PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESERACH

Mohamed Boudiaf University of M'sila

Faculty of Mathematics and Informatics

Departement of Mathematics

Master of Mathematics

Domain: Mathematics and Informatics
Specialty: Mathematics
Option: Algebra and Discrete Mathematics

Theme

Gaussian Integers and Applications

Presented by:
MAOUCHE FATIMA

in front of the jury composed of :

TALLAB ABDELHAMID	M.C.A,	University of M'sila	**President**.
LADJELAT LAHCENE	M.A.A,	University of M'sila	**Supervisor**.
KHADRAOUI ABDELMALEK	M.A.A,	Universiy of M'sila	**Examinator** .

University year 2023/2024

CONTENTS

Acknowledgement

First and foremost, i would like to thank "**Allah**" who bless me to finich this work**.**

The prophet Muhammad, may Allah bless him and grant him peace, said, " Allah does not thank the person who does not thank people ".

I am very grateful to my supervisor, **Mr.Lahcene Ladjelat**, for constant support, guidance, helped and encouraged me .

My since thanks to the presedent of the jury, **Mr.Tallab Abdelhamid,** to accept this task and to give interest to my work. Also, my thanks to **Mr.Khadraoui Abdelmalek,** to accept being the examiner of this thesis.

It is important for to thanks my familly: my parents, my husband, my sister may God have mercy on her, and my brothers who have always been an inexhaustible source of encouraguement.

A big thanks to my freinds, my colleagues and all teachers of the mathematics departement for their dedecation and their generosity.

Dedicaces

I dedicate this master's thesis to my beloved parents, whose unwavering support and encouragement have been the cornerstone of my academic journey. Thear love, guidance, and sacrifices have fueled my determination and shaped my success, To my sbling whose camaraderie and understanding have been a source of strength. To my sister, my she rest in peace. To my husband, my partner in life, whose love, support and companionship have been my greatest blessings. To my friends, mentors, and educators, whose wisdom and guidance. And to all those who believe in the power of knowledge and the pursuit of excellence, this thesis is dedicated to you.

Introduction

The Gaussian Integers are complex numbers whose real and imaginary parts are both integers. They form a ring $\mathbb{Z}[i]$ with nice properties: **Euclidean ring** and **Unique factorization domain.**
The Gaussian Integers play important roles in Number Theory, Cryptograph, Geometry of Numbers, and Coding Theory.
The goal of this work is to study some properties of the ring of Gaussian Integers $\mathbb{Z}[i]$: Constructions, Euclidean algorithm, gcd, lcm, unique factorization, irreducible elements,... and mention some of their applications in Number Theory (Sum of squares, Congruences), Geometry (Right triangle with rational angles and edges), and Analysis(Arctangent Identities for π).
This work is divided into three chapters as follow:
CHAPTER ONE, discuses the fundamental algebraic structures, needed to understand, the algebraic concept and structure of the ring of Gaussian Integers: ring, irreducible elements, unit element, Euclidean ring, division in a ring...
This chapter is necessary to understand the following chapters.
CHAPTER TWO is denoted to the study of the ring $\mathbb{Z}[i]$ of Gaussian Integers and its properties: groub of units, irreducible element in $\mathbb{Z}[i]$, Euclidean division (algorithm) in $\mathbb{Z}[i]$, Unique factorization of $\mathbb{Z}[i]$. Also it gives some representations of $\mathbb{Z}[i]$ as a quotient ring modulo polynomials of $\mathbb{Z}[X]$.
This chapter is the core of this work.
CHAPTER THREE is an introduction to some applications of Gaussian Integers in different areas: Number Theory (Sum of squares, Congruences), Geometry (Right triangle with rational angles and edges), and Analysis (Arctangent Identities for π).

CHAPTER1

ALGEBRAIC FOUNDATIONS

1.1 Ring

Definition 1.1 *A ring is a triple $(R, +, .)$ where R is a set, and " $+$ " and " $\cdot$ ", are binary operations on R (called addition and multiplication resbectively) so that :*

(1) $(R, +)$ is an abelian group (with identity denoted by 0 and the inverse of $x \in R$denoted by $-x$)

(2) Multiplication is associative :

for all $x,\ y,\ z \in R$ we have $x + (\ y + z\ ) =\ (\ x + y\ ) +\ z$

(3) The folowing distributive laws hold $\forall\ x,\ y,\ z \in R$:

$$x(y + z) = xy + xz$$

$$(x + y)z = xz\ +\ yz$$

Remark

(1) A ring R is **commutative** if $xy = yx$ for all $x, y \in R$

(2) A ring R is unitary if there exists an unitary element for the mulplication $(\cdot)$

Example 1.1

(1) $(\mathbb{Z}, +, \cdot)$ is a commutative unitary ring
(2) $\mathbb{Z}/n\mathbb{Z} = \{\ \overline{0},\ \overline{1}, ..., \overline{n-1}\ \}$ with $\overline{x} = x + n\mathbb{Z} = \{x + nk : k \in \mathbb{Z}\}$
$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative unitary ring defined by the two following laws:

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x+y} \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y} \end{aligned}$$

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is called the ring of integers modulo n.
(3) Let $\mathbb{Z}[i]$ be the subset of $\mathbb{C}$ defined by:

$$\mathbb{Z}[i] = \{\ \ a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\ \}$$

equiped with the addition and multiplication of complex numbers, the set $\mathbb{Z}[i]$ is a commutative unitary ring called the ring of *Gaussian integers*.

1.2 Subring

Definition 1.2 *A subset S of a ring R is a subring if S is a ring under the same operations as R and the multiplicative identity of S is the same as that of R.*

Example 1.2

(1) $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are a subrings of a ring $(\mathbb{C}, +, \times)$
(2) $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subring of $(\mathbb{Z}, +, .)$ for any $n \in \mathbb{N}$

1.3 Units of a ring

Definition 1.3 *An element $u \in R$ is called a unit if it has a multiplicative inverse: that is, there exists $u' \in R$ such that:*

$$u\ u' = \ u'u = \ 1$$

For a unitary ring R , denote by $U(R) = R^{\times}$ the set

$$U(R) = \{\ u \in R \mid u \text{ is a unit in } R\ \}$$

It is well known that $(U(R), \cdot)$ is a group called the group of unity of R.

1.4 Integral domain

Definition 1.4.1 *Let R be a ring, the zero divisor is an element $s \in R$ such that $s \neq 0$ and there exists an element $r \in R$ with $r \neq 0$, and $rs = 0$.*

for example, $\mathbb{Z}/6\mathbb{Z}$ has three: (2), (3) and (4).

