Hang Lung Mathematics Awards
Vol. 9 (2021), pp. 137–158

AN INVESTIGATION ON THE RINGS OF INTEGER-VALUED POLYNOMIALS ON GAUSSIAN INTEGERS AND INTEGER-VALUED CONTINUOUS FUNCTIONS

A RESEARCH REPORT SUBMITTED TO THE SCIENTIFIC COMMITTEE OF THE HANG LUNG MATHEMATICS AWARDS

TEAM MEMBER
MYRON LAM

TEACHER
MR. CHAN LONG TIN

SCHOOL
DIOCESAN BOYS' SCHOOL

AUGUST 2021

Abstract. This is an investigation on the ring of integer-valued polynomials on the Gaussian integers and the ring of integer-valued continuous function on rational integers, inspired by the results from integer-valued polynomials on the rational integers. Polynomials in the first ring map Gaussian integers to Gaussian integer values while functions in the second ring map rational integers to rational integers. This investigation explores their properties as rings, following a chain of class inclusions, which includes the most commonly known domains. The properties of rings of polynomials over algebraic integers, continuously differentiable functions on rational integers and continuous functions on Gaussian integers are also discussed.

Keywords. Rational Integers, Gaussian Integers, Integer-valued Polynomials, Basis, Binomial Polynomials, Continuous Functions, Kernel, Ring, Integral Domain, Integrally Closed Domain, Irreducible Element, Ideal, Principal Ideal, Gaussian Primes, Non-Noetherian Ring, Ascending Chain Condition on Principal Ideals

Contents

1. Introduction and Main Results

Integer-valued polynomials on the rational integers have been studied extensively by mathematicians for little more than a century. In 1915, George Pólya showed that the integer-valued polynomials are generated by the binomial polynomials. Subsequent studies showed that this set of polynomials formed an integrally closed and non-Noetherian ring.

In this report, we attempt to generalize these results to include the Gaussian integers and continuous functions, using mathematical tools that an average undergraduate maths student has access to. We denote the set of integer-valued polynomials on Gaussian integers by $\mathrm{Int}(\mathbb{Z}[i])$ and the set of integer-valued continuous functions on rational integers by $C(\mathbb{Z})$. We investigate the properties of these rings by following two chains of class inclusions:

$$\text{Rings} \supset \text{ID} \supset \text{Integrally Closed Domain} \supset \text{GCD Domain} \supset \text{UFD} \supset \text{PID} \supset \text{ED} \supset \text{Fields}$$

$$\text{Field} \implies \text{Artinian} \implies \text{Noetherian} \implies \text{ACCP}$$

We obtain the following results:

- **Theorem 1.** $\mathrm{Int}(\mathbb{Z}[i])$ has a basis.
- **Theorem 2.** $\mathrm{Int}(\mathbb{Z}[i])$ is non-Noetherian.
- **Theorem 3.** $\mathrm{Int}(\mathbb{Z}[i])$ satisfies the ascending chain condition on principal ideals.
- **Theorem 4.** $\mathrm{Int}(\mathbb{Z}[i])$ is an integrally closed domain.
- **Theorem 5.** $\mathrm{Int}(\mathbb{Z}[i])$ is not a GCD domain.
- **Theorem 6.** $C(\mathbb{Z})$ does not satisfy the ACCP.
- **Theorem 7.** $C(\mathbb{Z})$ is not a unique factorization domain.

2. Definitions and Prerequisites

Before we proceed to the crux of this paper, there is a need to define the terminology used in this term. Here we provide an overview of ring theory and an introduction to integer-valued polynomials.

2.1. **Overview of Ring Theory.** Theorems and remarks in this section are book-work, so their proofs are omitted.

Notation. Let $* : \{a\} \times S \to R$ be a binary operation. We define $a * S = \{a * s : s \in S\}$ and $S * a = \{s * a : s \in S\}$.

Definition (Group)**.** A *group* is a triple $(G, \cdot, e)$, where G is a set,$\cdot : G \times G \to G$ is a function and $e \in G$ is an element such that:

(1) For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(2) For all $a \in G$, we have $a \cdot e = e \cdot a = a$.
(3) For all $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition (Subgroup)**.** If $(G, \cdot, e)$ is a group and $H \subset G$ is a subset, then H is a *subgroup* if

(1) $e \in H$,
(2) $a, b \in H$ implies $a \cdot b \in H$,
(3) $\cdot : H \times H \to H$ makes $(H, \cdot, e)$ a group.

Definition (Abelian group)**.** A group G is *abelian* if $a \cdot b = b \cdot a$ for all $a, b \in G$.

Definition (Ring)**.** A *ring* is a quintuple $(R, +, \cdot, 0, 1)$, where R is a set,$+, \cdot : R \times R \to R$ are binary operations and $0, 1 \in R$ are elements such that:

(1) $(R, +, 0)$ is an abelian group.
(2) The operation $\cdot : R \times R \to R$ satisfies associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and identity $1 \cdot r = r \cdot 1 = r$.
(3) Multiplication distributes over addition, i.e.

$$r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$$
$$(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3)$$

Remark. The set of rational integers $\mathbb{Z}$ is a ring.

Definition (Commutative ring)**.** A ring R is *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in R$.

Definition (Subring)**.** Let $(R, +, \cdot, 0, 1)$ be a ring, and $S \subseteq R$ be a subset. We say S is a *subring* of R if $0, 1 \in S$, and the operations $+, \cdot$ make S into a ring in its own right. In this case we write $S \leq R$.

Definition (Overring)**.** We say R is an *overring* of S if S is a subring of R.

Definition (Unit)**.** An element $u \in R$ is a *unit* if there is another element $v \in R$ such that $u \cdot v = 1$.

Definition (Field)**.** A *field* is a non-zero ring F where every non-zero $u \in F$ is a unit.

Definition (Ideal)**.** A subset $I \subset R$ is an *ideal*, written $I \lhd R$, if

(1) I is an additive subgroup of $(R, +, 0)$.
(2) $a \in I, b \in R$ implies $a \cdot b \in I$.

Definition (Generator of ideal)**.** For an element $a \in R$, the *ideal generated by* a is

$$(a) = aR = \{a \cdot r : r \in R\} \lhd R$$

In general, let $a_1, \dots, a_k \in R$, the *ideal generated by* $a_1, \dots, a_k$ is

$$(a_1, \dots, a_k) = \{a_1 r_1 + \cdots + a_k r_k : r_1, \dots, r_k \in R\}$$

Definition (Principal ideal)**.** An ideal I is a *principal ideal* if $I = (a)$ for some $a \in R$.

Definition (Integral domain)**.** A non-zero ring R is an *integral domain* if for all $a, b \in R$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Definition (Zero divisor)**.** An element $x \in R$ is a *zero divisor* if $x \neq 0$ and there is a $y \neq 0$ such that $x \cdot y = 0 \in R$.

Definition (Field of fractions)**.** Let R be an integral domain. A *field of fractions* F of R is a field with the following properties:

(1) $R \leq F$.
(2) Every element of F may be written as $a \cdot b^{-1}$ for $a, b \in R$, where b^{-1} means the multiplicative inverse to $b \neq 0$ in F.

Remark. The set of rationals $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

Definition (Division)**.** For elements $a, b \in R$, we say a *divides* b, written $a \mid b$, if there exists $c \in R$ such that $b = ac$.

Definition (Associates)**.** $a, b \in R$ are *associates* if $a = bc$ for some unit c.

Definition (Irreducible)**.** $a \in R$ is *irreducible* if $a \neq 0$, a is not a unit, and if $a = xy$, then x or y is a unit.

Definition (Prime)**.** $a \in R$ is *prime* if a is non-zero, not a unit, and whenever $a \mid xy$, either $a \mid x$ or $a \mid y$.

Remark. If $r \in R$ is prime, then it is irreducible.

Definition (Euclidean domain)**.** An integral domain R is a *Euclidean domain* if there is a *Euclidean function* $\phi : R \setminus \{0\} \to \mathbb{Z}^+$ such that:

(1) $\phi(a \cdot b) \geq \phi(b)$ for all $a, b \neq 0$
(2) If $a, b \in R$, with $b \neq 0$, then there are $q, r \in R$ such that $a = b \cdot q + r$ and either $r = 0$ or $\phi(r) < \phi(b)$.

