The Propositions and Proofs in Algebra System

Shiqing Chen*
School of Economics, Guangzhou College of Commerce, Guangzhou 511363 China

*Corresponding author e-mail: 1040168586@qq.com

Abstract. In the study, it was proved that the algebra system \((a + bp, \oplus, \odot) = \{a + b\sqrt{2} | a, b \in Z\}\) is a Ring of integers and not a domain, and when \(\sqrt{2}\) is extended to the prime number, the conclusion is correct. When \(a\) and \(b\) are Rational number and Real number, it proves that Algebra System \((a + bp, \oplus, \odot) = \{a + b\sqrt{2} | a, b \in Z\}\) is a domain and extends \(\sqrt{2}\) to \(\sqrt{5}\) until \(p\) is the prime number. The conclusion is correct. Finally, the judgment method of Subdomains is used to prove that when \(a\) and \(b\) are plural, \(I = \{a + bi | a, b \in Q\}\) is a domain.

Keywords: Gaussian integer, Ring of integers, Domain, Isomorphism.

1. Introduction
The number like \(a + bi (a, b \in Z, i = \sqrt{-1})\) is called Gaussian integer, which was first proposed by Carl Friedrich Gauss when he studied the Quadratic indeterminate equation. \(Z[i] = \{a + bi | a, b \in Z, i = \sqrt{-1}\}\), it can be proved that the addition and multiplication of numbers in \(Z[i]\) is made into an exchange ring, which we call The Ring of Gaussian Integers. In addition, the situation where The Ring of Gaussian Integers is extended to \(Z[\sqrt{-n}]\) is called the potential of a gaussian ring of The Ring of Gaussian Integers. The Ring of Gaussian Integers is a special ring with a certain representative structure, which occupies an important position in Ring Theory. It not only incorporates the ideas of Ring Theory, but also contains the ideas of number theory. The study of The Ring of Gaussian Integers has always been one of the important topics for scholars. Through years of research, mathematicians have derived many important and meaningful ideas. in conclusion.  

Zhang Liguo (2017)[1] In view of the structural domain problem of Gaussian integer ring \(Z[i]\), discussed the structural characteristics of the ideal \((a+bi)\) of Gaussian integer ring \(Z[i]\), using it to classify the elements of Gaussian integer ring \(Z[i]\), for the purpose of studying the structural domain of Gaussian integer ring \(Z[i]\). The problem provides some new ideas.

Zhang Jingxiao (2011)[2] The non-zero elements in the gaussian integer ring are under the effect of mapping, and two methods for finding the greatest common factor of the elements in \(Z[i]\) are given: Euclidean algorithm and Generalized elementary transformation and its application.

Ou Yanling (2011) [3] applies the prime factor decomposition method to give a necessary and sufficient condition for whether an element in the Gaussian integer ring is a prime factor.
Song Wenqing (2002) [4] gave the prime factor of the gaussian integer ring, the prime element in its integer form is a prime number that can be expressed as $4n+3$, and the non-integer prime element $N(\alpha)$ is in prime form.

The study regards Gaussian integer as a more general form of $(a + bi, a, b \in A)$, where $A$ is a certain set of numbers, and $p$ is a prime element. Several propositions are derived and proved.

2. Basic concepts and theorems

Definition 1 The commutative ring without zero factor is called Ring of integers.

Definition 2 Suppose $R$ is a ring. If $|R| > 1$ and $R$ has identity elements and each non-zero element has an inverse element, it is called a division ring. The interchangeable division ring is called domain.

Definition 3 Let $R$ and $\overline{R}$ be two rings. If there is a $R \to \overline{R}$ mapping $\varphi$ satisfies

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad (\forall a, b \in R)$$

It is said that $\varphi$ is a Group homomorphism from $R$ to $\overline{R}$.

If $\varphi$ is (one variable, linear), then $\varphi$ is (Ring homomorphism, Ring homomorphisms and isomorphisms).

Especially when $\varphi$ is a ring homomorphism, it is called $R$ and $\overline{R}$ homomorphism, which is recorded as $R \sim \overline{R}$.