Definition 1.4.2 *R is an integral domain if R contains no zero divisors.*

Definition 1.4.3 *A ring R is an integral domain if $R \neq \{0\}$ and for all $r, s \in R$, if $r\ s = 0$, then either $r = 0$ or $s = 0$*

Example 1.3

1) $\mathbb{Z}$ is an integral domain.
2) In $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ is a zero divisors, then $\mathbb{Z}/6\mathbb{Z}$ is not integral domain.

1.5 Quotient ring

Definition 1.5 *Let R be a ring and I an ideal of R. Then the quotient ring of R by I, denoted R/I is the ring defined by the following binary operation:*

$$(r + I) + (s + I) = (r + s) + I \quad \forall r, s \in R$$

$$(r + I) \times (s + I) = (rs + I) \qquad \forall r, s \in R$$

Example 1.4

K commutative ring
$A = K[x]$ is the polynomial ring in x over K.
Let $f(x) \in K[x]$ of degree $n \geqslant 1$.
$I = (f(x)) = \{\ f(x) \cdot h(x) : h(x) \in K[x]\ \} = f(x) \cdot K[x]$

$I = (f(x))$ is called the ideal generated by $f(x)$
$K[x]/(f(x)) = \{g(x) + (f(x)) : g(x) \in K[x]\ \}$
$K[x]/(f(x)) = \{a_0 + a_1x + ... + a_{n-1}x^{n-1} + I \mid a_i \in K,\ n = \deg(f)\}$

1.5.1 The ring homomorphism

Definition 1.5.1 *Let R and S be rings.*

(1) A ring homomorphism is a map $\varphi : R \to S$ satisfying

(a) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$, and $\varphi(1_R) = 1_S$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$

(2) The kernel of the ring homomorphism φ, denoted $\ker\varphi$, is defined

$$\ker\varphi := \{a \in R : \varphi(a) = 0\}$$

(3) The image of a ring homomorphism φ, denoted $\mathrm{Im}\,\varphi$, is defined

$$\mathrm{Im}\,\varphi := \{\varphi(a) : a \in R\}$$

(4) A bijective ring homomorphism is called an isomorphism.

Example 1.5

Let $R = M_2(\mathbb{R})$ be a commutative unitary ring, and $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad a, b \in \mathbb{R} \right\}$
we define: $f : S \to \mathbb{C}$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a + ib$$

f is a ring isomorphism:

1) f is a ring homomorphism:

Let $x = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $y = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, and $x + y = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}$

we have $f(x) = a + ib$, and $f(y) = c + id$

i)

$$\begin{aligned} f(x+y) &= (a+c)+i(b+d) \\ f(x)+f(y) &= (a+ib)+(c+id) \\ &= (a+c)+i(b+d) \end{aligned}$$

then,

$$f(x+y) = f(x)+f(y)$$

ii)

$$\begin{aligned} f(x\cdot y) &= (ac-bd)+i(ad+bc) \\ f(x)\cdot f(y) &= (a+ib)\cdot(c+id) \\ &= ac+iad+icb-bd \\ &= (ac-bd)+i(ad+cb) \end{aligned}$$

then,

$$f(x\cdot y) = f(x)\cdot f(y)$$

2) f is a bijective:

$$[x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)\ ] \Leftrightarrow f \text{ bijective}$$

Let $x_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \in S$, and $x_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in S$

$$\begin{aligned} f(x_1) &= f(x_2) \Rightarrow a_1+ib_1 = a_2+ib_2 \\ &\Rightarrow a_1 = a_2 \text{ and } b_1 = b_2 \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

Then, f is a ring isomorphism.

1.5.2 The first isomorphism theorem

Theorem 1.5.2 (first isomorphism theorem)

Given any two rings R and S and a ring homomorphism $\varphi : R \longrightarrow S$, we have

- $\operatorname{Im}\varphi$ *is a subring of* S
- $\ker\ \varphi$ *is an ideal of* R
- $R/\ker\varphi \simeq \operatorname{Im}\varphi$

Example 1.6

We consider the application $\varphi : \mathbb{R}[x] \to \mathbb{R}$

$$f(x) \to \varphi(f(x)) = f(0)$$

φ is a surjective homomorphism of a ring
we have $\operatorname{Im}\varphi = \mathbb{R}$ and $\ker\varphi = (x)$
then, according to the first isomorphism theorem

$$\mathbb{R}/(x) \cong \mathbb{R}$$

1.6 Ideals of a ring

Definition 1.6.1 *Let R be a ring. An ideal I of R is a nonempty subset $I \subset R$ such that:*
(1) I is closed under addition: if $a, b \in I$, then $a + b \in I$
(2) The zero element of R is in I: $0 \in I$
(3) I is closed under additive inverses: if $a \in I$, then $-a \in I$
(4) If $r \in R$ and $x \in I$, then $r\ x \in I$ and $x\ r \in I$. In other words, I is closed under multiplication (on either side) by arbitrary ring elements.

Example 1.7

The subset $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$ for $n \in \mathbb{Z}$
we know that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition. So I just need to check closure under multiplication by elements of $\mathbb{Z}$.
Let $k \in \mathbb{Z}$ and let nz, where $x \in \mathbb{Z}$. Then $k \cdot (nz) = n(kz) \in n\mathbb{Z}$
Therefore, $n\mathbb{Z}$ is an ideal.

Definition 1.6.2 *Assume R is a commutative ring. An ideal I is called a prime ideal if $I \neq R$ and for all $a, b \in R$ if $ab \in I$, then $a \in I$ or $b \in I$.*

Example 1.8

(1) The ideal $6\mathbb{Z}$ is not prime in $\mathbb{Z}$ because $(2)(3) \in 6\mathbb{Z}$ but $2 \notin 6\mathbb{Z}$ and $3 \notin 6\mathbb{Z}$
(2) $I = (X^2 + 1)$ is a prime ideal in $\mathbb{Z}[X]$.

Proposition 1.6.3

I is a prime ideal of a commutative ring R,if and only if R/I is an integral domain.

Proof

Suppose that I is a prime ideal and suppose $(a + I)(b + I) = 0 + I$. Then $ab + I = 0 + I$, so $ab \in I$,and so either $a \in I$ or $b \in I$, thus either $a + I = 0 + I$ or $b + I = 0 + I$.

Conversely, Suppose R/I is an integral domain and suppose $ab \in I$. Then $(a+I)(b+I) = ab+I = 0+I$ so either $a+I = 0+I$ or $b+I = 0+I$ and so either $a \in I$ or $b \in I$.

Definition 1.6.4 *A proper ideal I of a commutative ring R is a maximal ideal of R if $I \neq R$* and *whenever J is another ideal with $I \subseteq J \subseteq R$ then $J = I$ or $J = R$.*

Example 1.9

The ideal $6\mathbb{Z}$ is not maximal in $\mathbb{Z}$ because $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Proposition 1.6.5

I is a maximal ideal of a commutative ring R, if and only if R/I is a field.

