

Integral Bases of Cubic Fields

A.Rameshkumar¹, D.Nagarajan²

Head, Department of Mathematics, Srimad Andavan Arts & Science College (Autonomous), Trichy, Tamilnadu,
India¹

Asst. Professor, Department of Mathematics, Srimad Andavan Arts & Science College (Autonomous), Trichy,
Tamilnadu, India²

ABSTRACT: We study on the discriminant and integral basis of the cubic field of the form $Q(\theta)$, where θ is a root of $\theta^3+a\theta^2+b=0$ ($a,b \in Q$). If K is a field extension of the rational numbers Q of degree $[K:Q] = 3$, then K is called a cubic field.

KEYWORDS: Integral Basis, cubic Field.

I. INTRODUCTION

The Propose of this paper is to describe few subjects concerned with integral bases of Cubic Fields. Any such field is isomorphic to a field of the form $Q[x]/f(x)$, where f is an irreducible cubic polynomial with coefficients in Q . If f has three real roots, then K is called a totally real cubic field. If f has a non-real root, then K is called a complex cubic field.

In Frazer Jarvis^[1], any cubic field F is of the form $F=Q(\theta)$ for some number θ that is a zero of the irreducible polynomial $g(X)=X^3+aX^2+b$ with a,b in Z . In section 2, we find a integral basis of the cubic field. In Cohen and Henri^[4], A field K is a number field if it is a finite extension of Q . The degree of K is the degree of the field extension $[K:Q]$. $Q(i)$ is a number field. A basis of the Principal ideal of the ring O_K of integers of a number field K generated by 1, is an integral basis for K . Suppose that K is a number field of degree n over Q . There are n embeddings $\sigma_1, \dots, \sigma_n$ from K into C . Assume that $\{\omega_1, \dots, \omega_n\}$ lie in K . Consider the matrix

$$\begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{pmatrix}$$

The discriminant of $\{\omega_1, \dots, \omega_n\}$ to be $\Delta\{\omega_1, \dots, \omega_n\}=(det M)^2$. If K is an number field of degree n and α is an element of K then there are two quantities associated with α , namely

$$\sigma_1(\alpha)+\sigma_2(\alpha)+\dots+\sigma_n(\alpha) \text{ and} \\ \sigma_1(\alpha)\sigma_2(\alpha)\dots\sigma_n(\alpha)$$

where $\sigma_k: K \rightarrow C, k=1,2,\dots,n$ are the n distinct monomorphisms from K to C . These quantities are the trace and norm of α respectively. The Integral basis for a number field E of degree m is a set $A = a_1, a_2, \dots, a_m$ of m algebraic integer in E such that every element of the ring of integer O_E of E .

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Let t be a cube-free integer. t is of the form $t = hk^2$, where h is square-free. Therefore k is square-free and $(h,k)=1$. Let $\theta = t^{1/3}$ and let E be the pure cubic field $Q(\theta)$. As $x^3 - t$ is irreducible polynomial of θ , we have $c = 0, d = -t$ and $\Delta = 4c^3 - 27d^2 = -27(-t)^2 = -27t^2$

An integral basis of E is

$$\begin{cases} \left\{ 1, \theta, \frac{\theta^2}{k} \right\} & , \text{if } t^2 \not\equiv 1 \pmod{9} \\ \left\{ 1, \theta, \frac{(k^2 \pm k^2\theta + \theta^2)}{3k} \right\} & , \text{if } t^2 \equiv \pm 1 \pmod{9} \end{cases}$$

The discriminant of E is

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

II. RELATED WORK

If E is a pure cubic field given in the form $E = Q(\theta), \theta^3 + c\theta + d = 0, c, d \in Z$ it is known that $-4c^3 - 27d^2 = -3p^2$ for some positive integer p and an integral basis for E has been given by Spearman and Williams^[2].