**Theorem 1** Let $R$ and $\overline{R}$ be a set of two algebraic operations each, and $R \sim \overline{R}$. Then when $R$ is a ring, $\overline{R}$ is also a ring.

**Theorem 2** Let $R$ and $\overline{R}$ be two rings, and $R \sim \overline{R}$. Then the image of the zero element of $R$ is the zero element of $\overline{R}$, and the element of $R$ of the negative element of $a$ is the negative element of the image of $a$; when $R$ is an exchange ring, $\overline{R}$ is also an exchange ring; when $R$ has an identity element, $\overline{R}$ There are also, and the identity of the identity element is the identity element.

**Theorem 3** Let $R$ and $\overline{R}$ be two rings, $R \equiv \overline{R}$. Then $R$ is the Ring of integers (division ring, domain) if and only if $\overline{R}$ is the Ring of integers (division ring, domain).

**Theorem 4** Suppose $F_i$ is a subset of domain $F$, and $|F_i| > 1$, then $F_i$ becomes a subdomain of $F$ if and only if

$$a, b \in F_i \Rightarrow a - b \in F_i,$$

$$a \neq 0, b \in F_i \Rightarrow \frac{b}{a} \in F_i.$$

In short, it is closed to "subtraction and division".

3. Proposition and proof

**Proposition 1**

If $(a + bp, \oplus, e) = \{a + b\sqrt{2} \mid a, b \in Z\}$, then $(a + bp, \oplus, e)$ is made into a unit with identity elements, but it is not a domain. Among them, $\oplus$ is addition, $e$ is multiplication, and $Z$ is ring of integers.

**Proof:**

$I = \{a + b\sqrt{2} \mid a, b \in Z\}$

$Q 0 = 0 + 0\sqrt{2} \in I$, $\therefore I \neq \phi$

(i) $\forall a + b\sqrt{2}, c + d\sqrt{2} \in I,$

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in I.$

(ii) The addition of I is obviously suitable for associative law and commutative law.
(iii) \(0 + 0\sqrt{2} = 0\) is the zero dollar of I
(iv) \(\forall a + b\sqrt{2} \in I, (-a) + (-b)\sqrt{2}\) is its negative element in I.
\(\therefore (I, +)\) constitutes a plus group.
\(\forall a + b\sqrt{2}, c + d\sqrt{2} \in I,\)
\((a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in I.\)
The multiplication of I is obviously suitable for associative law and commutative law.
The multiplication of I is also obviously suitable for the left and right distribution rates of addition.
\(\therefore (I, \cdot, \cdot)\) constitutes an exchange ring.
1 = 1 + 0\sqrt{2} is the identity element of I.
I is a number ring, it has no zero factor.
\(\therefore (I, +, \cdot)\) is a Ring of integers.
Take \(2 = 2 + 0\sqrt{2} \in I, 2 \neq 0\), but 2 has no inverse element in I, so I is not a domain.

Proposition 2
If \((a + bp, \oplus, \cdot) = \{a + bp \mid a, b \in Z\}, \) then \((a + bp, \oplus, \cdot)\) is made into a Ring of integers with identity elements, but it is not a domain. Among them, \(\oplus\) is addition, \(\cdot\) is multiplication, \(Z\) is ring of integers, and \(p\) is any prime number.

Proof:
\(I = \{a + bp \mid a, b \in Z\}\)
\(Q 0 = 0 + 0p \in I, \therefore I \neq \emptyset \)
(i) \(\forall a + bp, c + dp \in I,\)
\((a + bp) + (c + dp) = (a + c) + (b + d)p \in I.\)
(ii) The addition of I is obviously suitable for associative law and commutative law.
(iii) \(0 + 0p = 0\) is the zero dollar of I
(iv) \(\forall a + bp \in I, (-a) + (-b)p\) is its negative element in I.
\(\forall a + bp, c + dp \in I,\)
\((a + bp)(c + dp) = (ac + p^2bd) + (ad + bc)p \in I.\)
Obviously, \(p^2bd\) is an integer.
The multiplication of I is obviously suitable for associative law and commutative law.
The multiplication of I is also obviously suitable for the left and right distribution rates of addition.
\(\therefore (I, +, \cdot, \cdot)\) constitutes an exchange ring.
1 = 1 + 0p is the identity element of I.
I is a number ring, it has no zero factor.
\(\therefore (I, +, \cdot)\) is a Ring of integers.
Take \(2 = 2 + 0p \in I, 2 \neq 0\), but 2 has no inverse element in I, so I is not a domain.