Proof

Suppose that I is maximal and let $x + I \neq 0 + I$. Consider the set

$$J = \{rx + a \,|r \in R, a \in I\}$$

J is an ideal of R which contains but is larger than I.
Thus $J = R$ and so $1 = r'x + a'$ for some $r' \in I$ and so

$$(r' + I)(x + I) = r'x + I = 1 - a' + I = 1 + I$$

Conversely, suppose R/I is a field and $I \subsetneq J \subseteq R$. Let $b \in J$ with $b \notin I$.
Then $b + I \neq 0 + I$ and so $b + I$ is a unit in R/I and so there is some $c + I$ with $(b + I)(c + I) = 1 + I$.
Thus $bc + I = 1 + I$ and so $1 - bc \in I \subseteq J$. Since $b \in J$ we then have $bc \in J$ (because J is an ideal) and hence $1 \in J$ and so $J = R$.

Corollary 1.6.6

Any *maximal ideal is a prime ideal.*

Definition 1.6.7 *In a ring R, the ideal (S) generated by a subset S is the set of all finite sums of elements of the form $x\ s\ y$, with $s \in S$ and $x, y \in R$. If R a is commutative ring, then (S) is the set of all finite linear combinations of elements of S with coefficients in R.*

1.7 Principal ideal domain

Proposition 1.7 *In a commutative ring R, the principal ideal generated by $a \in R$ is the set $(a) = Ra$ of all multiples of a.*

Definition 1.7 *A principal ideal domain or PID is a domain in which every ideal is principal.*

Example 1.10

1) Any ideal of $\mathbb{Z}$ is a principal.
2) $(4, 6) = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z} \subset (2)$
3) Any comutative field is a *principal ideal domain*

1.7.1 irreductible element

Definition 1.7.1 *An element q of a domain R is irreducible when q is not zero or a unit, and $q = ab$ implies that a is a unit or b is a unit.*

Example 1.11

1) For $A = \mathbb{Z}$, $a = 3$, $U(A) = \{-1, 1\}$
Let $a = bc$, such that $b \in \mathbb{Z}$ and $c \in \mathbb{Z}$

$$\begin{aligned} b &\mid 3 \Rightarrow b = -1, 1, 3, -3 \\ b &= -1, 1 \Rightarrow b \in U(\mathbb{Z}) \\ b &= -3, 3 \Rightarrow c = -1, 1 \Rightarrow c \in U(\mathbb{Z}) \end{aligned}$$

Then, 3 *is irreducible in* $\mathbb{Z}$.

Proposition 1.7.2 *Let K be a field. In the ring $K[x]$* we have:
(1) every polynomial of degree 1 is irreducible;
(2) a polynomial of degree 2 or 3 with no root in K is irreducible;
(3) If $K = \mathbb{C}$, a polynomial is irreducible if and only if it has degree 1.

Example 1.12

Let $A = \mathbb{Q}[x]$ the ring of $\mathbb{Q}[x]$ and $f(x) = x^2 - 3$ a polynomial in $\mathbb{Q}[x]$.
$U(\mathbb{Q}[x]) = U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$
We will show that $f(x)$ is irreducible in $\mathbb{Q}[x]$:

(1) $f \neq 0$ and $f \notin U(\mathbb{Q})$

(2) Assume that $x^2 - 3 = g(x) \cdot h(x)$ with $g,\ h \in \mathbb{Q}[x]$
such that $\deg(f) = \deg(g) + \deg(h)$

if

$$\begin{aligned} x^2 - 3 &= (ax + b)(cx + d),\ a \neq 0, c \neq 0 \\ x^2 - 3 &= acx^2 + (ad + bc)x + bd \end{aligned}$$

$$\left\{ \begin{array}{c} ac = 0 \\ ad + bc = 0 \\ bd = -3 \end{array} \quad a, b, c, d \in \mathbb{Q} \right\}$$ the system is impossiple over $\mathbb{Q}$

The polynomial $x^2 - 3$ is irreducible in $\mathbb{Q}[x]$.

1.7.2 Least common multiple and a greatest common divisor

Let R be a commutative unitary ring.
Let a and b two elements of R.

Definition 1.7.2 *A greatest common divisors of* a and b if it exists, is an element δ in R such that,

$$\{ax + by \mid xy \in R\} = (\delta)$$

Example 1.13

1) Let $A = \mathbb{Z}$, $(4) + (6) = (2)$, $\delta = 2$
2) $A = Q[x]$, $(x^2 - 1) + (x^2 - 2x + 1) = (x - 1)$

Theorem 1.7.2 *In a principal ideal domain R, every $a, b \in R$ have a least common multiple and a greatest common divisor. Moreover, $m = \operatorname{lcm}(a, b)$ if and only if $Rm = Ra \cap Rb$, and $d = \gcd(a, b)$ if and only if $Rd = Ra + Rb$. In particular, $d = \gcd(a, b)$ implies $d = xa + yb$ for some $x, y \in R$.*

1.8 Euclidean domain

Definiton 1.8.1 *The ring A is said to be an Euclidean domain if :*

(1) A is an integral domain
(2) There is a mapping $v : A - \{0\} \to N$ such that for each $a \in R$ and $b \neq 0 \in R, \exists\ q\ r \in R$ such that $a = bq + r$, where either ($r = 0$ or $v(r) \prec v(b)$).

Proposition 1.8.2

Every Euclidean domain is a principal ideal domain .

1.9 Unique factorization domain

Definition 1.9.1 *A unique factorization domain is a domain R in which:*

(1) every element other than 0 and units, is a product of irreducible elements of R
(2) if two products $p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$ of irreducible elements of R are equal, then $m = n$ and the terms can be indexed so that $p_i = q_i$ for all i.

Proposition 1.9.2

Any principal ideal domain is a unique factorization domain.

CAPTER 2

THE RING OF GAUSSIAN INTEGERS

The Gaussian Integers are the set of complex numbers of the forme $a+bi$,where a and b are integers and i is the complex number satisfying $i^2=-1$. The set of all Gaussian Integers are denoted by $\mathbb{Z}[i]$.
i.e.,

$$\mathbb{Z}[i]=\{a+bi \mid a,\ b\in\mathbb{Z}\}.$$

2.1 The Ring of $\mathbb{Z}[i]$

Definition 2.1.1 *$\mathbb{Z}[i]$ is a ring since it is closed under addition and multiplication of complex numbers:*

$$(x+iy)+(p+iq)=(x+p)+i(y+q)$$

$$(x+iy)(p+iq)=(xp-yq)+i(xq+yp)$$

$\cdot$ $\mathbb{Z}[i]$ is a subring of the ring $(\mathbb{C},+,\times)$.

