Quadratic Algebraic Integers

Hassan S. Ali
Department of Mathematics, Faculty of Education, University of Benghazi, Ghenimes.
E-mail address: Hassansamor1972@gmail.com

Abstract

Certain the map from the set of all Quadratic Algebraic Integers into $S = \{(a b \overline{a} a) : a, b \in \mathbb{Z}\}$ is proved a ring isomorphism.

1. Introduction

Definition 1.1: (Fraleigh, J.B., 1994) A complex number $\alpha$ is called an algebraic number if it satisfies some polynomial equation $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ where $f(x) \in \mathbb{Q}[x]$.

Definition 1.2: (Fraleigh, J.B., 1994) An algebraic number $\alpha$ is an algebraic integer if it satisfies some monic polynomial equation $f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0$ with integer coefficients.

Definition 1.3: (Fraleigh, J.B., 1994) If $\alpha$ satisfies some polynomial equation of degree $n$, but none of lower degree we say that $\alpha$ is an algebraic integer of degree $n$.

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

Theorem 1.5: (Niven, I., Zuckerman, H.S., Montgomery, 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 $\mathbb{Q}$ is an algebraic number, it can be verified that $Q(\alpha) = \left\{f(\alpha)h(\alpha) : f, g \in \mathbb{Q}[x]\right\}$ constitutes a field.

Example 2.6: $Q(\sqrt{2}) = \{a + b\sqrt{2} + c\sqrt{4} : a, b, c \in \mathbb{Q}\}$.

Let $\alpha$ 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 $\alpha$ is rational and $Q(\alpha) = \mathbb{Q}$.

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

$$a_0x^2 + a_1x + a_2 = 0$$

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

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

$Q(\alpha)$ is called a quadratic field. Since $m$ is a square-free then every element of $Q(\sqrt{m})$ may be written uniquely in the form $t + u\sqrt{m}$, where $t$ and $u$ are rationales.

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

$$\alpha = a + b\sqrt{m}$$

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

$$c^2a^2 - 2ac + a^2 - b^2m = 0$$

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

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

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, $a^2 - q^2p^2 = m$. But $p^2|(a^2 - q^2p^2)$.

Therefore, $p^2|mb$ 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 $(a, c) = 1$. 

© 2017 University of Benghazi. All rights reserved.
If \( c \mid 2a \), then \( c = 1 \) or \( 2 \), i.e. (2) is true if \( c = 1 \) or 2.

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

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

(\( \alpha' \in \mathbb{Z} \), since \( a \), \( b \) odd), where \( \alpha', \beta \) \( \in \mathbb{Z} \) if \( f \equiv 1(\mod 4) \).

If \( m \equiv 1(\mod 4) \) then \( c = 2 \) 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 \( a = a + b\sqrt{m}, b, a \in \mathbb{Z} \). 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:

\[
A_\mathbb{m} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \text{ (mod 4)} \\ \mathbb{Z}[\frac{1 + \sqrt{m}}{2}] & \text{if } m \equiv 1 \text{ (mod 4)} \end{cases}
\]

Where \( m \) is a square-free integer.

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

### 3. Main result

**Theorem 3.8:** Let \( m \) be a square-free integer. Then \( A_\mathbb{m} \equiv \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \) if \( m \equiv 2, 3 \) (mod 4), and \( A_\mathbb{m} \equiv \left\{ \begin{pmatrix} (m-1)b & b \\ mb & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \) if \( m \equiv 1 \) (mod 4) as rings.

**Proof:**

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

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

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

Let \( \begin{pmatrix} a & b \\ mb & a \end{pmatrix} \), \( \begin{pmatrix} c & d \\ mc & c \end{pmatrix} \) \( \in S_1 \)

\[
\begin{pmatrix} a & b \\ mb & a \end{pmatrix} - \begin{pmatrix} c & d \\ mc & c \end{pmatrix} = \begin{pmatrix} a - c & b - d \\ m(b - d) & a - c \end{pmatrix} \in S_1
\]

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

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

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

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

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

Second, we will define two maps as follows:

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

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

where

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

\[\phi_2 : \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \to S_2 \]

\[
\phi_2(a + b\frac{1+\sqrt{m}}{2}) = \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix}
\]

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

It is clear that

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

\[
\phi_1((a + b\sqrt{m}) + (c + d\sqrt{m})) = \phi_1(ac + bd) + (ad + bc)\sqrt{m}
\]

\[
\begin{pmatrix} a + b \phi_1(m(b + c)) & ad + bc \\ m(ad + bc) & mb + ac \end{pmatrix} = \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix}
\]

Therefore, \( \phi_1 \) is a ring homomorphism.

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

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

Therefore, \( a = c, b = d \)

Therefore, \( a + b\sqrt{m} = c + d\sqrt{m} \). Therefore, \( \phi_1 \) is 1-1.

Let \( \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix} \in S_1 \), Take \( a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \).

\[
\phi_1(a + b\sqrt{m}) = \begin{pmatrix} a & b \\ \frac{(m-1)b}{4} & a + b \end{pmatrix}
\]

Therefore, \( \phi_1 \) is onto. Hence, \( \phi_1 \) is an isomorphism.

Let

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

It is clear that:

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

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

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

\[
= \phi_2 \left( \frac{a + m - 1}{4} bd + \frac{bc + ad + bd}{2} \right)\phi_2 \left( \frac{c + m - 1}{4} bd + \frac{bc + ad + bd}{2} \right)
\]

\[
= \phi_2 \left( \frac{(m-1)b}{4} a + b \right)\phi_2 \left( \frac{(m-1)d}{4} c + d \right)
\]

Therefore, \( \phi_2 \) 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,

\[
\frac{a}{4} + \frac{b}{a+b} = \frac{c}{4} + \frac{d}{c+d}
\]

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, \( \phi_2 \) is 1-1.

Let

\[
\left( \frac{a}{4} + \frac{b}{a+b} \right) \in S_2
\]

Take

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

\[
\phi_2 \left( a + b \frac{1 + \sqrt{m}}{2} \right) = \left( \frac{a}{4} + \frac{b}{a+b} \right)
\]

Therefore, \( \phi_2 \) is onto.

Hence, \( \phi_2 \) is an isomorphism.

References