Definition (Principal ideal domain)**.** A ring R is a *principal ideal domain* (PID) if it is an integral domain, and every ideal is a principal ideal.

Theorem. Let R be a Euclidean domain. Then R is a principal ideal domain.

Definition (Unique factorization domain)**.** An integral domain R is a *unique factorization domain* (UFD) if

(1) Every non-unit may be written as a product of irreducibles;
(2) If $p_1 \cdot p_2 \cdot \cdots \cdot p_n = q_1 \cdot q_2 \cdot \cdots \cdot q_m$ with p_i, q_j irreducible, then $n = m$, and they can be reordered such that p_i is an associate of q_i.

Theorem. Let R be a principal ideal domain. Then R is a unique factorization domain.

Definition (GCD domain)**.** d is a *greatest common divisor* (GCD) of $a_1, a_2, \ldots, a_n$ if $d \mid a_i$ for all i, and if any other d' satisfies $d' \mid a_i$ for all i, then $d' \mid d$. An integral domain R is a *GCD domain* if any two elements of R have a greatest common divisor.

Theorem. Let R be a unique factorization domain. Then R is a GCD domain.

Theorem. Let R be a GCD domain. If $p \in R$ is irreducible, then it is prime.

Definition (Polynomial)**.** Let R be a ring. Then a *polynomial* with coefficients in R is an expression

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

with $a_i \in R$.

Definition (Degree of polynomial)**.** The *degree* of a polynomial f is the largest m such that $a_m \neq 0$.

Theorem (Fundamental theorem of algebra)**.** Let $f \in (X) \lhd \mathbb{C}[X]$ have degree n. Counting repeated roots, $f(x) = 0$ has n roots in $\mathbb{C}$.

Definition (Polynomial ring)**.** We write $R[X]$ for the ring formed by the set of all polynomials with coefficients in R. The operations are performed the usual way.

Definition (Rational functions)**.** Let F be a field. f is a *rational function* if $f = \dfrac{P}{Q}$ for some $P, Q \in F[X]$ and $Q \neq 0$.

Theorem. Let F be a field. The set of rational functions in F forms a field $F(X)$.

Remark. Let R be a ring and let K be its field of fractions. $F(X)$ is the field of fractions of $R[X]$.

Definition (Integral element)**.** Let $a \in R$ and let $S \leq R$. a is *integral* over S if there exists $f \in S[X]$ such that $f(a) = 0$. R is *integral* over S if every element of R is integral.

Definition (Integrally closed domain)**.** Let R be an integral domain and let K be its field of fractions. R is an *integrally closed domain* if $a \in K$ integral over R implies $a \in R$.

Theorem. Let R be a GCD domain. Then R is an integrally closed domain.

Definition (Ascending chain condition)**.** A ring satisfies the *ascending chain condition* (ACC) if there is no infinite strictly increasing chain of ideals.

Definition (Noetherian ring)**.** A ring that satisfies the ascending chain condition is known as a *Noetherian ring*.

Definition (Finitely generated ideal)**.** An ideal I is *finitely generated* if it can be written as $I = (r_1, \ldots, r_n)$ for some $r_1, \ldots, r_n \in R$.

Theorem. A ring is Noetherian if and only if every ideal is finitely generated.

Definition (Descending chain condition)**.** A ring satisfies the *descending chain condition* (DCC) if there is no infinite strictly decreasing chain of ideals.

Definition (Artinian)**.** A ring that satisfies the descending chain condition is known as an *Artinian ring*.

Theorem. Let R be a Noetherian ring. Then R is an Artinian ring.

Theorem. If R is an Artinian integral domain, then R is a field.

Definition (Ascending chain condition on principal ideals)**.** A ring satisfies the *ascending chain condition on principal ideals* (ACCP) if there is no infinite strictly increasing chain of principal ideals.

Definition (Generating set)**.** Let R be a ring and let $V \subset U \subset R[X]$. V is a *generating set* of U if for every $f \in U$, there exist $f_1, \ldots, f_n \in V$ and $r_1, \ldots, r_n \in R$ such that $f = r_1 f_1 + \cdots + r_n f_n$.

Definition (Basis)**.** Let R be a ring and let $V \subset U \subset R[X]$. V is a *basis* of U if V is a generating set of U and if V is linearly independent, i.e. for every $f_1, \ldots, f_n \in V$, $r_1 f_1 + \cdots + r_n f_n = 0$ implies $r_1 = \cdots = r_n = 0$.

2.2. **Integer-valued polynomials.** We give a formal definition of what an integer-valued polynomial is.

Definition (Integer-valued polynomials)**.** Let D be an integral domain and let K be its field of fractions. $f \in K[X]$ is an *integer-valued polynomial* if $f(a) \in D$ whenever $a \in D$.

To proceed, we need to verify that $\mathrm{Int}(D)$ is indeed a ring.

Proposition 1. Integer-valued polynomials on an integral domain D, with quotient field K, form a commutative ring $\mathrm{Int}(D) = \{f \in K[X] : f(D) \subset D\}$ with $D[X] \subset \mathrm{Int}(D) \subset K[X]$.

Proof. Let $f, g, h \in \mathrm{Int}(D)$.

$$\begin{gathered}(f+g)+h = f+(g+h)\\ f+g = g+f\\ (f\cdot g)\cdot h = f\cdot(g\cdot h)\\ f\cdot g = g\cdot f\\ f\cdot(g+h) = f\cdot g + f\cdot h\end{gathered}$$

Associativity, commutativity and distributivity are satisfied. We also have

$$\begin{gathered}0, 1 \in \mathrm{Int}(D)\\ f+0 = 0+f = f\\ f\cdot 1 = 1\cdot f = f\\ f+(-f) = 0\end{gathered}$$

Additive identity, multiplicative identity and additive inverse exist. Moreover, if $r \in D$, then $f(r), g(r) \in D$ and thus $(f+g)(r), (fg)(r) \in D$. It follows that $\mathrm{Int}(D)$ is a ring.

Obviously, $f \in \mathrm{Int}(D)$ implies $f \in K[X]$. Moreover, since D is a ring, $f \in D[X]$ and $a \in D$ implies $f(a) \in D$. So $D[X] \subset \mathrm{Int}(D) \subset K[X]$. □

Proposition 2. $\mathrm{Int}(D)$ is an integral domain.

Proof. If $f, g \in \mathrm{Int}(D)$ and $f, g \neq 0$, then there exists $r \in D$ such that $f(r), g(r) \neq 0$. Since D is a integral domain, it follows that $f(r)g(r) \neq 0$ and $fg \neq 0$. There are no nonzero zero divisors and so $\mathrm{Int}(D)$ is a integral domain. □

Proposition 3. $\mathrm{Int}(D)$ is not a field.

Proof. Obviously, $X \in \mathrm{Int}(D)$ and $X \neq 0$. However, X^{-1} is not a polynomial and $X^{-1} \notin \mathrm{Int}(D)$. X is a nonzero element that has no multiplicative inverse in $\mathrm{Int}(D)$, so $\mathrm{Int}(D)$ is not a field. □

Proposition 4. $\mathrm{Int}(D)$ is not Artinian.

Proof. $(X) \supset (X^2) \supset \ldots$ is a strictly decreasing chain of ideals. □

Proposition 5. The field of fractions of $\mathrm{Int}(D)$ is $K(X)$.

Proof. $\mathrm{Int}(D) \subset K[X]$ and $K[X] \leq K(X)$, so $\mathrm{Int}(D) \leq K(X)$. Let $f \in K(X)$. Since $K(X)$ is the field of fractions of $D[X]$, $f = ab^{-1}$ for some $a, b \in D[X] \subset \mathrm{Int}(D)$. □

3. Polynomials on Rational Integers

In this section, we recap some well-known facts about the ring of integer-valued polynomials on rational integers. For proofs that are not entirely original, only a simple sketch will be provided.

Proposition 6. The binomial polynomials

$$\binom{X}{n} = \frac{X \ldots (X-n)}{n!} \quad \text{for } n = 0, 1, \ldots$$

form a basis of $\mathrm{Int}(\mathbb{Z})$.

