Libyan Journal of Science & Technology 6:1 (2017) 51–53

Faculty of Science - University of Benghazi

Libyan Journal of Science & Technology

(Formerly known as Journal of Science & It's Applications)

journal home page: www.sc.uob.edu.ly/pages/page/77

Quadratic Algebraic Integers

Hassan .S. Ali

Department of Mathematics, Faculty of Education, University of Benghazi, Ghemines.

E–mail address: Hassansamor1972@gmail.com

ARTICLE INFO

Article history:
Received 15 September 2017
Revised 04 November 2017
Accepted 08 November 2017
Available online 30 December 2017

Keywords:
Algebraic Integers, Integral Domain, Quadratic Algebraic Integers.

ABSTRACT

Certain the map from the set of all Quadratic Algebraic Integers into $S = \left\{\begin{pmatrix} a & b \\ Db & a \end{pmatrix} : a, b \in \mathbb{Z}\right\}$ is proved a ring isomorphism.

1. Introduction

Definition1.1: (Fraleigh, J.B., 1994) A complex number α is called an algebraic number if is satisfies some polynomial equation $f(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$ where $f(x) \in \mathbb{Q}[x]$

Definition1.2: (Fraleigh, J.B., 1994) An algebraic number α is an algebraic integer if it satisfies some manic polynomial equation

$$f(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0$$

with integer coefficients

Definition1.3: (Fraleigh, J.B., 1994) If α satisfies some polynomial equation of degree n, but none of lower degree we say that α is an algebraic integer of degree n.

Theorem 1.4: (Niven, I., Zuckerman, H.S., Mantgmery, H.L., 1991) The set of all algebraic numbers is a field.

Theorem 1.5: (Niven, I., Zuckerman, H.S., Mantgmery, H.L., 1991) The set of all algebraic integers is an integral domain

2. Preliminaries

The field discussed in the theorem 1.5 contains all algebraic numbers. An algebraic number field is any subfield of this field. For example, if α is an algebraic number, it can be verified that

$\mathbb{Q}(\alpha) = \left\{\frac{f(\alpha)}{h(\alpha)} : h(\alpha) \neq 0; f, g \in \mathbb{Z}[x]\right\}$ constitutes a field.

Example 2.6: $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \;:\; a, b, c \in \mathbb{Q}\}$.
Let α satisfy the polynomial equation:

$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_0, a_1, \ldots, a_n$ are integers, not all zero and n is minimum. If n=1, then α is rational and

$$\mathbb{Q}(\alpha) = \mathbb{Q}.$$

If n=2, we say that α is a "quadratic", then α is a root of quadratic equation:

$$a_0x^2 + a_1x + a_2 = 0 \qquad (1)$$

and thus $\alpha = \frac{a+b\sqrt{m}}{c}$ for some integers a, b, c, m *with* $c \neq 0$, *m is a square*-free and $(a, b, c) = 1$

$\frac{f(\sqrt{m})}{h(\sqrt{m})} = \frac{t+u\sqrt{m}}{v+w\sqrt{m}} = \frac{(t+u\sqrt{m})(v-w\sqrt{m})}{v^2-w^2m} = \frac{a+b\sqrt{m}}{c} = \alpha \;;\; t, u \in \mathbb{Q}$

Therefore, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}) = \{t + u\sqrt{m} \;:\; t, u \in \mathbb{Q}\}$

$\mathbb{Q}(\alpha)$ is called a quadratic field. Since m is a square-free then every element of $\mathbb{Q}(\sqrt{m})$ may be written uniquely in the form

$t + u\sqrt{m}$, where t and u are rationals.

Now if a_0=1 in the quadratic equation (1) then α is called a quadratic algebraic integer.

$$\because\; \alpha = \frac{a + b\sqrt{m}}{c}$$

$$\therefore\; c\alpha = a + b\sqrt{m}\,.(c\alpha - a)^2 = b^2m.$$

$$\frac{c^2}{c^2}\alpha^2 - \frac{2ac}{c^2}\alpha + \frac{a^2 - b^2m}{c^2} = 0$$

Since α is an algebraic integer, then $c|2a$ and

$$c^2|(a^2 - b^2m) \qquad (2)$$

If $(a, c) > 1$ and $c|2a$, then a and c have some common prime factor, say p , and p does not divide b since $(a, b, c) = 1$.

Then $p^2|a^2$ *and* $p^2|c^2$ *Therefore* $p^2|(a^2 - mb^2)$ (from (2))

Therefore, $a^2 - b^2m = qp^2$ for some q $\in \mathbb{Z}$

Therefore, $a^2 - qp^2 = mb^2$. But $p^2|(a^2 - qp^2)$.

Therefore, $p^2|mb^2$ and p does not divide b.

Therefore, $p^2|m$, which is impossible , since m is a square-free .

Therefore, (2) is true only if $(a, c) = 1$.

If $c|2a$, then c=1 or 2, i.e (2) is true iff c=1 or 2.