Proposition 3
If \((a + bp, \oplus, \cdot) = \{a + b\sqrt{2} \mid a, b \in Q\}, \) then \((a + bp, \oplus, \cdot)\) becomes a domain. Among them, \(\oplus\) is addition, \(\cdot\) is multiplication, and \(Q\) is the rational number domain.

Proof:
\(I = \{a + b\sqrt{2} \mid a, b \in Q\}\)
\(Q 0 = 0 + 0\sqrt{2} \in I, \therefore I \neq \emptyset \)
(i) \(\forall a + b\sqrt{2}, c + d\sqrt{2} \in I,\)
\((a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in I.\)
(ii) The addition of I is obviously suitable for associative law and commutative law.
(iii) \( 0 + 0\sqrt{2} = 0 \) is the zero dollar of \( I \)
(iv) \( \forall a + b\sqrt{2} \in I, (-a) + (-b)\sqrt{2} \) is its negative element in \( I \).
\[ \therefore (I, +) \text{ constitutes a plus group.} \]
\[ \forall a + b\sqrt{2}, c + d\sqrt{2} \in I, \]
\[ (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in I. \]
The multiplication of \( I \) is obviously suitable for associative law and commutative law.
The multiplication of \( I \) is also obviously suitable for the left and right distribution rates of addition.
\[ \therefore (I, +, \cdot) \text{ constitutes an exchange ring.} \]
\[ 1 = 1 + 0\sqrt{2} \] is the identity element of \( I \).
\( I \) is a number ring, it has no zero factor.
\therefore (\( I, +, \cdot \)) is a Ring of integers.
\[ \forall a + b\sqrt{2} \in I \]
\[ 1 = (a + b\sqrt{2}) \frac{1}{a + b\sqrt{2}} = (a + b\sqrt{2}) \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \]
\[ = (a + b\sqrt{2}) \left[ \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \right] \]
Obviously, \( \frac{a}{a^2 - 2b^2} \) and \( \frac{b}{a^2 - 2b^2} \) are both rational numbers.
Therefore, any element in it has an inverse element.
\therefore (\( I, +, \cdot \)) constitutes a domain.

**Proposition 4**
If \( (a + bp, \oplus, e) = \{a + b\sqrt{2} \mid a, b \in R\} \), then \( (a + bp, \oplus, e) \) becomes a domain. Among them, \( \oplus \) is addition, \( e \) is multiplication, and \( R \) is real domain.

Proof: \( A = \{a + b\sqrt{2} \mid a, b \in Q\} \), \( B = \{a + b\sqrt{2} \mid a, b \in R\} \)
\[ \forall a + b\sqrt{2} \in A, \varphi(a + b\sqrt{2}) = a + b\sqrt{2} \in B \]
Obviously, \( \varphi \) is a linear of \( A \to B \), and it has been proved that \( \varphi \) is an isomorphic bijection.
\[ \forall a + b\sqrt{2}, c + d\sqrt{2} \in A, \]
\[ \varphi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \varphi((a + c) + (b + d)\sqrt{2}) = \]
\[ = (a + c) + (b + d)\sqrt{2} = (a + b\sqrt{2}) + (c + d\sqrt{2}) \]
\[ = \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2}) \]
\[ \varphi((a + b\sqrt{2}) \times (c + d\sqrt{2})) = \varphi((ac + 2bd) + (cb + ad)\sqrt{2}) = \]
\[ = (ac + 2bd) + (cb + ad)\sqrt{2} = (a + b\sqrt{2}) \times (c + d\sqrt{2}) \]
\[ = \varphi(a + b\sqrt{2}) \varphi(c + d\sqrt{2}) \]
Because a rational number must be a real number, \( (ac + 2bd), (cb + ad) \) is a real number.
So \( \varphi \) is the Isomorphism of \( A \to B \), and \( A \) is the domain. From Theorem 3, we know that \( B \) is also the domain.

