PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 7, July 1998, Pages 1949–1953
S 0002-9939(98)04422-0

p-INTEGRAL BASES OF A CUBIC FIELD

ŞABAN ALACA

(Communicated by William W. Adams)

Abstract. A p-integral basis of a cubic field K is determined for each rational prime p, and then an integral basis of K and its discriminant $d(K)$ are obtained from its p-integral bases.

1. Introduction

Let $K = Q(\theta)$ be an algebraic number field of degree n, and let O_K denote the ring of integral elements of K. If $O_K = \alpha_1 Z + \alpha_2 Z + \cdots + \alpha_n Z$, then $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is said to be an integral basis of K. For each prime ideal P and each nonzero ideal A of K, $\nu_P(A)$ denotes the exponent of P in the prime ideal decomposition of A.

Let P be a prime ideal of K, let p be a rational prime, and let $\alpha \in K$. If $\nu_P(\alpha) \geq 0$, then α is called a P-integral element of K. If α is P-integral for each prime ideal P of K such that $P | pO_K$, then α is called a p-integral element of K. Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ 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 is given as $\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$, where the a_i are p-integral elements of Q, then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is called a p-integral basis of K.

In Theorem 2.1 a p-integral basis of a cubic field K is determined for every rational prime p, and in Theorem 2.2 an integral basis of K is obtained from its p-integral bases.

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

$$x^3 - ax + b = 0, \qquad a, b \in Z \text{ with } \nu_p(a) < 2 \text{ or } \nu_p(b) < 3; \tag{1.1}$$

see [2, p. 579]. The discriminant of θ is $\Delta = 4a^3 - 27b^2$ and $\Delta = i(\theta)^2 d(K)$, where $d(K)$ denotes the discriminant of K, and $i(\theta)$ is the index of θ. For each rational prime p, set $s_p = \nu_p(\Delta)$ and $\Delta_p = \Delta / p^{s_p}$.

The following three theorems are the special cases for $n = 3$ of Theorem 2.1, Theorem 3.1 and Theorem 3.3, respectively, given in [1].

Theorem 1.1. *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial* (1.1). *Let p be a rational prime, and let $\alpha = (x + y\theta + \theta^2)/p^m$, where*

Received by the editors December 26, 1996.
1991 *Mathematics Subject Classification.* Primary 11R16, 11R29.
Key words and phrases. Cubic field, p-integral basis, integral basis, discriminant.

$x, y, m \in Z$, $m \geq 0$. Set

$$\begin{aligned} X &= 3x + 2a, \\ Y &= 3x^2 + 4ax - ay^2 + 3by + a^2, \\ Z &= x^3 + 2ax^2 - axy^2 + 3bxy + a^2x - by^3 + aby + b^2. \end{aligned}$$

Then α is a p-integral if and only if

$$X \equiv 0 (\mathrm{mod}\, p^m), \qquad Y \equiv 0 (\mathrm{mod}\, p^{2m}), \qquad Z \equiv 0 (\mathrm{mod}\, p^{3m}).$$

Theorem 1.2. *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial* (1.1)*. Let p be a rational prime, and let*

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

be p-integral in K with the integers i and j as large as possible. Then

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

is a p-integral basis of K, and

$$\nu_p(d(K)) = \nu_p(\Delta) - 2(i + j).$$

Theorem 1.3. *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial* (1.1)*. If there are no rational primes dividing $i(\theta)$, then $\{1, \theta, \theta^2\}$ is an integral basis of K. Let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing $i(\theta)$. Let*

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

be a p_r-integral basis of K $(r = 1, 2, \ldots, s)$ as given in Theorem 1.2*. Define the integers $X_i^{(j)}$ $(i = 0, 1, \ldots, j-1, j = 1, 2)$ by*

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

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

$$\left\{ 1, \frac{X_0^{(1)} + \theta}{T_1}, \frac{X_0^{(2)} + X_1^{(2)}\theta + \theta^2}{T_2} \right\}.$$

2. p-integral bases of a cubic field

Theorem 2.1. *Let $K = Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial* (1.1)*. Then a 2-integral basis, a 3-integral basis, and a $p(> 3)$-integral basis of K are given in Table* A*, Table* B*, and Table* C*, respectively. (Note that the notation $a \equiv b (\mathrm{mod}\, m)$ has been shortened to $a \equiv b(m)$ in the tables.)*

Proof. The ideas of the proof are illustrated in one case for each table.