Definition 2.1.2 *The ring $\mathbb{Z}[i]$ is a commutative ring if and only if $\alpha\beta=\beta\alpha$ such that $\alpha=(a+bi)$ and $\beta=(c+di)$, for all $\alpha,\ \beta\in\mathbb{Z}[i]$.*

2.2 The norm

Definition 2.2.1 *The norm of a Gaussian integere $\alpha=x+iy$ is*

$$N(\alpha):=|\alpha|^2=x^2+y^2$$

for example, $N(2+7i)=2^2+7^2=53$.

Lemma 2.2.2 *The norm $N : \mathbb{Z}[i] \to \mathbb{N}$ is a multiplicative function: for α and β in $\mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha) N(\beta)$*

Proof Let α, $\beta \in \mathbb{Z}[i]$ such that $\alpha = x + iy$ and $\beta = u + iv$, then

$$\begin{aligned} N(\alpha\beta) &= (xu - yv)^2 + (xv + yu)^2 \\ &= \left(x^2 + y^2\right)\left(u^2 + v^2\right) \\ &= N(\alpha) N(\beta) \end{aligned}$$

2.3 Units in $\mathbb{Z}[i]$

Definition 2.3.1 *A Gaussian integer u is said to be a unit if it has a multiplicative inverse.*
That is $u \in \mathbb{Z}[i]$ is a unit if and only if there exists $v \in \mathbb{Z}[i]$ such that $uv = 1$.

Proposition 2.3.2 *A Gaussian integer u is a unit*
if and only if $N(u) = 1$.
Furthermore, u is a unit if and only if $u \in \{-1,\ 1,\ -i,\ i\}$.

Proof Suppose $u \in \mathbb{Z}[i]$ is a unit.
Then, there exists $x \in \mathbb{Z}[i]$ such that $ux = 1$.
Taking the norm of this equation we find that

$$N(ux) = N(u) N(x) = 1$$

Hence $N(u) = 1$.

Conversely, suppose $u \in \mathbb{Z}[i]$ such that $N(u) = 1$.
Thene, if $u = a + bi$ for a, $b \in \mathbb{Z}$

$$N(u) = N(a + ib) = a^2 + b^2 = 1$$

So the set of solutions to $a^2 + b^2 = 1$ in $\mathbb{Z} \times \mathbb{Z}$ is:

$$\{(1, 0), (0, 1), (-1, 0), (0, -1)\}$$

Thene $u \in \{\pm 1,\ \pm i\}$ is a unit of $\mathbb{Z}[i]$.

2.4 Associates elements

Definition 2.4.1 *Let $\alpha, \beta \in \mathbb{Z}[i]$ are said to be associates if $\alpha = \beta u$ for some unit u.*
That is $\alpha = i^k \beta$ for some positive integer k.
We note that associates have the same norm since:

$$\alpha = i^k \beta \Rightarrow N(\alpha) = N\left(i^k\right) N(\beta) = N(\beta)$$

2.5 Ideals in $\mathbb{Z}[i]$

Definition 2.5.1 *Let $\beta \in \mathbb{Z}[i]$. We define the ideal of β to be the set of all $\mathbb{Z}[i]$ multiple of β :*

$$(\beta) := \{\ \beta x \mid x \in \mathbb{Z}[i]\ \}$$

From this definition, it follows that $\beta \mid \alpha$ if and only if $\alpha \in (\beta)$.
We also see that if $u \in \mathbb{Z}[i]$ is a unit then $(u) = \mathbb{Z}[i]$.

2.5.1 Representation of $\mathbb{Z}[i]$ as a quotient ring

Let φ be the mapping $\quad \varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}$
$\qquad\qquad\qquad\qquad\qquad\quad f(x) \longrightarrow f(i)$

Proposition 2.5.1

φ is a ring homomorphism with kernel $\ker \varphi = (x^2 + 1)$
and image $\operatorname{Im} \varphi = \mathbb{Z}[i]$.

Proof

$$\begin{aligned}
\varphi(f(x) + g(x)) &= \varphi((f+g)(x)) = (f+g)(i) \\
&= f(i) + g(i) \\
&= \varphi(f(x)) + \varphi(g(x)) \\
\varphi(f(x)\, g(x)) &= \varphi(f(x))\, \varphi(g(x)) \\
\varphi(1) &= 1
\end{aligned}$$

we have

$$\operatorname{Im}\varphi = \{f(i) \mid f \in \mathbb{Z}[X]\}$$

For $f(x) = a_0 + a_1X + \cdots + a_nX^n$ for some $a_i \in \mathbb{Z}$, $n \in \mathbb{N}$

$f(i) = a_0 + a_1i + a_2i^2 + \cdots + a_ni^n$ such that $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i$, $i^6 = -1$, $i^7 = -i$, $i^8 = 1$

$f(i) = a_0 + a_1i - a_2 - a_3i + a_4 + \cdots + a_ni^n$

$f(i) = (a_0 - a_2 + a_4 + \cdots) + i(a_1 - a_3 + a_5 + \cdots)$

$f(i) = a + ib$ for some $a, b \in \mathbb{Z}$, $f(i) \in \mathbb{Z}[i]$

$\operatorname{Im}\varphi = \{ f(i) \mid f \in \mathbb{Z}[X] \} = \mathbb{Z}[i]$

$\ker\varphi = \{ f(x) \in \mathbb{Z}[X] \mid f(i) = 0 \} = (X^2 + 1)$

$p(x) = X^2 + 1 \longrightarrow p(i) = 0 \Rightarrow p(x) \in \ker\varphi$
$\Rightarrow (p(x)) \subset \ker\varphi \cdots (*)$

$f(x) \in \ker\varphi \subset \mathbb{Z}[X]$
$f(x) = (X^2 + 1)q(x) + r(x)$ $\deg r \leq 1$
$f(i) = 0$ and $r(i) = 0$
$r(x) = aX + b$, $r(i) = 0$
$r(i) = ai + b = 0 \Rightarrow a = 0$ or $b = 0$
$r(x) = 0$
Thene, $f(x) = (X^2 + 1)q(x)$ such that $q(x) \in \mathbb{Z}[x]$
$f(x) \in (X^2 + 1) = (p(x))$

$$\ker\varphi \subset (p(x)) \cdots (**)$$

From $(*)$ and $(**)$

$$\ker\varphi = (p(x)) = \left(X^2 + 1\right)$$

Proposition 2.5.1

We have $\mathbb{Z}[i] \cong \mathbb{Z}[x] / (x^2 + 1)$

Proof

Let φ the homomorphism defined as in proposition.
According to the first isomorphism theorem

$$\mathbb{Z}[X] / \ker \varphi \cong \operatorname{Im} \varphi$$

$$\mathbb{Z}[X] / \left(X^2 + 1\right) \cong \mathbb{Z}[i]$$

This means that each Gaussian integer $a + ib \mid a, b \in \mathbb{Z}$.
Can be represented as a polynomial $a + bx$ in $\mathbb{Z}[x]$ modulo $x^2 + 1$.