Proof. (Sketch) Let B be the ring generated by the binomial polynomials, i.e.

$$B = \left\{ a_1 f_1 + \cdots + a_n f_n : n \in \mathbb{N}, a_i \in \mathbb{Z}, f_i \in \left\{ \binom{X}{m} \right\}_{m \in \mathbb{N}} \right\}$$

We first show that every binomial polynomial is integer-valued, so $B \subset \mathrm{Int}(\mathbb{Z})$. Next, by induction on n, we show that for any $f \in \mathrm{Int}(\mathbb{Z})$ of degree n, we can write $f = \sum_{i=0}^{n} a_i \binom{X}{i}$ for some $a_0, \ldots, a_n \in \mathbb{Z}$. Hence $\mathrm{Int}(\mathbb{Z}) \subset B$ and $\mathrm{Int}(\mathbb{Z}) = B$. The binomial polynomials form a basis of $\mathrm{Int}(\mathbb{Z}) = B$. □

By Hilbert's basis theorem, the ring $\mathbb{Z}[X]$ is a Noetherian ring. However, $\mathrm{Int}(\mathbb{Z})$ does not inherit this property.

Proposition 7. Int($\mathbb{Z}$) is not Noetherian.

Proof. (Sketch) Let $\mathfrak{I}_n = \left(\binom{X}{1}, \ldots, \binom{X}{n}\right) \lhd \text{Int}(\mathbb{Z})$. It is possible to show that for all prime p, $\binom{X}{p} \notin \mathfrak{I}_m$ for all $1 \leq m \leq p-1$. It follows that for primes $r < s$, $\mathfrak{I}_r \subset \mathfrak{I}_s$ is proper and that $\{\mathfrak{I}_p\}_{p \text{ prime}}$ is a strictly increasing chain of ideals. □

This is significant since Int($\mathbb{Z}$) is one of the simpler and more natural textbook examples of non-Noetherian rings.

Proposition 8. Int($\mathbb{Z}$) satisfies the ascending chain condition on principal ideals.

Proof. Let $a_1, a_2, \cdots \in \text{Int}(\mathbb{Z})$ such that $(a_1) \subset (a_2) \subset \ldots$ is a chain of ideals in Int($\mathbb{Z}$). If $a_m \mid a_n$ and a_m and a_n are not associates, then $(a_n) \subset (a_m)$. Moreover, $\dfrac{a_n}{a_m} \notin \text{Int}(\mathbb{Z})$ and $a_n \notin (a_m)$. In fact, $(a_n) \subset (a_m)$ is proper (i.e. $(a_n) \neq (a_m)$) if and only if $a_m \mid a_n$ and a_m and a_n are not associates. Since the number of factors of a_1 is finite, there exists $N \in \mathbb{N}$ such that $a_N, a_{N+1}, \ldots$ are equal up to associates. The choice of $a_1, a_2, \ldots$ is arbitrary, so Int($\mathbb{Z}$) satisfies the ascending chain condition on principal ideals. □

Next, we show that Int($\mathbb{Z}$) is integrally closed.

Proposition 9. Int($\mathbb{Z}$) is an integrally closed domain.

Proof. Let $f \in \mathbb{Q}(X)$ be non-zero and integral over Int($\mathbb{Z}$), i.e.

$$f^n + g_{n-1}f^{n-1} + \cdots + g_1 f + g_0 = 0$$

where $g_j \in \text{Int}(\mathbb{Z})$ for $j = 0, 1, \ldots, n-1$. We can write $f = \dfrac{a}{b}$ where $a, b \in \mathbb{Z}[X]$ are non-zero and have no common factors. Then,

$$a^n + g_{n-1}a^{n-1}b + \cdots + g_1 ab^{n-1} + g_0 b^n = 0$$

Since a and b have no common factors in $\mathbb{Z}[X]$, by fundamental theorem of algebra, we can find $\alpha \in \mathbb{C}$ such that $b(\alpha) = 0$ but $a(\alpha) \neq 0$.

$$\begin{aligned} (a^n + g_{n-1}a^{n-1}b + \cdots + g_1 ab^{n-1} + g_0 b^n)(\alpha) &= 0 \\ a^n(\alpha) + g_{n-1}(\alpha)a^{n-1}(\alpha)b(\alpha) + \cdots + g_1(\alpha)a(\alpha)b^{n-1}(\alpha) + g_0(\alpha)b^n(\alpha) &= 0 \\ a^n(\alpha) &= 0 \end{aligned}$$

We arrive at a contradiction. It follows that b must be constant and so $f \in \mathbb{Z}[X]$. For all $a \in \mathbb{Z}$, we have

$$f^n(a) + g_{n-1}(a)f^{n-1}(a) + \cdots + g_1(a)f(a) + g_0(a) = 0$$

So $f(a)$ is integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is integrally closed, $f(a) \in \mathbb{Z}$ for all $a \in \mathbb{Z}$ and so $f \in \text{Int}(\mathbb{Z})$. □

Lastly, recall that in a GCD domain, irreducible and prime are equivalent. We use this to show that Int($\mathbb{Z}$) is not a GCD domain.

Lemma 1. $\binom{X}{r}$ is irreducible but not prime.

Corollary 1. Int($\mathbb{Z}$) is not a GCD domain, unique factorization domain, principal ideal domain or Euclidean domain.

4. Polynomials on Gaussian Integers

Here we consider integer-valued polynomials on a domain that is not $\mathbb{Z}$, namely the set of Gaussian integers $\mathbb{Z}[i]$, which is defined below:

Definition (Gaussian integers)**.** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$ is the set of *Gaussian integers*. $\mathbb{Z}[i]$ is a ring.

Definition (Gaussian rationals)**.** $\mathbb{Q}(i) = \left\{\frac{a}{b} : a, b \in \mathbb{Z}[i]\right\} = \{a + bi : a, b \in \mathbb{Q}\} = \mathbb{Q}[i]$ is the set of *Gaussian rationals*. $\mathbb{Q}(i)$ is the field of fractions of $\mathbb{Z}[i]$.

Remark. $1, -1, i$ and $-i$ are the units of $\mathbb{Z}[i], \mathbb{Q}(i), \mathbb{Z}[i][X], \mathbb{Q}(i)[X]$ and Int($\mathbb{Z}[i]$).

$\mathbb{Z}[i]$ is a Euclidean domain, with Euclidean function $f(a + bi) = a^2 + b^2$. So $\mathbb{Z}[i]$ is an integral domain and Int($\mathbb{Z}[i]$) is well-defined.

4.1. **Construction of Basis.** We know that the binomial polynomials form a basis for Int($\mathbb{Z}$). This leaves us to contemplate whether Int($\mathbb{Z}[i]$) has a basis of similar form. Moreover, if there really exists a basis for Int($\mathbb{Z}[i]$), what are the leading coefficients of the terms of basis? To answer these questions, it makes sense for us to consider the set of leading coefficients of polynomials of degree n within Int($\mathbb{Z}[i]$).

Lemma 2. For each non-negative $n \in \mathbb{Z}$, let R_n be the union of 0 and the set of leading coefficients of polynomials of degree n in Int($\mathbb{Z}[i]$), i.e.

$R_n = \{r \in \mathbb{Q}(i) : rX^n + r_{n-1}X^{n-1} + \cdots + r_0 \in \text{Int}(\mathbb{Z}[i]) \text{ for some } r_0, \ldots, r_{n-1} \in \mathbb{Q}(i)\}$

Then $\mathbb{Z}[i] = R_0 \subset R_1 \subset \cdots \subset R_p \subset R_{p+1} \subset \cdots \subset \mathbb{Q}(i)$ and $R_pR_q \subset R_{p+q}$ for all $p, q \in \mathbb{N}$.

Proof. By definition, $R_n \subset \mathbb{Q}(i)$. When $n = 0$, $R_n = \{r \in \mathbb{Q}(i) : r \in \text{Int}(\mathbb{Z}[i])\} = \mathbb{Z}[i]$.

Let $r \in R_p$. Then there is an integer-valued polynomial f of degree p whose leading coefficient is r. Xf is also an integer-valued polynomial. Xf has degree $p + 1$ and leading coefficient r , so $r \in R_{p+1}$. R_p is a subset of R_{p+1}.

