angew. Math. **228**(1967), 15-37.
- [45] G. B. Mathews, *On the algebraic integers derived from an irreducible cubic equation*, Proc. London Math. Soc. **24**(1893), 327-336.
- [46] D. Maurer, *A matrix criterion for normal integral bases*, Illinois J. Math. **22**(1978), 672-681.
- [47] Y. Motoda, *On biquadratic fields*, Mem. Fac. Sci. Kyushu Univ. Ser. A **29**(1975), 263-268.
- [48] M. Pohst, *Über biquadratische Zahlkörper gleicher Diskriminante*, Abhand Math. Sem. Hamburg, **43**(1975), 192-197.
- [49] E. A. Sergeev, *An integral basis of algebraic fields*, Mat. Zametki **13**(1973), 229-234.
- [50] R. Smadja, *Sur le groupe des classes des corps de nombres*, C. R. Acad. Sci. Paris Sér. A-B **276**(1973), A1639-A1641.
- [51] B. K. Spearman and K. S. Williams, *The conductor of a cyclic quartic field using Gauss sums*, Preprint 1994.
- [52] B. K. Spearman and K. S. Williams, *The conductor of a cyclic quartic field*, Preprint 1994.
- [53] L. Tornheim, *Minimal basis and inessential discriminant divisors for a cubic field*, Pacific J. Math. **5**(1955), 623-631.
- [54] G. F. Voronoi, *Concerning algebraic integers derivable from a root of an equation of the third degree*, Master's Thesis, St. Petersburg, (1894).

- [55] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York-Heidelberg-Berlin, (1982).
- [56] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Book Company Inc., 1963.
- [57] K. S. Williams, *Integers of biquadratic fields*, *Canad. Math. Bull.* **13**(1970), 519–526.
- [58] Z. Xianke, *Cyclic quartic fields and genus theory of their subfields*, *J. Number Theory* **18**(1984), 350–355.

END

25-05-95

FIN