A: $a \equiv 1 (\mathrm{mod}\, 4)$ and $b \equiv 2 (\mathrm{mod}\, 4)$. By Theorem 1.1, $(x + y\theta + \theta^2)/2$ is not a 2-integral element of K for any pair of integers x, y. Thus by Theorem 1.2, $\{1, \theta, \theta^2\}$ is a 2-integral basis of K and $\nu_2(d(K)) = s_2 = 3$.

B: $a \equiv 3 (\mathrm{mod}\, 9)$, $\nu_3(b) = 0, b^2 \equiv 4 (\mathrm{mod}\, 9)$, $b^2 \not\equiv a + 1 (\mathrm{mod}\, 27)$. Then $s_3 = \nu_3(\Delta) = 5$. By Theorem 1.1, $(x + \theta)/3$ is not a 3-integral element of K for any rational integer x, and $(1 - b\theta + \theta^2)/3$ is a 3-integral element of K. One can also see that $(x + y\theta + \theta^2)/3^2$ is not a 3-integral element of K for any pair of integers

TABLE A

Condition	2-integral basis	s_2	$\nu_2(d(K))$
$b \equiv 1(2)$	$\{1, \theta, \theta^2\}$	0	0
$a \equiv 0(2), b \equiv 2(4)$	$\{1, \theta, \theta^2\}$	2	2
$a \equiv 0(2), b \equiv 4(8)$	$\{1, \theta, \theta^2/2\}$	4	4
$a \equiv 2(4), b \equiv 0(8)$	$\{1, \theta, \theta^2/2\}$	5	3
$a \equiv 1(4), b \equiv 0(4)$	$\{1, \theta, (\theta + \theta^2)/2\}$	2	0
$a \equiv 3(4), b \equiv 0(4)$	$\{1, \theta, \theta^2\}$	2	2
$a \equiv 1(4), b \equiv 2(4)$	$\{1, \theta, \theta^2\}$	3	3
$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 1(2)$	$\{1, \theta, (x + y\theta + \theta^2)/2^m\}$ $m = (s_2 - 3)/2$ $3x \equiv -2a(2^m)$ $ay \equiv 3(b/2)(2^m)$	$s_2 \geq 5$ $s_2 \equiv 1(2)$	3
$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 0(2)$ $\Delta_2 \equiv 3(4)$	$\{1, \theta, (x + y\theta + \theta^2)/2^m\}$ $m = (s_2 - 2)/2$ $3x \equiv -2a(2^m)$ $ay \equiv 3(b/2)(2^m)$	$s_2 \geq 4$ $s_2 \equiv 0(2)$	2
$a \equiv 3(4)$ $b \equiv 2(4)$ $s_2 \equiv 0(2)$ $\Delta_2 \equiv 1(4)$	$\{1, \theta, (x + y\theta + \theta^2)/2^{m+1}\}$ $m = (s_2 - 2)/2$ $3x \equiv -2a(2^{m+1})$ $ay \equiv 3(b/2) + 2^m(2^{m+1})$	$s_2 \geq 4$ $s_2 \equiv 0(2)$	0