Let $s \in R_q$. There is an integer-valued polynomial g of degree q whose leading coefficient is s. Then fg is an integer-valued polynomial of degree $p + q$ and with leading coefficient rs. It follows that R_pR_q is a subset of R_{p+q}. □

Obviously, each R_n is additive group. In Int($\mathbb{Z}$), R_n is generated by $(n!)^{-1}$ and $n!R_n = \mathbb{Z}$. In Int($\mathbb{Z}[i]$), this is obviously not the case for all n, but we can achieve something similar. To do this, we need the following lemma:

Lemma 3. Let $y_0, \ldots, y_n \in \mathbb{C}$. There exists a unique polynomial $f \in \mathbb{C}[X]$ with degree n such that $f(j) = y_j$ for $j = 0, 1, \ldots, n$. Moreover, we can write

$$f = N = \sum_{j=0}^{n} \left(\sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} y_k \right) \binom{X}{j}$$

Proof. Suppose two such polynomials $f \neq g$ exist. $f - g$ has at most degree n, so $f - g$ has at most n roots. However, $f(j) = g(j) = y_j$ and $(f - g)(j) = 0$ for $j = 0, 1, \ldots, n$. We arrive at a contradiction. So if it exists, the polynomial is unique.

Now it suffices for us to check that $N(m) = y_m$ for $m = 0, 1, \ldots n$.

$$\begin{aligned}
N(m) &= \sum_{j=0}^{n} \left(\sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} y_k \right) \binom{m}{j} \\
&= \sum_{j=0}^{n} \sum_{k=0}^{j} (-1)^{j-k} \frac{m(m-1)\ldots(m-j+1)}{k!(j-k)!} y_k \\
&= \sum_{k=0}^{n} \left(\sum_{j=k}^{n} (-1)^{j-k} \frac{m(m-1)\ldots(m-j+1)}{k!(j-k)!} \right) y_k \\
&= \sum_{k=0}^{n} \left(\sum_{j=0}^{n-k} (-1)^{j} \frac{m(m-1)\ldots(m-j-k+1)}{j!\,k!} \right) y_k \\
&= \sum_{k=0}^{m} \left(\sum_{j=0}^{m-k} (-1)^{j} \frac{m(m-1)\ldots(m-j-k+1)}{j!\,k!} \right) y_k \\
&= y_m + \sum_{k=0}^{m-1} \frac{(m-k)!}{k!} m \ldots (m-k+1) \left(\sum_{j=0}^{m-k} (-1)^{j} \binom{m-k}{j} \right) y_k \\
&= y_m + \sum_{k=0}^{m-1} \frac{(m-k)!}{k!} m \ldots (m-k+1)(1-1)^{m-k} y_k \\
&= y_m
\end{aligned}$$

□

With this, we can show that $n!R_n \subset \mathbb{Z}[i]$.

Lemma 4. Let $n \in \mathbb{Z}$ be non-negative. There exists $a \in \mathbb{Z}[i] \setminus \{0\}$ such that $aR_n \subset \mathbb{Z}[i]$.

Proof. Consider aR_n when $a = n!$. From previous result, a polynomial $f \in \mathrm{Int}(\mathbb{Z}[i])$ of degree n is uniquely determined by the values $f(0), f(1), \ldots, f(n)$:

$$f = \sum_{j=0}^{n} \left(\sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} f(k) \right) \binom{X}{j}$$

The leading coefficient of f is $\dfrac{1}{n!} \displaystyle\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$. $\binom{n}{k}$ is always a rational integer and $f(k)$ is by definition a Gaussian integer. So the leading coefficient of $n!f$ is a Gaussian integer. It follows that $n!R_n \subset \mathbb{Z}[i]$. □

In fact, we can establish a stronger relation between aR_n and $\mathbb{Z}[i]$.

Lemma 5. Let $n \in \mathbb{Z}$ be non-negative and let $a \in \mathbb{Z}[i]$. If $aR_n \subset \mathbb{Z}[i]$, then $aR_n \lhd \mathbb{Z}[i]$.

Proof. Let $q, r \in R_n$. Then there is some f, g with degree n and leading coefficients q, r respectively such that $f, g \in \mathrm{Int}(\mathbb{Z}[i])$. If q, r are distinct, $f + g \in \mathrm{Int}(\mathbb{Z}[i])$ has degree n and leading coefficient $q + r$. So R_n is closed under addition. Moreover, additive identity 0 and additive inverse $-r$ belong inside R_n. Thus, R_n is an additive subgroup of $\mathbb{Z}[i]$. Lastly, for all $s \in \mathbb{Z}[i]$, $sf \in \mathrm{Int}(\mathbb{Z}[i])$ with degree n and leading coefficient rs, so $rs \in R_n$. □

We have created an ideal of $\mathbb{Z}[i]$. The next logical step would be to use the fact that $\mathbb{Z}[i]$ is a principal ideal domain.

Lemma 6. $R_n = a_n\mathbb{Z}[i]$ for some $a_n^{-1} \in \mathbb{Z}[i]$. In fact, a_n^{-1} divides $n!$.

Proof. $\mathbb{Z}[i]$ is a principal ideal domain, so since there is non-zero $aR_n \lhd \mathbb{Z}[i]$, $aR_n = (b) = b\mathbb{Z}[i]$ for some $b \in \mathbb{Z}[i]$. By taking $a_n = ba^{-1}$, $a_n \in \mathbb{Q}(i)$ and $R_n = a_n\mathbb{Z}[i]$. Since $X^n \in \mathrm{Int}(\mathbb{Z}[i])$ and $1 \in R_n$, $a_n^{-1} \in \mathbb{Z}[i]$. Lastly, $a_n n!\mathbb{Z}[i] = n!R_n \subset \mathbb{Z}[i]$, so $a_n n! \in \mathbb{Z}[i]$. □

Using this result and polynomial reduction, we can prove that $\mathrm{Int}(\mathbb{Z}[i])$ does in fact have a basis.

Theorem 1. There is a set of polynomials $f_0, f_1, \ldots$, with each f_j having degree j and leading coefficient a_j, that forms a basis of $\mathrm{Int}(\mathbb{Z}[i])$.

Proof. Let $f_n \subset \mathrm{Int}(\mathbb{Z})$ for $n = 0, 1, \ldots$ be a set of polynomials where the degree of each f_n is n and the leading coefficient is a_n. By observation, each f_n has a different degree of polynomial, so they must be linearly independent. Next, let g be an integer-valued polynomial with degree m. It is possible to find $b_m \in \mathbb{Z}[i]$ such that $g - b_m f_m$ has degree $m-1$, since $R_n = a_n\mathbb{Z}[i]$. Repeat the process and we have $g = b_m f_m + \cdots + b_0 f_0$. □

4.2. **Ring structure.** We use similar methods as in $\mathrm{Int}(\mathbb{Z})$ to prove some properties that $\mathrm{Int}(\mathbb{Z}[i])$ has as a ring. The first thing is to prove that $\mathrm{Int}(\mathbb{Z}[i])$ is not Noetherian, we need to construct a strictly increasing chain of ideals. However, $\binom{X}{n} \notin \mathrm{Int}(\mathbb{Z}[i])$ for $n > 2$. We overcome this fact by considering $f = \frac{1}{p}\left(X^{p^2} - X\right)(X^p - X) \in \mathrm{Int}(\mathbb{Z}[i])$ for positive rational Gaussian prime p instead.

Lemma 7. There are infinitely many Gaussian primes which are integers.

Proof. Let p be prime in $\mathbb{Z}$. If $p = a^2 + b^2$ for some non-zero $a, b \in \mathbb{Z}$, then $p = (a + bi)(a - bi)$ and so p is not irreducible and not prime in $\mathbb{Z}[i]$. On the other hand, if p is not prime in $\mathbb{Z}[i]$, then $p = uv$ for some non-units $u, v \in \mathbb{Z}[i]$. Taking norms, $p^2 = |u|^2|v|^2$. Since u and v are not units, $|u|^2 = |v|^2 = |p|$. By taking $u = a + ib$, we have $|p| = |u|^2 = a^2 + b^2$. So p is prime in $\mathbb{Z}[i]$ if and only if $|p| \neq a^2 + b^2$ for all non-zero $a, b \in \mathbb{Z}$.

If $|p| \equiv 3 \pmod 4$, then $|p| \neq a^2 + b^2$ for all $a, b \in \mathbb{Z} \setminus \{0\}$, since a square mod 4 can only be 0 or 1. Thus it suffices to show that there are infinitely many primes in the form $4k + 3$ where k is non-negative.