2.5.2 Matrix representation of Gaussian integers

Let Ψ be the mapping $\quad \Psi : \mathbb{Z}[i] \longmapsto M_2(\mathbb{Z})$

$$a + ib \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

we have, $\ker \Psi = \{0\}$ and $\operatorname{Im} \Psi = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,\ b \in \mathbb{Z} \right\}$

According to the first isomorphism theorem

$$\mathbb{Z}[i] \cong \operatorname{Im} \Psi$$

$$\Psi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \Psi(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

for example,

Let $x = 1 + i \longmapsto 1 + x \bmod X^2 + 1 \longmapsto \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

and $y = 2 - i \longmapsto 2 - x \bmod X^2 + 1 \longmapsto \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}$

$$\begin{aligned} x + y = 3 &\longmapsto (1 + x) + (2 - x) \bmod X^2 + 1 \\ &\longmapsto 3 \bmod X^2 + 1 \\ &\longmapsto \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} x \cdot y = 3 + i &\longmapsto (1+x)(2-x) \bmod X^2+1 \\ &\longmapsto -x^2 + x + 2 \bmod X^2+1 \\ &\longmapsto -(-1) + x + 2 \bmod X^2+1 \\ &\longmapsto 3 + x \bmod X^2+1 \\ &\longmapsto \begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} \end{aligned}$$

2.6 Divisibility in $\mathbb{Z}[i]$

Definition 2.6.1 *Given $\alpha, \beta \in \mathbb{Z}[i]$.*
We write $\alpha|\beta \iff \exists\gamma$ such that $\beta = \gamma\alpha$.

Example 2.1

since $(14 - 3i) = (4 + 5i)(1 - 2i)$, $4 + 5i$ divides $14 - 3i$.

Theorem 2.6.2 *A Gaussian integer $\alpha = a + bi$ is divisible by an ordinary integer c if and only if $c \mid a$ and $c \mid b$ in $\mathbb{Z}$.*

Proof To say $c \mid (a + bi)$ in $\mathbb{Z}[i]$ is the same as $a + bi = c(m + ni)$ for some $m, n \in \mathbb{Z}$, and that is equivalent to $a = cm$ and $b = cn$, or $c \mid a$ and $c \mid b$.

Theorem 2.6.3 *For α, β in $\mathbb{Z}[i]$, if $\beta \mid \alpha$ in $\mathbb{Z}[i]$ then $N(\beta) \mid N(\alpha)$ in $\mathbb{Z}$.*

Proof Write $\alpha = \beta\gamma$ for $\gamma \in \mathbb{Z}[i]$. Taking the norm of both sides, we have $N(\alpha) = N(\beta)N(\gamma)$. This equation is in $\mathbb{Z}$, so it shows $N(\beta) \mid N(\alpha)$ in $\mathbb{Z}$.

Corollary

If $\alpha \in \mathbb{Z}[i]$ and $N(\alpha)$ is prime in $\mathbb{N}$, then α is irreducible in $\mathbb{Z}[i]$.

Proof

Let $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = p$ prime in $\mathbb{N}$. then $\alpha \notin U(\mathbb{Z}[i])$ and $\alpha \neq 0$. Suppose $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$.
Then $N(\alpha) = N(\beta) \cdot N(\gamma)$. This implies either $N(\beta) = 1$ (and hence $\beta \in U(\mathbb{Z}[i])$) or $N(\gamma) = 1$ (and hence $\gamma \in U([0])$).

Thus α is irreducible in $\mathbb{Z}[i]$.

2.7 The Euclidean division theorem in $\mathbb{Z}[i]$

Theorem 2.7.1 *Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then $\exists\ \gamma, \rho \in \mathbb{Z}[i]$ for which $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$.*

· The norm gives the required notion that the remainder ρ be smaller than the divisor β.

Proof Since $N(\rho/\beta) = N(\rho)/N(\beta)$, our job is to find ρ such that $N(\rho/\beta) < 1$. and we want $\rho/\beta = \alpha/\beta - \gamma$.
it is enough for us to find any $\gamma \in \mathbb{Z}[i]$ within distance 1 of α/β.
Let γ be any suitable value and define $\rho = \alpha - \beta\gamma$, whence

$$N(\rho) = N(\alpha - \beta\gamma) = N(\alpha/\beta - \gamma)\, N(\beta) < N(\beta)$$

Example 2.2

Let $\alpha = 4 + 5i$ and $\beta = 3$. Then $\alpha/\beta = (4 + 5i)/3$
$4 + 5i = 3(1 + 2i) + (1 - i)$ $\qquad N(\rho) = 2$.

2.8 The Euclidean algorithm in $\mathbb{Z}[i]$

2.8.1 The greatest common divisors in $\mathbb{Z}[i]$

Definition 2.8.1 *Given $\alpha, \beta \in \mathbb{Z}[i]$, consider the set $S = \{\kappa\alpha + \lambda\beta : \kappa, \lambda \in \mathbb{Z}[i]\}$ A greatest common divisor δ of α and β is a non-zero element of S with minimal norm.*

Theorem 2.8.1

Let α, $\beta \in \mathbb{Z}[i]$ be non-zero. Recursively apply the division, starting with this pair, and make the divisor and remainder in one equation the new divident and divisor in the next, provided the remainder is not zero:

$$\begin{aligned} \alpha &= \beta\gamma_1 + p_1, \quad N(p_1) < N(\beta) \\ \beta &= p_1\gamma_2 + p_2, \quad N(p_2) < N(p_1) \\ p_1 &= p_2\gamma_3 + p_3, \quad N(p_3) < N(p_2) \\ &\vdots \end{aligned}$$

The last non-zero remainder is a greatest common divisor of α and β.

Example 2.3

We show $4+5i$ that and $4-5i$, and which are conjugates, are relatively prime in $\mathbb{Z}[i]$:

$$\begin{aligned} 4+5i &= (4-5i)\,i - (1-i) \\ 4-5i &= -(1-i)(-4) - i \\ -(1-i) &= -i(1+i) + 0 \end{aligned}$$

The last non-zero remainder is a unit, $4+5i$ and $4-5i$ are relatively prime.
Here's an example where the greatest common divisor is not a unit.
Let $\alpha = 11+3i$ and $\beta = 1+8i$.
Then

$$\begin{aligned} 11+3i &= (1+8i)(1-i) + 2 - 4i \\ 1+8i &= (2-4i)(-1+i) - 1 + 2i \\ 2-4i &= (-1+2i)(-2) + 0 \end{aligned}$$

so a greatest common divisor of α and β is $-1+2i$.