**Proposition 5**
If \((a + bp, \oplus, e) = \{a + b\sqrt{5} \mid a, b \in R\}\), then \((a + bp, \oplus, e)\) becomes a domain. Among them, \(\oplus\) is addition, \(e\) is multiplication, and \(R\) is real domain.

**Proof:** \(I = \{a + b\sqrt{5} \mid a, b \in R\}\)

1. \(Q 0 = 0 + 0\sqrt{5} \in I, \quad \therefore I \neq \phi\)
2. \(\forall a + b\sqrt{5}, c + d\sqrt{5} \in I,\)
   \((a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (b + d)\sqrt{5} \in I.\)
3. \(0 + 0\sqrt{5} = 0\) is the zero dollar of \(I\)
4. \(\forall a + b\sqrt{5} \in I, (-a) + (-b)\sqrt{5}\) is its negative element in \(I.\)

\(\therefore (I, +)\) constitutes a plus group.

\(\forall a + b\sqrt{5}, c + d\sqrt{5} \in I,\)
\((a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 2bd) + (ad + bc)\sqrt{5} \in I.\)

The multiplication of \(I\) is obviously suitable for associative law and commutative law. The multiplication of \(I\) is also obviously suitable for the left and right distribution rates of addition. \(\therefore (I, +, \cdot)\) constitutes an exchange ring.

\(1 = 1 + 0\sqrt{5}\) is the identity element of \(I.\)

\(I\) is a number ring, it has no zero factor. \(\therefore (I, +, \cdot)\) is a Ring of integers.

\(\forall a + b\sqrt{5} \in I\)
\(1 = (a + b\sqrt{5}) \cdot \frac{1}{a + b\sqrt{5}} = (a + b\sqrt{5}) \cdot \frac{a - b\sqrt{5}}{(a + b\sqrt{5})(a - b\sqrt{5})} = \)
\((a + b\sqrt{5}) \left[ \frac{a}{a^2 - 5b^2} - \frac{b}{a^2 - 5b^2} \sqrt{5} \right].\)

Obviously, \(\frac{a}{a^2 - 5b^2}\) and \(-\frac{b}{a^2 - 5b^2}\) are real numbers,

Therefore, any element in it has an inverse element. \(\therefore (I, +, \cdot)\) constitutes a domain.

**Proposition 6**
If \((a + bp, \oplus, e) = \{a + bp \mid a, b \in R\}\), then \((a + bp, \oplus, e)\) becomes a domain. Among them, \(\oplus\) is addition, \(e\) is multiplication, \(R\) is real domain, and \(p\) is prime.

**Proof:** \(I = \{a + bp \mid a, b \in R\}\)

1. \(Q 0 = 0 + 0p \in I, \quad \therefore I \neq \phi\)
2. \(\forall a + bp, c + dp \in I,\)
   \((a + bp) + (c + dp) = (a + c) + (b + d)p \in I.\)
3. \(0 + 0p = 0\) is the zero dollar of \(I\)
4. \(\forall a + bp \in I, (-a) + (-b)p\) is its negative element in \(I.\)

\(\therefore (I, +)\) constitutes a plus group.

\(\forall a + bp, c + dp \in I,\)
\((a + bp)(c + dp) = (ac + p^2bd) + (ad + bc)p \in I.\)
The multiplication of I is obviously suitable for associative law and commutative law.
The multiplication of I is also obviously suitable for the left and right distribution rates of addition.
\( \therefore (I, +, \cdot) \) constitutes an exchange ring.
I = 1 + 0p is the identity element of I.
I is a number ring, it has no zero element.
\( \therefore (I, +, \cdot) \) is a Ring of integers.
\( \forall a + bp \in I \)
\[
1 = \frac{1}{a + bp} \cdot (a + bp) = \frac{a - bp}{(a + bp)(a - bp)} =
\]
\[
= (a + bp) \left[ \frac{a}{a^2 - p^2b^2} - \frac{b}{a^2 - p^2b^2} p \right]
\]
Obviously, \( \frac{a}{a^2 - p^2b^2} \) and \( \frac{b}{a^2 - p^2b^2} \) are real numbers,
Therefore, any element in I has an inverse element.
\( \therefore (I, +, \cdot) \) constitutes a domain.