TABLE B

Condition	3-integral basis	s_3	$\nu_3(d(K))$
$\nu_3(a) = 0$	$\{1, \theta, \theta^2\}$	0	0
$\nu_3(a) = \nu_3(b) = 1$	$\{1, \theta, \theta^2\}$	3	3
$1 = \nu_3(b) < \nu_3(a)$	$\{1, \theta, \theta^2\}$	5	5
$2 = \nu_3(b) = \nu_3(a)$	$\{1, \theta, \theta^2/3\}$	6	4
$2 = \nu_3(b) < \nu_3(a)$	$\{1, \theta, \theta^2/3\}$	7	5
$1 = \nu_3(a) < \nu_3(b)$	$\{1, \theta, \theta^2/3\}$	3	1
$\nu_3(b) = 0, \nu_3(a) \geq 1$ $a \not\equiv 3(9)$ $b^2 \equiv a + 1(9)$	$\{1, \theta, (1 - b\theta + \theta^2)/3\}$	3	1
$\nu_3(b) = 0, \nu_3(a) \geq 1$ $a \not\equiv 3(9)$ $b^2 \not\equiv a + 1(9)$	$\{1, \theta, \theta^2\}$	3	3
$\nu_3(b) = 0$ $a \equiv 3(9)$ $b^2 \equiv 4(9)$ $b^2 \not\equiv a + 1(27)$	$\{1, \theta, (1 - b\theta + \theta^2)/3\}$	5	3
$\nu_3(b) = 0$ $a \equiv 3(9)$ $b^2 \not\equiv 4(9)$	$\{1, \theta, \theta^2\}$	4	4
$\nu_3(b) = 0$ $a \equiv 3(9)$ $b^2 \equiv a + 1(27)$	$\{1, (b + \theta)/3,$ $(x + y\theta + \theta^2)/3^m\}$ $m = [(s_3 - 2)/2]$ $x \equiv (-2a/3)(3^m)$ $2ay \equiv 3b(3^{m+2})$	$s_3 \geq 6$	$s_3 - 2[s_3/2]$

TABLE C

Condition	$p(>3)$-integral basis	s_p	$\nu_p(d(K))$
$\nu_p(a)=0, \nu_p(b)\geq 1$ or $\nu_p(a)\geq 1, \nu_p(b)=0$	$\{1,\theta,\theta^2\}$	0	0
$1=\nu_p(b)\leq \nu_p(a)$	$\{1,\theta,\theta^2\}$	2	2
$2=\nu_p(b)\leq \nu_p(a)$	$\{1,\theta,\theta^2/p\}$	4	2
$1=\nu_p(a)<\nu_p(b)$	$\{1,\theta,\theta^2/p\}$	3	1
$\nu_p(a)=\nu_p(b)=0$	$\{1,\theta,(x+y\theta+\theta^2)/p^m\}$ $m=[s_p/2]$, $3x\equiv -2a(p^m)$, $2ay\equiv 3b(p^m)$	$s_p\geq 0$	$s_p-2[s_p/2]$

x, y. Thus, by Theorem 1.2, $\{1,\theta,(1-b\theta+\theta^2)/3\}$ is a 3-integral basis of K and $\nu_3(d(K))=3$.

C: $\nu_p(a)=\nu_p(b)=0$. Set $U=9by-2a^2$ and $V=2ay-3b$. Then $Y=(2^2a^2X^2-U^2-3\Delta y^2)/2^2 3a^2$ and $Z=(2^2a^3X^3-3aXU^2-3^2a\Delta Xy^2-3U^3-3^2\Delta Uy^2+2a\Delta U+3^3bV^3+23^2b\Delta V-\Delta^2)/2^2 3^3 a^3$.