Corollary 2.8.2 *For non-zero α and β in $\mathbb{Z}[i]$, let δ be a greatest common divisor produced by Euclid's algorithm. Any greatest common divisor of α and β is a unit multiple of δ.*

Theorem 2.8.3 *Let δ be any greatest common divisor of two non-zero Gaussian integers α and β. Then $\delta = \alpha x + \beta y$ for some x, $y \in \mathbb{Z}[i]$.*

2.9 Gaussian prime and irreducible elements

Corollary 2.9.1 *The non-zero Gaussian integers α and β are relatively prime if and only if we can write*

$$1 = \alpha x + \beta y$$

for some $x, y \in \mathbb{Z}[i]$.

Proof If α and β are relatively prime, then 1 is a greatest common divisor of α and β, so $1 = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$, then any common divisor of α and β is a divisor of 1, and thus is a unit. That says α and β are relatively prime .

Example 2.4

Let $\alpha = 10 + 91i$ and $\beta = 7 + 3i$. By Euclid's algorithm ,

$$\begin{aligned} \alpha &= \beta(6+11i) + 1 - 4i, \\ \beta &= (1-4i)(2i) + -1 + i, \\ 1-4i &= (-1+i)(-3+i) - 1, \\ -1+i &= -1(1-i) + 0, \end{aligned}$$

so the last non-zero remainder is -1. That tells us α and β are relatively prime.

$$\begin{aligned}
-1 &= 1-4i-(-1+i)(-3+i) \\
&= 1-4i-(\beta-(1-4i)(2i))(-3+i) \\
&= (1-4i)(1+(2i)(-3+i))-\beta(-3+i) \\
&= (1-4i)(-1-6i)+\beta(3-i) \\
&= (\alpha-\beta(6+11i))(-1-6i)+\beta(3-i) \\
&= \alpha(-1-6i)+\beta(-(6+11i)(-1-6i)+3-i) \\
&= \alpha(-1-6i)+\beta(-57+46i)
\end{aligned}$$

we can negate to write 1 as a $\mathbb{Z}[i]$ combination of α and β :

$$1=\alpha(1+6i)+\beta(57+46i).$$

Definition 2.9.2 *Let π be a Gaussian integer such that $N(\pi)\geqslant 2$ ($\pi\neq 0$ and not a unit).*
· *π is a Gaussian prime if $\pi\mid\alpha\beta \implies \pi\mid\alpha$ or $\pi\mid\beta$.*
· *π is irreducible if $\pi=\alpha\beta \implies \alpha$ or β is a unit.*

Proposition 2.9.3

π is a Gaussian prime $\iff$ π is irreducible.

Proof
suppose π is a Gaussian prime and that $\pi=\alpha\beta$. Certainly $\pi\mid\alpha\beta$.
Since π is prime we assume that $\pi\mid\alpha$. But then $\alpha=\pi\gamma$ for some $\gamma\in\mathbb{Z}[i]$, whence

$$\pi=\alpha\beta=\pi\gamma\beta\Rightarrow 1=\gamma\beta$$

This says that β is a unit and so π is irreducible.

Conversely, suppose π is irreducible and that $\pi\mid\alpha\beta$.
Let $\delta=\kappa\pi+\lambda\alpha=\gcd(\pi,\alpha)$. Then δ divides both π,α.
But π is irreducible, whence δ is a unit or a unit multiple of π.
- If δ is a unit , then $\delta\beta=\kappa\pi\beta+\lambda\alpha\beta$ is divisible by π. But δ is a unit,

so $\pi \mid \beta$.
- If δ is a unit multiple of π, then $\pi \mid \alpha$.

Example 2.5

1) $N(2) = 4$, 2 is not a Gaussian prime, since $2 = (1+i)(1-i)$. However, both factors $1 \pm i$ are Gaussian primes, since $N(1 \pm i) = 2$ is prime.

2.10 Unique factorization domain

Definition 2.10.1 *An integral domain is a unique factorisation domain (UFD for short) if each non-zero element $a \in A$ is expressible in the form*

$$\alpha = \epsilon p_1 \cdots p_r$$

where ϵ is a unit, and $p_1 \cdots p_r$ are irreducibles, and if moreover this expression is unique up to order and multiplication by units. i.e., if

$$\alpha = \epsilon' p_1' \cdots p_s'$$

then $r = s$, and (p_i' and p_i are associates).
If $r \geqslant 1$ we could of course ϵ with one of the irreducible.

Theorem 2.10.2 *$\mathbb{Z}[i]$ is a Unique Factorisation Domain.*

Proof If $z \in \mathbb{Z}[i]$ is a product of irreducibles, the assertion is true.
If not, then z is not a unit and is not irreducible, suppose $z = wt$
Thus, w and t are not a units.
Then by induction on $N(z)$:

$$N(z) = N(w) N(t) \Rightarrow N(w), N(t) < N(z)$$

Hence w, t are products of irreducibles.

CHAPTER 3

SOME APPLICATIONS

3.1 The sum of squares

Let $n \in \mathbb{N}$, we will study the proplem of existing of $a, b \in \mathbb{N}$ such that $n = a^2 + b^2$. Let Σ be the set:

$$\Sigma = \left\{ \; n \in \mathbb{N} \mid n = a^2 + b^2; \; a, b \in \mathbb{N} \; \right\}$$

Proposition 3.1.1

if $n \equiv 3 (\mathrm{mod}\, 4)$ *we have* $n \notin \Sigma$.

Proof

if a is even then, $a^2 \equiv 0 \,\mathrm{mod}\, 4$,
if a is odd, $a^2 \equiv 1 \,\mathrm{mod}\, 4$.
Then $a^2 + b^2 \equiv 0, 1, 2 (\mathrm{mod}\, 4)$.

Lemma 3.1.2

$p \in \Sigma \Leftrightarrow p$ *is not irreducible in* $\mathbb{Z}[i]$.

Proof

If $p = a^2 + b^2$, $p = (a + ib)(a - ib)$ and $a, b \neq 0$.
Thene,$(a + ib)$, $(a - ib) \notin \mathbb{Z}[i]^*$, so that p is not irreducible.

Conversely, if $p = zz'$ with z, $z' \neq \pm 1$, $\pm i$, so $N(p) = N(z) N(z') = p^2$ and $N(z)$, $N(z') \neq 1$, $N(z) = p$, thene $p \in \Sigma$.