Proposition 7
If \( (a + bp, \oplus, e) = \{a + bi \mid a, b \in \mathbb{Q}\} \), then \( (a + bp, \oplus, e) \) becomes a domain. Among them, \( \oplus \)
is addition, \( e \) is multiplication, and \( \mathbb{Q} \) is the rational number domain.

Proof: \( I = \{a + bi \mid a, b \in \mathbb{Q}\} \), obviously I is a non-empty subset of complex domain C.
Q 0 = 0 + 0i \( \in I \),
And 0 is the zero element of I.
\( \forall a + bi \in I, (-a) + (-b)i \) is its negative element in I.
\( (a + bi) + [(-a) + (-b)i] = 0 \in I \), that is, subtraction is closed to I.
Obviously, 1 \( \in I \) is the identity element of I.
\[
\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (cb - ad)i}{c^2 + d^2}
\]
\[
= \left[ \frac{ac + bd}{c^2 + d^2} + \frac{cb - ad}{c^2 + d^2} i \right] \in I
\]
That is, division is closed to I.
According to Theorem 4, we know that I is a subdomain of complex domain C.

4. Conclusion
Regarding the general form of Gaussian integer as \( a + bp(a, b \in A) \), A is a certain number set, and p is
a prime number. Prove that the algebra formula \( (a + bp, \oplus, e) = \{a + \sqrt{p} \mid a, b \in \mathbb{Z}\} \) is a Ring of
integers is not a domain and extend \( \sqrt{p} \) to \( p \) as a prime number, the conclusion is correct.
When a and b are rational numbers and real numbers, it proves that the algebra formula
\( (a + bp, \oplus, e) = \{a + \sqrt{p} \mid a, b \in \mathbb{Z}\} \) is a number field and extends \( \sqrt{p} \) to \( \sqrt{5} \) until p is a prime
number. The conclusion is correct. Finally, it is proved by the subdomain judgment method: when a
and b are complex numbers, \( I = \{a + bi \mid a, b \in \mathbb{Q}\} \) is the domain.
Acknowledgements
This research work was supported by Guangdong Higher Education Teaching Revolution Project: Experiencing Teaching and Mode Design of Cultivation of Internet Finance Talents under the Background of Financial Science Technology, project number: 2018SJJXGG01; Guangzhou College of Commerce Higher Education Teaching Revolution Project: Teaching Reform and Practice of Securities Investment under the Cultivation Method of Applied Talents, project number: 2018XJJXGG01. Foundation projects: Guangdong Undergraduate Higher Education Teaching Quality Engineering project: “Guangzhou College of Commerce -Applied Training Base of Mobile Commerce and E-commerce Logistics”, project number: SJJD201501; Guangdong College Characteristic Innovative Project (humanities and social sciences category): “Virtual Reality Experimental Teaching Center of Guangzhou College of Commerce”, project number: 2015WTSCX114.

References
[1] Liguo. Zhang, Guahuan Z [i] Discussion on the number of alloys Classification, J. Journal of Shenyang Ligong University. Vol.36 No.3 (2017) 98-100
[2] Jing Xiao. Zhang, the greatest common factor and its solution of elements in the Gauss integral ring Z[i], J. Journal of the University of Texas. Vol.27 No.2 (2011) 15-17
[3] Ou Yanling, Discussion on the Necessary and Sufficient Conditions for Discriminating Prime Elements in Gaussian Integer Rings, J. Journal of Higher Correspondence Education (Natural Science Edition). Vol.24 No.1 (2011) 82-84
[4] Wen Qing. Song, Simple Elements of Gaussian Domain, J. University Mathematics. Vol.18 No.1 (2002) 32-34