C=2 iff $a^2 - b^2m = 4q$ for some $q \epsilon \mathbb{Z}$ (from (2)) iff $b^2m \equiv a^2(\text{mod}4)$, and we also have a odd since $(a,c) = 1$ iff $b^2m \equiv a^2 \equiv 1\ (mod4)$, which requires that b be odd iff $b^2m \equiv 1(mod4)$ and $b^2 \equiv 1(mod4)$, iff $b^2m \equiv b^2(mod4)$, $(b^2,4) = 1$ iff $m \equiv 1(mod4)$.

$$\alpha = \frac{a+b\sqrt{m}}{2} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{m}}{2}\right) = a' + b\left(\frac{1+\sqrt{m}}{2}\right)$$

$(a' \in \mathbb{Z}, since\ a, b\ odd)$, where $a', b \in \mathbb{Z}\ iff\ m \equiv 1(mod4)$.

If $m \not\equiv 1(mod4)$ then $c \neq 2$ and hence then $m \equiv 2\ or\ 3\ (mod\ 4)$ and $c = 1$. Therefore if $m \equiv 2\ or\ 3\ (mod\ 4)$, then $c = 1$ and $\alpha = a + b\sqrt{m}$, $a, b\ \epsilon\ \mathbb{Z}$. Thus we have the following:

Theorem 2.7: (Dummit, D.S, Foote, R.M., 1999) The set of all Quadratic Algebraic Integers is given as follows:

$$A_m = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if} \quad m \equiv 2\ or\ 3\ (mod\ 4) \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right] & \text{if} \quad m \equiv 1\ (mod\ 4) \end{cases}$$

Where m is a square-free integers.

Theorem 1.7: (Dummit, D.S, Foote, R.M., 1999) A_m is a subdomain of the quadratic field $\mathbb{Q}(\sqrt{m})$. A_m is called a Quadratic Algebraic Integers (ring)

3. Main result

Theorem3.8: Let m be a square-free integer. Then

$$A_m \cong \left\{\begin{pmatrix} a & b \\ mb & a \end{pmatrix} : a, b \in \mathbb{Z}\right\} \text{ if } m \equiv 2, 3\ (mod\ 4),$$

and

$$A_m \cong \left\{\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a+b \end{pmatrix} : a, b \in \mathbb{Z}\right\} \text{ if } m \equiv 1\ (mod\ 4) \text{ as rings}$$

Proof:

Let $S_1 = \left\{\begin{pmatrix} a & b \\ mb & a \end{pmatrix} : a, b \in \mathbb{Z}\right\}$ and

$$S_2 = \left\{\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a+b \end{pmatrix} : a, b \in \mathbb{Z}\right\}$$

First, we will show that S_1 and S_2 are subrings of $M_2(\mathbb{Z})$, the ring of all 2×2 matrices over $\mathbb{Z}$.

Let $\begin{pmatrix} a & b \\ mb & a \end{pmatrix}, \begin{pmatrix} c & d \\ md & c \end{pmatrix} \in S_1$

$$\begin{pmatrix} a & b \\ mb & a \end{pmatrix} - \begin{pmatrix} c & d \\ md & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ m(b-d) & a-c \end{pmatrix} \in S_1$$

$$\begin{pmatrix} a & b \\ mb & a \end{pmatrix} - \begin{pmatrix} c & d \\ md & c \end{pmatrix} = \begin{pmatrix} ac+mbd & ad+bc \\ m(bc+ad) & mbd-ac \end{pmatrix} \in S_1$$

Therefore, S_1 is a subring of $M_2(\mathbb{Z})$.

Let

$$\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a+b \end{pmatrix}, \quad \begin{pmatrix} c & d \\ \frac{(m-1)d}{4} & c+d \end{pmatrix} \in S_2$$

$$\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a+b \end{pmatrix} - \begin{pmatrix} c & d \\ \frac{(m-1)d}{4} & c+d \end{pmatrix} =$$

$$\begin{pmatrix} a-c & b-d \\ \frac{(m-1)(b-d)}{4} & (a-c)+(b-d) \end{pmatrix} \in S_2$$

$$\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & (a+b) \end{pmatrix}\begin{pmatrix} c & d \\ \frac{(m-1)d}{4} & c+d \end{pmatrix} =$$

$$\begin{pmatrix} ac + \frac{(m-1)bd}{4} & ad+b(c+d) \\ \frac{(m-1)(bc+(a+b)d)}{4} & \frac{(m-1)bd}{4} + (a+b)(c+d) \end{pmatrix}$$

$$= \begin{pmatrix} ac + \frac{(m-1)bd}{4} & ad+bc+bd \\ \frac{(m-1)(bc+ad+bd)}{4} & ac + \frac{(m-1)bd}{4} + (ad+bc+bd) \end{pmatrix} \in S_2$$

Therefore, S_2 is a subring of $M_2(\mathbb{Z})$.