Proposition 3.1.3 *The number $n \in \mathbb{N}$ is expressible as a sum of two squares if and only if each rational prime $p \equiv 3 \bmod 4$ occurs to an even power in n.*

Proof Suppose first n is the sum of two squares. We show by induction on n that it must have the stated form.
Suppose

$$n = x^2 + y^2 = (x + iy)(x - iy)$$

and suppose $p \mid n$, where $p \equiv 3 \bmod 4$. Then

$$p \mid x + iy \text{ or } p \mid x - iy$$

In either case

$$p \mid x \text{ and } p \mid y$$

But $p^2 \mid n$ and we can divide the equation by p^2 :

$$n \mid p^2 = (x \mid p)^2 + (y \mid p)^2$$

But now the result for n follows from that for $n \mid p^2$.
Now suppose that n has this form, say

$$n = 2^e p_1^{e_1} \cdots p_r^{e_r} q_1^{2f_1} \cdots q_s^{2f_s}$$

Where $p_1, \cdots, p_r$ are primes $\equiv 1 \bmod 4$ and $q_1, \cdots, q_s$ are primes $\equiv 3 \bmod 4$.
Each rational prime p_i splits into conjugate primes, say

$$p = \pi_i \overline{\pi}_i$$

Let

$$\theta = m + in = (1 + i)^e \, \pi_1^{e_1} \cdots \pi_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$$

Then

$$\begin{aligned} N(\theta) &= m^2+n^2 \\ &= N(1+i)^e N(1+i)^e N(\pi_1)^{e_1}\cdots N(\pi_r)^{e_r} N(q_1)^{f_1}\cdots N(q_s)^{f_s} \\ &= 2^e p_1^{e_1}\cdots p_r^{e_r} q_1^{2f_1}\cdots q_s^{2f_s} \\ &= n. \end{aligned}$$

Example 3.1
Since

$$2317 = 7\cdot 331,$$

7 occurs just once in 2317 is not the sum of two squares.
But

$$2009 = 7\cdot 7\cdot 41$$

Here 7 occurs twice, while $41 \equiv 1 \bmod 4$. Hence 2009 is the sum of two squares.
Our argument shows that if

$$2009 = m^2+n^2$$

then

$$7 \mid m, n$$

If we set

$$m = 7a,\ n = 7b$$

then

$$41 = a^2+b^2$$

Now it is easy to see that a, $b = 5$, 7 (if we restrict to positive solutions), i.e.,

$$2009 = 35^2+40^2$$

The argument also gives the number of ways of expressing a number as the sum of two squares.

3.2 congruences in $\mathbb{Z}[i]$

Definition 3.2.1

Two Gaussian integers α and β are said to be congruent modulo a Gaussian number μ if $\mu \mid (\alpha - \beta)$.
We write,

$$\alpha \equiv \beta (\bmod \mu).$$

For example, $1 + 12i \equiv 2 - i \bmod 3 + i$, we subtract and divide:

$$(3+i) \mid (1 + 12i - (2 - i)) = (3 + i) \mid (13i - 1) = 1 + 4i$$

The congruences modulo μ is a compatible relation with respect to addition and multiplications defenid in $\mathbb{Z}[i]$:
If $\alpha \equiv \alpha' \bmod \mu$, and $\beta \equiv \beta' \bmod \mu$
Then $\alpha + \beta \equiv \alpha' + \beta' \bmod \mu$
$\alpha\beta \equiv \alpha'\beta' \bmod \mu$.

A Gaussian integer can be reduced modulo α, if $\alpha \neq 0$, to get a congruent Gaussian integer with small norm by dividing by α and using the remainder.

Example 3.2 Let's compute $(3 + 2i)^2 \bmod (4 + i)$.
Since $(3 + 2i)^2 = 5 + 12i$ and $5 + 12i = (4 + i)(2 + 3i) - 2i$,
we have $(3 + 2i)^2 \equiv -2i \bmod (4 + i)$.

Theorem 3.2.1 *If π is a prime in $\mathbb{Z}[i]$, then $\alpha\beta \equiv 0 \bmod \pi$ if and only if $\alpha \equiv 0 \bmod \pi$ or $\beta \equiv 0 \bmod \pi$.*

Theorem 3.2.2 *For α and β in $\mathbb{Z}[i]$ with $\beta \neq 0$, $\alpha x \equiv 1 \bmod \beta$ is solvable if and only if α and β are relatively prime in $\mathbb{Z}[i]$. If α and β are relatively prime then any linear congruence $\alpha x \equiv \gamma \bmod \beta$ has a unique solution.*

Example 3.3

This congruences $(1+8i)\,x \equiv 1 \bmod (11+3i)$ has not solvable,
since $1+8i$ and $11+3i$ have a common factor of $-1+2i$ by example 2.3

Example 3.4

This congruences $(7+3i)\,x \equiv 1 \bmod (10+91i)$, has a solution
$7+3i$ and $10+91i$ are relatively prime.
Moreover, by using Euclid's algorithm

$$(7+3i)\,(57-46i) + (10+91i)\,(1+6i) = 1$$

so a solution is $x = 57-46i$.

Proposition 3.2.3 *For a, b and c in $\mathbb{Z}$, $a \equiv b \bmod c$ in $\mathbb{Z}$ if and only if $a \equiv b \bmod c$ in $\mathbb{Z}[i]$.*
And we write

$$c \mid (a-b) \ \text{ in } \mathbb{Z} \Leftrightarrow c \mid (a-b) \ \text{ in } \mathbb{Z}[i]$$

Example 3.5

Let $\pi = 3$, which is prime in $\mathbb{Z}[i]$. Take $\alpha = i$.
Then $\alpha^{\pi-1} = i^2 = -1$, but -1 is not congruent $1 \bmod 3$,
so $\alpha^{\pi-1}$ is not congruent $1 \bmod \pi$.

3.3 Arctangent Identities for π

The Gregory series for arctangent:

$$\arctan x = x - x^3/3 + x^5/5 - x^7/7 + x^9/9 - \cdots, \ |x| \le 1$$

putting $x = 1$, we get

$$\pi/4 = \arctan 1$$

to yield Leibniz's series

$$\pi/4 = 1 - 1/3 + 1/5 - 1/7 + 1/9 - \cdots$$

utilize the x^n terms in Gregory's series and have been instrumental in the calculation of π.

$$\pi = r \arctan x$$

Lemma 3.3.1 *Let $z \neq 0$ be a Gaussian integer. There is a natural number n such that z^n is real if and only if z lies on one of the four lines in $\mathbb{C}$:*

$$\operatorname{Im} z = 0, \operatorname{Re} z = \operatorname{Im} z, \operatorname{Re} z = 0, \text{ and } \operatorname{Re} z = -\operatorname{Im} z.$$

Proof Let $n = 1$, 2, or 4. let $z^n = m \in \mathbb{Z}$ where $0 \neq z = a + ib$.
Where z is a nonunit and is primitive, that is, $\gcd(a, b) = 1$. In this case, let w be any Gaussian prime divisor of z. Then $w \mid m$ and so $\overline{w} \mid \overline{m} = m$, since m is real. As $\overline{w}$ is a Gaussian prime that divides $m = z^n$, we see that $\overline{w} \mid z$.