Suppose we have a list of positive primes $p_1, \ldots, p_m$ such that each $p_i \equiv 3 \pmod 4$. Consider $4p_1 \ldots p_m - 1$. Note that if $q \equiv 3 \pmod 4$ then q has at least one prime factor $p \equiv 3 \pmod 4$, and that $4p_1 \ldots p_m - 1$ is not divisible by $p_1, \ldots, p_m$. So we have found another prime p_{m+1} in the form $4k + 3$ that is not on our list. By repeating this process, we construct a set of infinitely many Gaussian primes. □

Lemma 8. Let p be an odd prime with $p > 0$ and $p \equiv 3 \pmod 4$. Then the polynomial $f = \frac{1}{p}\left(X^{p^2} - X\right)(X^p - X) \in \mathrm{Int}(\mathbb{Z}[i])$.

Proof. Let $a, b \in \mathbb{Z}$.

$$\begin{aligned}
f(a+bi) &= \frac{1}{p}\left((a+bi)^{p^2} - (a+bi)\right)\left((a+bi)^p - (a+bi)\right) \\
&= \frac{1}{p}\left(\sum_{j=0}^{p^2}\binom{p^2}{j}a^{p^2-j}(bi)^j - a - bi\right)\left(\sum_{j=0}^{p}\binom{p}{j}a^{p-j}(bi)^j - a - bi\right) \\
&= \frac{1}{p}\left(a^{p^2} + (bi)^{p^2} - a - bi\right)(a^p + (bi)^p - a - bi) \\
&\quad + \frac{1}{p}\left(a^{p^2} + (bi)^{p^2} - a - bi\right)\sum_{j=1}^{p-1}\binom{p}{j}a^{p-j}(bi)^j \\
&\quad + \frac{1}{p}(a^p + (bi)^p - a - bi)\sum_{j=1}^{p^2-1}\binom{p^2}{j}a^{p^2-j}(bi)^j \\
&\quad + \frac{1}{p}\sum_{j=1}^{p-1}\binom{p}{j}a^{p-j}(bi)^j\sum_{j=1}^{p^2-1}\binom{p^2}{j}a^{p^2-j}(bi)^j
\end{aligned}$$

The latter three terms are Gaussian integers, since p divides $\binom{p}{j}$ for $j = 1, \ldots, p-1$. Next, since $p \equiv 3 \pmod 4$, $(bi)^p - bi = i(b^p - b)$. By Fermat's little theorem, p divides $a^p - a$ and $b^p - b$, so the first term in the equality is also a Gaussian integer. $f(a + bi) \in \mathbb{Z}[i]$ and so $f \in \mathrm{Int}(\mathbb{Z}[i])$. □

We use functions in this form to construct a strictly increasing chain of ideals, which proves that $\mathrm{Int}(\mathbb{Z}[i])$ is non-Noetherian.

Theorem 2. $\mathrm{Int}(\mathbb{Z}[i])$ is not Noetherian.

Proof. Let $p_1, p_2, \ldots$ be Gaussian primes which are positive rational integers. For each $n > 0$, let $f_n = \dfrac{1}{p_n}\left(X^{p_n^2} - X\right)(X^{p_n} - X)$ and let $\mathfrak{I}_n = (f_1, \ldots, f_n) \lhd \mathrm{Int}(\mathbb{Z}[i])$. Fix $n > 0$ and suppose $f_{n+1} \in \mathfrak{I}_n$. We can write

$$f_{n+1}(x) = \frac{g_1(x)}{m_1} f_1(x) + \cdots + \frac{g_n(x)}{m_n} f_n(x)$$

where each $g_j \in \mathbb{Z}[i][X]$ and $m_j \in \mathbb{N}$. Define $a_j = g_j(0)$ for $j = 1, \ldots, n$.

The coefficient of x^2 in $f_{n+1}(x)$ is $\dfrac{1}{p_{n+1}}$ and the coefficient of x^2 in $\dfrac{g_j(x)}{m_j} f_j(x)$ is $\dfrac{a_j}{m_j p_j}$. By comparing the coefficients of x^2 on both sides, we have

$$\frac{1}{p_{n+1}} = \frac{a_1}{m_1 p_1} + \cdots + \frac{a_n}{m_n p_n}$$

For each j, $a_j = g_j(0)$ and $\dfrac{g_j}{m_j} \in \mathrm{Int}(\mathbb{Z}[i])$. So $g_j \in m_j \,\mathrm{Int}(\mathbb{Z}[i])$ and $a_j \in m_j \mathbb{Z}[i]$. In other words, there exists $b_j \in \mathbb{Z}[i]$ such that $a_j = m_j b_j$.

$$\frac{1}{p_{n+1}} = \frac{b_1}{p_1} + \cdots + \frac{b_n}{p_n}$$

p_{n+1} does not divide $p_1 \ldots p_n$, so we arrive at a contradiction. It follows that $f_{n+1} \notin \mathfrak{I}_n$, $\mathfrak{I}_{n+1} \neq \mathfrak{I}_n$ for all $n > 0$, and $\mathfrak{I}_1 \subset \mathfrak{I}_2 \subset \ldots$ is a strictly increasing chain of ideals in $\mathrm{Int}(\mathbb{Z}[i])$. $\mathrm{Int}(\mathbb{Z}[i])$ is not Noetherian. □

Theorem 3. $\mathrm{Int}(\mathbb{Z}[i])$ satisfies the ascending chain condition on principal ideals.

Proof. The proof is same as in $\mathrm{Int}(\mathbb{Z})$ except we take $a_1, a_2, \cdots \in \mathrm{Int}(\mathbb{Z}[i])$. □

We follow the other chain of class inclusions. Observe that for **Proposition 9**, the only property of $\mathbb{Z}$ that is relevant to the proof is that it is integrally closed. $\mathbb{Z}[i]$ is also integrally closed (it is a GCD domain) and it is a subset of $\mathbb{C}$, so the fundamental theorem of algebra can be applied here.

Theorem 4. $\mathrm{Int}(\mathbb{Z}[i])$ is an integrally closed domain.

Proof. Let $f \in \mathbb{Q}[i](X)$ be non-zero and integral over $\mathrm{Int}(\mathbb{Z}[i])$, i.e.

$$f^n + g_{n-1} f^{n-1} + \cdots + g_1 f + g_0 = 0$$

where $g_j \in \mathrm{Int}(\mathbb{Z}[i])$ for $j = 0, 1, \ldots, n-1$. We can write $f = \dfrac{a}{b}$ where $a, b \in \mathbb{Z}[i][X]$ are non-zero and have no common factors. Then,

$$a^n + g_{n-1} a^{n-1} b + \cdots + g_1 a b^{n-1} + g_0 b^n = 0$$

Since a and b have no common factors in $\mathbb{Z}[i][X]$, by fundamental theorem of algebra, we can find $\alpha \in \mathbb{C}$ such that $b(\alpha) = 0$ but $a(\alpha) \neq 0$.

$$\begin{aligned}(a^n + g_{n-1}a^{n-1}b + \cdots + g_1ab^{n-1} + g_0b^n)(\alpha) &= 0\\ a^n(\alpha) + g_{n-1}(\alpha)a^{n-1}(\alpha)b(\alpha) + \cdots + g_1(\alpha)a(\alpha)b^{n-1}(\alpha) + g_0(\alpha)b^n(\alpha) &= 0\\ a^n(\alpha) &= 0\end{aligned}$$

We arrive at a contradiction. It follows that b must be constant and so $f \in \mathbb{Z}[i][X]$. For all $a \in \mathbb{Z}[i]$, we have

$$f^n(a) + g_{n-1}(a)f^{n-1}(a) + \cdots + g_1(a)f(a) + g_0(a) = 0$$

So $f(a)$ is integral over $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is integrally closed, $f(a) \in \mathbb{Z}[i]$ for all $a \in \mathbb{Z}$ and so $f \in \mathrm{Int}(\mathbb{Z}[i])$. □

To prove that $\mathrm{Int}(\mathbb{Z}[i])$ is not a GCD domain, it suffices to find an element that is irreducible but not prime. This is not difficult:

Lemma 9. $\frac{1}{2}(i+1)X(X-1)$ is irreducible in $\mathrm{Int}(\mathbb{Z}[i])$.