Second, we will define two maps as follows:

$\phi_1 : \mathbb{Z}[\sqrt{m}] \to S_1$ define by:

$\phi_1(a+b\sqrt{m}) = \begin{pmatrix} a & b \\ mb & a \end{pmatrix}$ where

$A_m = \mathbb{Z}[\sqrt{m}]$ $when\ m \equiv 2\ or\ 3\ (mod\ 4)$

$\phi_2 : \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \to S_2$ define by:

$\phi_2\left(a + b\frac{1+\sqrt{m}}{2}\right) = \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a+b \end{pmatrix}$ where

$A_m = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ when $m \equiv 1\ (mod\ 4)$ and we will show that ϕ_1 and ϕ_2 are isomorphism.

Let $a + b\sqrt{m}$, $c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$.

It is clear that

$$\phi_1\left((a+b\sqrt{m}) + (c+d\sqrt{m})\right) = \phi_1(a+b\sqrt{m}) + \phi_1(c+d\sqrt{m})$$

$$\phi_1\left((a+b\sqrt{m}) + (c+d\sqrt{m})\right) = \phi_1(ac+bdm) + (ad+bc)\sqrt{m})$$

$$= \begin{pmatrix} ac+bdm & ad+bc \\ m(ad+bc) & ac+bdm \end{pmatrix} = \begin{pmatrix} a & b \\ mb & a \end{pmatrix}\begin{pmatrix} c & d \\ mb & c \end{pmatrix}$$

$$= \phi_1(a+b\sqrt{m})\phi_1(c+d\sqrt{m})$$

Therefore, ϕ_1 is a ring homomorphism.

Let $\phi_1(a+b\sqrt{m}) = \phi_1(c+d\sqrt{m})$

Therefore, $\begin{pmatrix} a & b \\ mb & a \end{pmatrix} = \begin{pmatrix} c & d \\ md & c \end{pmatrix}$

Therefore, $a = c, b = d$

Therefore, $a + b\sqrt{m} = c + d\sqrt{m}$. Therefore, ϕ_1 is 1-1.

Let $\begin{pmatrix} a & b \\ mb & a \end{pmatrix} \in S_1$. Take $a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$.

$\phi_1(a+b\sqrt{m}) = \begin{pmatrix} a & b \\ mb & a \end{pmatrix}$.

Therefore, ϕ_1 is onto. Hence, ϕ_1 is an isomorphism.

Let

$$a + b\frac{1+\sqrt{m}}{2}\ ,\ c + d\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$

It is clear that:

$$\phi_2\left(\left(a + b\frac{1+\sqrt{m}}{2}\right) + \left(c + d\frac{1+\sqrt{m}}{2}\right)\right)$$

$$= \phi_2\left(a + b\frac{1+\sqrt{m}}{2}\right) + \phi_2\left(c + d\frac{1+\sqrt{m}}{2}\right)$$

$$\phi_2\left(\left(a + b\frac{1+\sqrt{m}}{2}\right)\left(c + d\frac{1+\sqrt{m}}{2}\right)\right)$$

$$= \phi_2\left(ac + \frac{m-1}{4}bd + \frac{1+\sqrt{m}}{2}(bc + ad + bd)\right)$$

$$= \begin{pmatrix} ac + \frac{m-1}{4}bd & bc + ad + bd \\ \frac{m-1}{4}(bc + ad + bd) & ac + \frac{m-1}{4}bd + bc + ad + bd \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix}\begin{pmatrix} c & d \\ \frac{(m-1)d}{4} & c + d \end{pmatrix}$$

$$= \phi_2\left(a + b\frac{1+\sqrt{m}}{2}\right)\phi_2\left(c + d\frac{1+\sqrt{m}}{2}\right)$$

Therefore, ϕ_2 is a ring homomorphism.

Let

$$\phi_2\left(a + b\frac{1+\sqrt{m}}{2}\right) = \phi_2\left(c + d\frac{1+\sqrt{m}}{2}\right)$$

Therefore

$$\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix} = \begin{pmatrix} c & d \\ \frac{(m-1)b}{4} & c + d \end{pmatrix}$$

Therefore,

$$a = c, b = d$$

Therefore,

$$\left(a + b\frac{1+\sqrt{m}}{2}\right) = \left(c + d\frac{1+\sqrt{m}}{2}\right)$$

Thus, ϕ_2 is 1-1.

Let

$$\begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix} \in S_2$$

Take

$$a + b\frac{1+\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$

$$\phi_2\left(a + b\frac{1+\sqrt{m}}{2}\right) = \begin{pmatrix} a & b \\ \frac{(m-1)b}{b} & a + b \end{pmatrix}$$

Therefore, ϕ_2 is onto.

Hence, ϕ_2 is an isomorphism.

References

Dummit, D.S, Foote, R.M. (1999) A abstract algebra Prentice-Hall Newjersey, 249, .pp. 228-231

Fraleigh, J.B., (1994) A first Course In Abstract algebra, Fifth Edition, Addison - wesley, Massachusetts .pp.447-453.

Niven, I., Zuckerman, H.S., Mantgmery, H.L.(1991) An Introduction To The Theory of Numbers , Fifth Edition, John.Wiley, Newyork. pp. 178-189