III. INTEGRAL BASES OF CUBIC FIELDS

Theorem 3.1

Let θ be a root of the cubic equation $x^3 + ax^2 + b = 0 (a, b \in Q)$. Then $y_0 + y_1\theta + y_2\theta^2 (y_0, y_1, y_2 \in Q)$ is a root of the cubic equation

$$x^3 + Ax^2 + Bx + C,$$

where $A = 3y_0 - ay_1 + a^2y_2; B = 3y_0^2 + 2aby_2^2 - 2ay_0y_1 + 2a^2y_0y_2 + 3by_0y_1y_2;$
 $C = y_0^3 - by_1^3 - b^2y_2^3 + 2aby_0y_2^2 - ay_0^2y_1 + a^2y_0^2y_2 + aby_1^2y_2 + 3by_0y_1y_2$

Proof

Let $\theta, \theta', \theta'' \in C$ be the three roots of the cubic equation $x^3 + ax^2 + b = 0$ So that $\theta + \theta' + \theta'' = -a, \theta\theta' + \theta'\theta'' + \theta\theta'' = 0, \theta\theta'\theta'' = -b.$

$$\begin{aligned} \text{Then } \theta^2 + \theta'^2 + \theta''^2 &= (\theta + \theta' + \theta'')^2 - 2(\theta\theta' + \theta'\theta'' + \theta\theta'') \\ &= a^2, \theta^2\theta'^2 + \theta'^2\theta''^2 + \theta''^2\theta^2 \\ &= (\theta\theta' + \theta'\theta'' + \theta\theta'')^2 - 2\theta\theta'\theta''(\theta + \theta' + \theta'') \\ &= 2ab, \theta\theta'^2 + \theta^2\theta'\theta'' + \theta^2\theta''^2 + \theta\theta''^2 + \theta'^2\theta'' \\ &= (\theta + \theta')\theta\theta' + (\theta + \theta'')\theta\theta'' + (\theta' + \theta'')\theta'\theta'' \\ &= -\theta\theta'\theta'' - \theta\theta'\theta'' - \theta\theta'\theta'' \\ &= 3b \end{aligned}$$

Now Assume that

$$\alpha = y_0 + y_1\theta + y_2\theta^2; \alpha' = y_0 + y_1\theta' + y_2\theta'^2; \alpha'' = y_0 + y_1\theta'' + y_2\theta''^2$$

Then

$$\alpha + \alpha' + \alpha'' = 3y_0 - ay_1 + a^2y_2$$

$$\alpha\alpha' + \alpha'\alpha'' + \alpha\alpha'' = 3y_0^2 + 2aby_2^2 - 2ay_0y_1 + 2a^2y_0y_2 + 3by_1y_2$$

and

$$\alpha\alpha'\alpha'' = y_0^3 + y_1^3\theta\theta'\theta'' + y_2^3\theta\theta'\theta''^2 + y_0y_1^2(\theta\theta' + \theta'\theta'' + \theta\theta'')$$

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

$$\begin{aligned}
 &+ y_0 y_2^2 (\theta^2 \theta'^2 + \theta'^2 \theta''^2 + \theta''^2 \theta^2) + y_0^2 y_1 (\theta + \theta' + \theta'') \\
 &+ y_0^2 y_2 (\theta^2 + \theta'^2 + \theta''^2) + y_1^2 y_2 \theta \theta' \theta'' (\theta + \theta' + \theta'') \\
 &+ y_1 y_2^2 \theta \theta' \theta'' (\theta + \theta' + \theta'') \\
 &+ y_0 y_1 y_2 (\theta \theta'^2 + \theta'^2 \theta'' + \theta \theta''^2 + \theta''^2 \theta' + \theta \theta' \theta'' + \theta'^2 \theta'') \\
 &= y_0^3 - b y_1^3 - b^2 y_2^3 + 2 a b y_0 y_2^2 - a y_0^2 y_1 + a^2 y_0^2 y_2 + a b y_1^2 y_2 + 3 b y_0 y_1 y_2
 \end{aligned}$$

The result now follows as $y_0 + y_1 \theta + y_2 \theta^2$ is a root of

$$(x - \alpha)(x - \alpha')(x - \alpha'') = x^3 - (\alpha + \alpha' + \alpha'')x^2 + (\alpha \alpha' + \alpha \alpha'' + \alpha' \alpha'')x - \alpha \alpha' \alpha''.$$

Example 3.1

Let θ be a root of $\theta^3 - 3\theta^2 + 27 = 0$. We have $a = -3, b = 27, y_0 = 0, y_1 = 1/3, y_2 = 0$. Then, we find $A = 0, B = 0, C = -1$ and $\theta/3$ is a root of $x^3 - 1 = 0$.