Proof. Let $r = a + bi$ where $a, b \in \mathbb{Z}$.

$$\begin{aligned}\frac{1}{2}(i+1)r(r-1) &= \frac{1}{2}(1+i)(a+bi)(a-1+bi)\\ &= \frac{1}{2}(a^2 - 2ab - a - b^2 + b) + \frac{1}{2}(a^2 + 2ab - a - b^2 + b)i\end{aligned}$$

$a^2 - a$ and $b^2 - b$ are products of two consecutive integers. Thus $a^2 - 2ab - a - b^2 + b$ and $a^2 + 2ab - a - b^2 + b$ are always even and $\frac{1}{2}(i+1)X(X-1) \in \mathrm{Int}(\mathbb{Z}[i])$. By careful observation, $\frac{1}{2}(i+1)$ is not a Gaussian integer and $kX, k(X+1) \in \mathrm{Int}(\mathbb{Z}[i])$ if and only if $k \in \mathbb{Z}[i]$. It follows that $\frac{1}{2}(i+1)X(X-1)$ cannot be expressed as the product of two or more non-units and thus it is irreducible in $\mathrm{Int}(\mathbb{Z}[i])$. □

Theorem 5. $\mathrm{Int}(\mathbb{Z}[i])$ is not a GCD domain.

Proof. In a GCD domain, an element is prime if and only if it is irreducible. $\frac{1}{2}(i+1)X(X-1)$ is irreducible and divides $X(X-1)$, but it does not divide X or $X-1$. $\frac{1}{2}(i+1)X(X-1)$ is irreducible but not prime in $\mathrm{Int}(\mathbb{Z}[i])$, so $\mathrm{Int}(\mathbb{Z}[i])$ is not a GCD domain. □

Corollary 2. $\mathrm{Int}(\mathbb{Z}[i])$ is not a unique factorization domain, a principal ideal domain or a Euclidean domain.

5. Continuous Functions on Rational Integers

Another avenue of further investigation is to include integer-valued functions other than polynomials. Since all polynomials are continuous, it makes sense to consider the set of integer-valued continuous functions. For example, $\sin(\pi X)$ is one such function.

Definition (Continuous function)**.** $f : \mathbb{R} \to \mathbb{R}$ is a *continuous function* if at every $a \in \mathbb{R}$, for all $\epsilon > 0$ there exists $\delta > 0$ such that $|f(x) - f(a)| < \epsilon$ whenever $a - \delta < x < a + \delta$.

Definition (Kernel)**.** Let $f : \mathbb{R} \to \mathbb{R}$. The kernel of f, written $\ker(f)$, is the set $\{a \in \mathbb{R} : f(a) = 0\}$.

In general, the sum, product and composition of any two continuous functions is continuous, and the quotient of two continuous functions, if well-defined on $\mathbb{R}$, is also continuous. A sufficient (but not necessary) condition for the quotient to be well-defined is the kernel of the divisor is empty.

Definition (Integer-valued continuous function)**.** Let $f : \mathbb{R} \to \mathbb{R}$ be a function. f is an *integer-valued continuous function* if f is continuous and $f(\mathbb{Z}) \subset \mathbb{Z}$.

Proposition 10. The set of integer-valued continuous functions $\mathbb{R} \to \mathbb{R}$ on the rational integers forms a ring. We denote this ring by $C(\mathbb{Z})$.

Proof. Obviously, addition is associative, commutative and distributive over multiplication, and multiplication is associative. Also, $0, 1 \in C(\mathbb{Z})$ and $-f \in C(\mathbb{Z})$ if $f \in C(\mathbb{Z})$. Let $f, g \in C(\mathbb{Z})$. $f + g$ and fg are also continuous functions. We have $(f+g)(\mathbb{Z}) \subset f(\mathbb{Z})+g(\mathbb{Z}) \subset \mathbb{Z}$. Similarly, $(fg)(\mathbb{Z}) \subset f(\mathbb{Z})g(\mathbb{Z}) \subset \mathbb{Z}$. $f+g, fg \in C(\mathbb{Z})$, the set is closed under multiplication and addition. □

We have thus verified that $C(\mathbb{Z})$ is a ring. In fact, it is not difficult to observe that $C(\mathbb{Z})$ is an overring of $\mathrm{Int}(\mathbb{Z})$. Since this ring includes elements other than polynomials, it may be interesting for us to investigate the units, associates, factors and irreducibles.

Proposition 11. Let $f \in C(\mathbb{Z})$. f is a unit if and only if $f(\mathbb{Z}) = \{1\}$ or $\{-1\}$ and $\ker(f) = \emptyset$.

Proof. f is a unit if and only if there exists $g \in C(\mathbb{Z})$ such that $fg = 1$. $f(z)g(z) = 1$ for all $z \in \mathbb{Z}$, so it follows that $f(\mathbb{Z}) = \{1, -1\}$. Moreover, $f(r)g(r) = 1$ for all $r \in \mathbb{R}$. Since f, g must be continuous, $f(r), g(r) \neq 0$. In other words, $\ker(f)$ is empty. Lastly, by the intermediate value theorem, if $f(a) = 1$ and $f(b) = -1$ for some $a, b \in \mathbb{Z}$, then f has a root, which contradicts $\ker(f) = \emptyset$. Thus $f(\mathbb{Z}) = \{1\}$ or $\{-1\}$. □

Proposition 12. Let $f, g \in C(\mathbb{Z})$. If f and g are associates, then $\ker(f) = \ker(g)$ and $f(z) = g(z)$ for all $z \in \mathbb{Z}$ or $f(z) = -g(z)$ for all $z \in \mathbb{Z}$.

Proof. If f and g are associates, then $f = gh$ for some unit $h \in C(\mathbb{Z})$. By **Proposition 11**, $h(\mathbb{Z}) = \{1\}$ or $\{-1\}$ and $\ker(h) = \emptyset$. We then have $\ker(f) = \ker(gh) = \ker(g)$. Lastly, $f(z) = g(z)h(z)$ for all $z \in \mathbb{Z}$, which means $f(z) = g(z)$ for all $z \in \mathbb{Z}$ or $f(z) = -g(z)$ for all $z \in \mathbb{Z}$. □

However, the converse of this statement is not true: consider $f(x) = |x|$ for $-1 < x < 1$ and $f(x) = 1$ otherwise and $g(x) = \sqrt{|x|}$ for $-1 < x < 1$ and $g(x) = 1$ otherwise. $\ker(f) = \ker(g) = \{0\}$ and $f(z) = g(z)$ for all $z \in \mathbb{Z}$. But $\dfrac{f}{g}$ is not a unit and $\dfrac{g}{f}$ is not continuous, so f and g are not associates.

Lemma 10. Let $f, g \in C(\mathbb{Z})$. If g divides f, then $\ker(g) \subset \ker(f)$ and $g(z) \mid f(z)$ for all $z \in \mathbb{Z}$ and $z \notin \ker(g)$.

Proof. Let $g \mid f$. $f = gh$ for some $h \in C(\mathbb{Z})$. For all $z \in \mathbb{Z}$, $f(z) = g(z)h(z)$, so $g(z) \mid f(z)$ if $g(z) \neq 0$. Moreover, if $g(a) = 0$, then $f(a) = g(a)h(a) = 0$, so $\ker(g) \subset \ker(f)$. □

Lemma 11. Let $f, g \in C(\mathbb{Z})$. If $\ker(g)$ is empty and $g(z)$ divides $f(z)$ for all $z \in \mathbb{Z}$, then g divides f.

Proof. Let $h = \dfrac{f}{g}$. Then $h(z) = \dfrac{f(z)}{g(z)}$ for all $z \in \mathbb{Z}$. $g(z)$ divides $f(z)$, so h is integer-valued. Next, since $\ker(g)$ is empty, $\dfrac{f}{g}$ is well-defined and continuous. Thus $h \in C(\mathbb{Z})$, $f = gh$ and g divides f. □

Using this lemma, we can find functions that, excluding associates, has infinitely many factors. In the following theorem, we give an example of such a function and use it to prove that $C(\mathbb{Z})$ does not satisfy the ACCP.

Theorem 6. $C(\mathbb{Z})$ does not satisfy the ascending chain condition on principal ideals.