Let $m=[s_p/2]$. Define integers x and y by $3x\equiv -2a(\operatorname{mod} p^m)$ and $2ay\equiv 3b(\operatorname{mod} p^m)$, respectively. Note that $p^{2m}|\Delta$. Then

$$3bU=(4a^3-\Delta)y-6a^2b\equiv 0(\operatorname{mod} p^m).$$

So, $U\equiv 0(\operatorname{mod} p^m)$. Hence, $X\equiv 0(\operatorname{mod} p^m)$, $Y\equiv 0(\operatorname{mod} p^{2m})$, and $Z\equiv 0(\operatorname{mod} p^{3m})$. Thus, by Theorem 1.1, $(x+y\theta+\theta^2)/p^m$ is a p-integral element of K. Therefore, by Theorem 1.2, $\{1,\theta,(x+y\theta+\theta^2)/p^m\}$ is a p-integral basis of K, and $\nu_p(d(K))=s_p-2[s_p/2]$. □

Remark 2.1. Note that for any rational prime p, a p-integral basis of K is given in the form $\{1,\theta,(R_p+S_p\theta+\theta^2)/p^{T_p}\}$ except in the case

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

when a 3-integral basis is of the form $\{1,(b+\theta)/3,(R_3+S_3\theta+\theta^2)/3^{T_3}\}$. Furthermore, for only finitely many rational primes p, T_p is nonzero.

Remark 2.2. The discriminant of a cubic field given in [2, Theorem 2] follows from Theorem 2.1.

The following theorem follows from Theorem 1.3 and Theorem 2.1.

Theorem 2.2. *Let $K=Q(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial* (1.1). *For every rational prime p, set R_p, S_p and T_p as in Remark* 2.1. *Let R and S be integers such that for all primes p*

$$R\equiv R_p(\operatorname{mod} p^{T_p})\quad \textit{and}\quad S\equiv S_p(\operatorname{mod} p^{T_p}).$$

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

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

when an integral basis is

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

3. Examples

Example 3.1. Let $K = Q(\theta)$, where $\theta^3 - \theta + 4 = 0$. Here $a = 1$ and $b = 4$. Then $\Delta = -2^2 \cdot 107$. Hence $s_2 = 2$, $s_{107} = 1$ and $s_p = 0$ for every rational prime $p \neq 2, 107$. So $R_2 = 0, S_2 = 1$ and $T_2 = 1$. Therefore $R = 0, S = 1$ and $T = 2$. Hence $\{1, \theta, (\theta + \theta^2)/2\}$ is an integral basis of K and $d(K) = -107$.

Example 3.2. Let $K = Q(\theta)$, where $\theta^3 - 255\theta + 3850 = 0$. Here $a = 255$ and $b = 3850$. Then $\Delta = -2^4 \cdot 3^6 \cdot 5^3 \cdot 229$. So, $R_2 = 2, S_2 = -1, T_2 = 1, R_3 = 1, S_3 = 2, T_3 = 2, R_5 = 0, S_5 = 0$, and $T_5 = 1$. Therefore $R = 10, S = -25$, and $T = 90$. Hence $\{1, (3850 + \theta)/3, (10 - 25\theta + \theta^2)/90\}$ is an integral basis of K, and $d(K) = -2^2 \cdot 5 \cdot 229$.

Example 3.3. Let $K = Q(\beta)$, where $\beta^3 - \beta^2 - 82\beta + 311 = 0$. Set $\theta = 3\beta - 1$. Then $K = Q(\beta) = Q(\theta)$, and $\theta^3 - 741\theta + 7657 = 0$. Hence, $\Delta = 3^6 \cdot 13^2 \cdot 19^2$. Then $R_3 = 1, S_3 = 2$, and $T_3 = 2$. Therefore, R, S, and T can be taken as $R = 1, S = 1$ and $T = 3^2$. Hence

$$\{1, (1+\theta)/3, (1 + 2\theta + \theta^2)/3^2\} = \{1, \beta, \beta^2\}$$

is an integral basis of K, and $d(K) = 13^2 \cdot 19^2$.

References

1. Ş. Alaca, *p-Integral Bases of Algebraic Number Fields*, submitted for publication.
2. 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. MR **84d:**12003

Centre for Research in Algebra and Number Theory, Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6

E-mail address: salaca@math.carleton.ca