This shows that $\theta/3$ is an algebraic integer of $Q(\theta)$.

Example 3.2

Let θ be a root of $\theta^3 - 3\theta^2 + 27 = 0$. We have $a = -3, b = 27, y_0 = 0, y_1 = 0, y_2 = 1/3$. Then, we find $A = 3, B = -18, C = -27$ and $\theta^2/3$ is a root of $x^3 + 3x^2 - 18x - 27 = 0$. This shows that $\theta^2/3$ is an algebraic integer of $Q(\theta)$.

Theorem 3.2

Let a, b be integers such that $x^3 + ax^2 + b \in \mathbb{Z}[x]$ is irreducible. Let $\theta \in \mathbb{C}$ be a root of $x^3 + ax^2 + b$ so that $F = Q(\theta)$ is a cubic field and $\theta \in \mathcal{O}_F$. Then $D(\theta) = -4ba^3 - 27b^2$.

Proof

Let $f(x) = \text{irr}_Q(\theta) = x^3 + ax^2 + b$. Let $\theta_1, \theta_2, \theta_3$ be the conjugates of θ over Q , so that $(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 + ax^2 + b$. We find that $\theta + \theta' + \theta'' = -a, \theta \theta' + \theta' \theta'' + \theta \theta'' = 0, \theta \theta' \theta'' = -b$.

Now $f(x) = 3x^2 + 2ax$, so that $f'(\theta_1)f'(\theta_2)f'(\theta_3) = 27b^2 + 4ba = 3$.

Hence we find that $D(\theta) = (-1)^3 f'(\theta_1)f'(\theta_2)f'(\theta_3) = -4a^3b - 27b^2$.

Example 3.3

Let $F = Q(\theta), \theta^3 - 3\theta^2 + 27 = 0$. The polynomial $x^3 - 3x^2 + 27 \in \mathbb{Z}[x]$ is irreducible, so F is a cubic field. We compute $D(\theta) = -3^6 \cdot 2$.

In Saban Alaca [3], let d_1 be the denominator of a minimal integer in θ of degree 1. We see that $d_1^{2(3-1)} | D(\theta)$. That is, $d_1^4 | -3^6 \cdot 2$. So that $d_1 = 1$ or 3. $\theta/3$ is an integer of F . So we must have $d_1 = 3$ and $\theta/3$ is a minimal integer in θ of degree 2. We have $d_2^{2(3-2)} | D(\theta)$. that is, $d_2^2 | -3^6 \cdot 2$. So that $d_2 = 1$ or 3. $\theta^2/3$ is an integer of F . Hence $\theta^2/3$ is a minimal integer in θ of degree 2. $\{1, (\theta/3), ((\theta^2)/3)\}$ is an integral basis for F .

IV. CONCLUSION

We conclude that we found the discriminant and the integral bases of the cubic field. Integral bases is essential concept in algebraic number theory. The study of the number of cubic fields whose discriminant is less than a given bound is a current area of research. We can develop our further research of finding normal and power integral bases of the cubic field. We can improve the result for the cyclic cubic field.

REFERENCES

- [1] Frazer Jarvis, "Algebraic number Theory", Springer International Publishing Switzerland, 2014.
- [2] Alaca, S., and Kenneth Williams, S., "Introductory Algebraic Number Theory". Cambridge University Press, 2004.
- [3] Alaca, S., "p-integral bases of algebraic number fields", Ph.D. Thesis, Carleton University, Ottawa, Ontario, Canada, 1994.
- [4] Cohen, Henri, "A course in Computational Algebraic Number Theory", Graduate Texts in Mathematics, Berlin, New York, Springer - Verlag, 1996.