Proof. Let $f_0, f_1, \cdots \in C(\mathbb{Z})$ with the following:

$$f_0(x) = 2, f_n(x) = \begin{cases} 2 & \text{for } x \leq 0 \text{ or } x \geq n+1 \\ 2-x & \text{for } 0 < x < 1 \\ 1 & \text{for } 1 \leq x \leq n \\ x-n+1 & \text{for } n < x < n+1 \end{cases} \qquad \text{for } n = 1, 2, \ldots$$

For each n, $f_n \in C(\mathbb{Z})$ and $f_n \mid f_{n-1}$. The chain of principal ideals $(f_0) \subset (f_1) \subset \ldots$ is non-terminating. □

Corollary 3. $C(\mathbb{Z})$ is not Noetherian.

Now we turn our attention to irreducible elements. We find a necessary and sufficient condition for an element in $C(\mathbb{Z})$ to be irreducible. This includes conditions on the kernel of the function and the values that it can take.

Lemma 12. Let $f \in C(\mathbb{Z})$. If $\ker(f)$ is not empty, then f is not irreducible.

Proof. Let $f(a) = 0$. Define functions g, h with the following: If there exists $b > a$ such that $|f(b)| = 1$ and $|f(x)| < 1$ for $x \in (a, b)$, then let $g(x) = 1$ and $h(x) = f(x)$ for $x > b$. Similarly, if there exists $c < a$ such that $|f(c)| = 1$ and $|f(x)| < 1$ for $x \in (c, a)$, then let $g(x) = 1$ and $h(x) = f(x)$ for $x < c$. Lastly, for the remaining values, let $g(x) = \sqrt{|f(x)|}$ and $h(x) = \operatorname{sgn}(f(x))\sqrt{|f(x)|}$.

One can verify that g, h are continuous and take integer values on integer points. Moreover, since $g(a) = h(a) = 0$, $\ker(g), \ker(h)$ are non-empty and thus g, h are not units. $f = gh$, so f is not irreducible. □

Lemma 13. Let $f \in C(\mathbb{Z})$. If $|f(z)| \neq 1$ is composite for some $z \in \mathbb{Z}$, then f is not irreducible.

Proof. Let $f(z) = pq$ for some non-units $p, q \in \mathbb{Z}$. Assume without loss of generality that $p > 0$. Let g such that

$$g(x) = \begin{cases} 1 & \text{for } x < z-1 \text{ or } x > z+1 \\ p + (p-1)(x-z) & \text{for } z-1 \leq x \leq z \\ p + (1-p)(x-z) & \text{for } z < x \leq z+1 \end{cases}$$

Obviously, $g \in C(\mathbb{Z})$ is not a unit and $h = \dfrac{f}{g} \in C(\mathbb{Z})$. Moreover, $h(z) = q$ is not a unit in $\mathbb{Z}$, so h is not a unit in $C(\mathbb{Z})$. Since $f = gh$, f is not irreducible. □

Lemma 14. Let $f \in C(\mathbb{Z})$. If $|f(a)|, |f(b)| \neq 1$ for some distinct $a, b \in \mathbb{Z}$, then f is not irreducible.

Proof. If $f(a) = 0$, then f is not irreducible by **Lemma 12**.

If $f(a) > 0$, let g such that

$$g(x) = \begin{cases} 1 & \text{for } x < a-1 \text{ or } x > a+1 \\ f(a) + (f(a)-1)(x-a) & \text{for } a-1 \leq x \leq a \\ f(a) + (1-f(a))(x-a) & \text{for } a < x \leq a+1 \end{cases}$$

If instead $f(a) < 0$, let

$$g(x) = \begin{cases} -1 & \text{for } x < a-1 \text{ or } x > a+1 \\ -f(a) - (f(a)-1)(x-a) & \text{for } a-1 \leq x \leq a \\ -f(a) - (1-f(a))(x-a) & \text{for } a < x \leq a+1 \end{cases}$$

Obviously, $g \in C(\mathbb{Z})$ is not a unit and $h = \dfrac{f}{g} \in C(\mathbb{Z})$. Moreover, $h(b)$ is not a unit in $\mathbb{Z}$, so h is not a unit in $C(\mathbb{Z})$. Since $f = gh$, f is not irreducible. □

Proposition 13. Let $f \in C(\mathbb{Z})$. f is irreducible if and only if $\ker(f)$ is empty and for some $a \in \mathbb{Z}$, $f(\mathbb{Z} \setminus \{a\}) = \{1\}$ or $\{-1\}$ and $f(a)$ is prime in $\mathbb{Z}$.

Proof. By **Lemmas 12, 13 and 14**, f is irreducible only if $\ker(f)$ is empty and for some $a \in \mathbb{Z}$, $f(\mathbb{Z} \setminus \{a\}) = \{1\}$ or $\{-1\}$ and $f(a)$ is prime in $\mathbb{Z}$.

Now suppose $\ker(f)$ is empty and for some $a \in \mathbb{Z}$, $f(\mathbb{Z} \setminus \{a\}) = \{1\}$ and $f(a)$ is prime in $\mathbb{Z}$. Suppose that f is not irreducible, i.e. $f = gh$ for some non-units g, h. $\ker(g), \ker(h) \subset \ker(f) = \emptyset$, so $\ker(g), \ker(h)$ are also empty. By **Lemma 10**, for all $z \in \mathbb{Z}$ and $z \neq a$, $g(z)h(z) = f(z) = 1$, so $g(\mathbb{Z} \setminus \{a\}), h(\mathbb{Z} \setminus \{a\}) \subset \{-1, 1\}$. Given that $\ker(g) = \ker(h) = \emptyset$, by intermediate value theorem, we have $g(\mathbb{Z} \setminus \{a\}) = h(\mathbb{Z} \setminus \{a\}) = \{1\}$ or $g(\mathbb{Z} \setminus \{a\}) = h(\mathbb{Z} \setminus \{a\}) = \{-1\}$. Assume, WLOG, that it is the former. Since $f(a) = g(a)h(a)$ is prime and irreducible in $\mathbb{Z}$, either $g(a) = f(a)$ and $h(a) = 1$ or $g(a) = 1$ and $h(a) = f(a)$. In both cases, it contradicts g, h being non-units. So f is irreducible.

If instead $f(\mathbb{Z} \setminus \{a\}) = \{-1\}$ and $f(a) < 0$, we arrive at a similar result. Either $g(\mathbb{Z} \setminus \{a\}) = \{1\}$ and $h(\mathbb{Z} \setminus \{a\}) = \{-1\}$ or $g(\mathbb{Z} \setminus \{a\}) = \{-1\}$ and $h(\mathbb{Z} \setminus \{a\}) = \{1\}$.

In the first case, either $g(a) = -f(a)$ and $h(a) = -1$ or $g(a) = 1$ and $h(a) = f(a)$. In the second case, either $g(a) = f(a)$ and $h(a) = 1$ or $g(a) = -1$ and $h(a) = f(a)$. These all contradict g, h being non-units. f is irreducible.

Thus, if $\ker(f)$ is empty and for some $a \in \mathbb{Z}$, $f(\mathbb{Z} \setminus \{a\}) = \{1\}$ or $\{-1\}$ and $f(a)$ is prime in $\mathbb{Z}$, then f is irreducible. □

Some elements cannot be expressed as a product of irreducibles and $C(\mathbb{Z})$ is not a UFD.

Theorem 7. $C(\mathbb{Z})$ is not a unique factorization domain.