$\cdot$ If w is a Gaussian prime dividing z, and w and $\overline{w}$ are not associates, then $w\overline{w} \in \mathbb{Z}$ divides z.

As z is primitive, the fact implies that z is a product of Gaussian primes, each of which is an associate of its conjugate. Let $v = c + id$ be such a Gaussian prime factor of z.
As v and $\overline{v}$ are associates, we see that $c = 0$, $d = 0$, or $c = \pm d$.
The first two cases are not possible, since z is primitive.
The third case implies $c = \pm 1$ since v is prime.
It follows that v is an associate of $1 + i$ and $z = u(1 + i)^l$ for some unit u and natural number l.
Throughout this section $k \in \mathbb{Z}$ and $n \in \mathbb{N}$.

Corollary 3.3.2 *The only rational values of $\tan k\pi/n$ are 0 and ± 1.*

Proof Suppose $\tan k\pi/n = b/a$ where $b \in \mathbb{Z}$ and $a \in \mathbb{N}$. Thene

$$k\pi/n = \arg(a + ib) \Rightarrow k\pi = \arg(a + ib)^n \in \mathbb{Z}$$

and so argument of $a + ib$,namely $k\pi/n$, is an integer multiple of $\pi/4$ by the lemma.

Corollary 3.3.3 *Identities of the form* $k\pi = n \arctan x$ *with* x *rational have* $x = 0$ *or* $x = \pm 1$. *In particular,* $\pi = 4 \arctan 1$ *is the most efficient such identity for computing* π *using Gregory's series.*

Proof Given $k\pi/n = \arctan x$, apply tan and use the previous corollary. Multiple-angle rational arctangent identities for π have the form

$$k\pi/n = \sum_{j=1}^{l} m_j \arctan b_j/a_j \qquad (1)$$

where all variables are rational integers. It is natural to assume, without loss of generality, That $n \in \mathbb{N}$, $\gcd(k, n) = 1$, $\gcd(m_1, \cdots, m_l) = 1$, the values $\mid b_j/a_j \mid$ are distinct, and that for all $j : m_j \in \mathbb{N}$, $b_j \neq 0$, $a_j \in \mathbb{N}$, and $\gcd(a_j, b_j) = 1$. We note that $k = 0$.

Corollary 3.3.4 *If (1) holds, then* $k\pi/n = j\pi/4$ *for some integer* j. *In particular* $n = 1, 2,$ *or* 4.

Proof Modulo 2π we have

$$k\pi/n = \sum_{j=1}^{l} m_j \ \arctan b_j/a_j = \sum_{j=1}^{l} m_j \arg(a_j + ib_j) = \arg \prod_{j=1}^{l} (a_j + ib_j)^{mj}$$

Let z denote the product above. Then z^n is real and so $\arg z = k\pi/n$ is a multiple of $\pi/4$ by the lemma.

Corollary 3.3.5 *A right triangle with rational acute angles and rational legs is a* $45 - 45 - 90$ *triangle.*

Proof Suppose triangle ABC has a right angle at C , rational legs a and b opposite the angles at A and B respectively, and the angle β at B is a rational multiple of π. Then $\tan\beta = b/a$ is rational and equals $+1$ by corollary 3.3.1,
since side lengths are positive. Therefore, $\beta = \pi/4$.

Conclusion

In this work, we have studied some properties of the ring of Gaussian Numbers $\mathbb{Z}[i]$: Constructions, Euclidean algorithm, gcd, lcm, unique factorization, irreducible elements,... and mention some of their application in Number Theory (Sum of squares, Congruences), Geometry (Right triangle with rational angles and edges), and Analysis(Arctangent Identities for π).

BIBLIOGRAPHY

[1] J. S. Calcut, Gaussian Integers and Arctangent Identities for π. https://isis2.cc.oberlin.edu/faculty/jcalcut/gausspi.pdf

[2] K. Conrad, The Gaussian integers, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf

[3] L. Goldmakher, Basic notions from ring theory, https://web.williams.edu/mathematics/lg5/394/Rings.pdf

[4] J. M. Howie, Fields and Galois Theory. Springer Undergraduate Mathematics Series. 2006.

[5] P. A. Grillet, Abstract Algebra. Second edition, Graduate Texts in Mathematics, 2007.

[6] A.Kaeli, The Arithmetic of the Gaussian integers, https://personal.math.ubc.ca/~anstee/math444/GaussianIntegersfinal.pdf

[7] H. A. Priestley, Introduction to Groups,Rings and Field,2011. https://people.maths.ox.ac.uk/flynn/genus2/sheets0405/grfnotes1011.pdf

[8] E. Landin, S. Hussein, Gaussian Integers and other Quadratic Integer rings, degree project in technology, first cycle, 15 credits stockholm, sweden 2021.

[9] S.Moy, An Introduction to the Theory of Field Extensions, https://math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPagers/May.pdf

[10] S.Waner, Introduction to Rings and Fields, Department of Mathematics, Hofstra University, Second printing 2003.

ملخص

يهدف هذا العمل الى دراسة بعض خصائص حلقة الأعداد الجاوسية : وهي أعداد مركبة حيث جزؤها الحقيقي والتخيلي عدد صحيح. ترتبط هذه الخصائص بالهيكل الجبري للحلقة : البناء ، الخوارزمية الإقليدية ، القاسم المشترك الأكبر ، المضاعف المشترك الأصغر ، الحلقات المعاملية . أخيرا ، نذكر بعض تطبيقاتها في نظرية الأعداد والهندسة والتحليل.

كلمات مفتاحية

الحلقة ، المجال ، حلقة الاعداد الصحيحة الغاوسية.

Abstract

The goel of this work is to study some properties of the ring of Gaussian Numbers Z[i] : complex numbers whose real and imaginary parts are both integers (in z) . These properties are related to the algebraic structure of the ring : construction, Euclidean algorithm, gcd, lcm, unique factorization. Finaly , we mention some of their applications in Number Theory, geometry, and Analysis

Key words

Ring, Ideal, the ring of gaussian integers.

Résumé

Le but de ce travail est d'étudier certaines propriétés de l'anneau des nombres de Gauss Z[i] : des nombres complexes dont les parties réelles et imaginaires sont toutes deux des entiers (dans Z). Ces propriétés sont liées à la structure algébrique de l'anneau : construction, algorithme Euclidean, pgcd, ppcm, anneau factoriels. Enfin, nous mentionnons quelques-unes de leurs applications en Théorie des Nombres, Géométrie et Analyse.

Mot-clés

Anneau , Ideal , Anneau des entiers de Gauss .