Proof. If f is the product of n irreducible elements, then $f(\mathbb{Z} \setminus S) = \{1\}$ or $\{-1\}$ for some finite set $S \subset \mathbb{Z}$ with $|S| \leq n$. As such, any nonzero constant non-unit function cannot be factorized into a product of irreducibles. It follows that $C(\mathbb{Z})$ is not a UFD. □

6. Discussion

In this paper, we have shown that $\mathrm{Int}(\mathbb{Z}[i])$ has a basis, is integrally closed and non-Noetherian, satisfies the ACCP, but is not a GCD domain; and that $C(\mathbb{Z})$ does not satisfy the ACCP and is not a UFD. Our results lead us to question whether these properties hold for different but similarly defined rings:

6.1. **Polynomials on Algebraic Integers.** What if we consider polynomials on rings of algebraic integers $\mathbb{Z}[a]$ other than $\mathbb{Z}$ and $\mathbb{Z}[i]$? In particular, $\mathbb{Z}[a] = \{r_0 + r_1 a + \cdots + r_{n-1}a^{n-1} : r_0, \ldots, r_{n-1} \in \mathbb{Z}\}$ where $a \in \mathbb{C}$ is the root of some degree n monic polynomial with coefficients in $\mathbb{Z}$. One would expect that as a ring $\mathrm{Int}(\mathbb{Z}[a])$ has the same properties as $\mathrm{Int}(\mathbb{Z}[i])$ and $\mathrm{Int}(\mathbb{Z})$. We have the following propositions:

Proposition 14. $\mathrm{Int}(\mathbb{Z}[a])$ has a basis.

Proof. (Outline) Similar to **Theorem 1**, we can show that the union of zero and the set of leading coefficients of degree n polynomials is equal $b_n\mathbb{Z}[a]$ for some $b_n^{-1} \in \mathbb{Z}[a]$, so $\mathrm{Int}(\mathbb{Z}[a])$ is generated by a set of polynomials $f_0, f_1, \ldots$ where each $\deg f_j = j$ and b_n is the leading coefficient of f_j. □

Proposition 15. $\mathrm{Int}(\mathbb{Z}[a])$ satisfies the ascending chain condition on principal ideals.

Proof. Polynomials have a finite number of factors and $(b) \subset (c)$ if and only if b divides c, so every increasing chain of principal ideals eventually stabilizes. □

Proposition 16. $\mathrm{Int}(\mathbb{Z}[a])$ is an integrally closed domain.

Proof. (Outline) $\mathbb{Z}[a]$ is a subset of $\mathbb{C}$ and so the fundamental theorem of algebra applies. Moreover, $\mathbb{Z}[a]$ is an integrally closed domain, so by following the same steps as the proofs of **Proposition 9** and **Theorem 4**, we arrive at our desired result. □

We also make the following claims:

Claim 1. $\mathrm{Int}(\mathbb{Z}[a])$ is non-Noetherian.

Claim 2. $\mathrm{Int}(\mathbb{Z}[a])$ is not a GCD domain.

It is harder to use similar methods as before to prove these claims. To address the first claim, we pose this question: is $f = p^{-1}(X^{p^2} - X)(X^p - X)$ an element of $\mathrm{Int}(\mathbb{Z}[a])$ for prime $p \in \mathbb{N}$? This may be difficult to determine since we need to consider the powers of the sum of more than two terms.

Next, for the second claim, we must contemplate how we can construct an element that is irreducible but not prime in $\mathrm{Int}(\mathbb{Z}[a])$? For example, if $a = \sqrt{2}$, then $\dfrac{X^2(X-1)}{2}$ is an irreducible element that is not prime, and if $a = \sqrt{d}$ for square-free $d > 0$, then $\dfrac{X^2(X-1)\dots(X-d+1)}{d}$ is irreducible and not prime. In fact, we have the following:

Lemma 15. If $f \in \mathrm{Int}(\mathbb{Z}[a])$ has degree $n > 2$, leading coefficient z^{-1} where $z \in \mathbb{Z}[a]$ is not a unit and zf has a factor g with $1 < \deg g < n$, then f is not prime.

Proof. $zf = gh$ where $h \in \mathrm{Int}(\mathbb{Z}[a])$ and $1 < \deg h < n$. f divides zf but does not divide g or h, since $\deg g, \deg h < n$. So f is not prime. □

If we can find an irreducible element f that satisfies this criteria, then we can prove that $\mathrm{Int}(\mathbb{Z}[a])$ is not a GCD domain.

6.2. **Continuously Differentiable Functions on Rational Integers.** On the other hand, what happens if, aside from continuity, we impose additional conditions on the integer-valued functions, such as differentiability? Let $C^n(\mathbb{Z})$ be the set of continuous integer-valued functions f such that the derivatives $f', f'', \dots, f^{(n)}$ exist and are continuous. Also let $C^\infty(\mathbb{Z})$ be the set of infinitely differentiable integer-valued functions with continuous derivatives. $C^\infty(\mathbb{Z})$ and each $C^n(\mathbb{Z})$ are rings and we have

$$C(\mathbb{Z}) = C^0(\mathbb{Z}) \supset C^1(\mathbb{Z}) \supset \cdots \supset C^n(\mathbb{Z}) \supset C^{n+1}(\mathbb{Z}) \supset \cdots \supset C^\infty(\mathbb{Z}) \supset \mathrm{Int}(\mathbb{Z})$$

Lemma 16. Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 1 + \exp\left(1 - \dfrac{1}{x(2-x)}\right)$ for $0 < x < 2$ and $f(x) = 1$ otherwise. Then $f \in C^\infty(\mathbb{Z})$.

Proof. If $a, b \in C^\infty(\mathbb{Z})$, then $a \circ b \in C^\infty(\mathbb{Z})$. Let $u(x) = \exp\left(-x^{-1}\right)$ for $x > 0$ and $u(x) = 0$ otherwise. u is infinitely continuously differentiable, so $f(x) = 1 + eu(x(2-x))$ is also infinitely continuously differentiable. Lastly, since $f(1) = 2$ and $f(z) = 1$ for all $z \in \mathbb{Z} \setminus \{1\}$, $f \in C^\infty(\mathbb{Z})$. □

With this we construct a set of functions $g_0, g_1, \dots \in C^\infty(\mathbb{Z})$ such that g_n divides g_m whenever $n < m$. As a result, we have the following propositions:

Proposition 17. $C^\infty(\mathbb{Z})$ and $C^n(\mathbb{Z})$ for $n \in \mathbb{N}$ do not satisfy the ascending chain condition on principal ideals.

Proof. Consider function $g(x) = f(x-2k)$ for $2k \leq x < 2k+2, k \in \mathbb{Z}$. For each non-negative integer n, let $g_n(x) = 1$ for $0 \leq x \leq 2n$ and $g_n(x) = g(x)$ otherwise. We have $g_0 = g$ and g_n divides g_m for all $n < m$. $(g) \subset (g_1) \subset \ldots$ is a strictly increasing chain of principal ideals. □

Corollary 4. $C^\infty(\mathbb{Z})$ and $C^n(\mathbb{Z})$ are not Noetherian.

Proposition 18. $C^\infty(\mathbb{Z})$ and $C^n(\mathbb{Z})$ are not unique factorization domains.

Proof. If $C^\infty(\mathbb{Z})$ is an UFD, then up to associates, $C^\infty(\mathbb{Z})$ has a finite number of factors, which is not the case for $g(x) = f(x-2k)$ for $2k \leq x < 2k+2, k \in \mathbb{Z}$. □

6.3. **Continuous Functions on Gaussian Integers.** Lastly, what happens if we consider the ring of continuous functions $\mathbb{C} \to \mathbb{C}$ which are integer-valued on the Gaussian integers $C(\mathbb{Z}[i])$? It is essentially a higher dimensional version of $C(\mathbb{Z})$, so one can imagine that they share similar properties with regards to its units, irreducibles and ring structure.

Proposition 19. The units of this ring are functions f such that $f(\mathbb{Z}[i]) \subset \{1, -1, i, -i\}$ and $\ker(f) = \emptyset$.

Proof. If f is a unit, then $fg = 1$ for some $g \in C(\mathbb{Z}[i])$ and $f(z)g(z) = 1$ for all $z \in \mathbb{Z}[i]$, which implies that $\ker(f) = \emptyset$ and $f(z) = 1, -1, i$ or $-i$ for all $z \in \mathbb{Z}[i]$. On the other hand, if $f(\mathbb{Z}[i]) \subset \{1, -1, i, -i\}$ and the kernel of f is empty, then $\dfrac{1}{f}$ is continuous and integer-valued on $\mathbb{Z}[i]$. □

Note that we cannot force f to map the Gaussian integers to exactly one of the units because the intermediate value theorem does not apply for functions on $\mathbb{C}$. Next, we find that **Lemmas 10 and 11** also apply for $C(\mathbb{Z}[i])$. In particular, to prove the following lemmas, we can simply follow the exact same line of argument as before.

Lemma 17. g divides f in $C(\mathbb{Z}[i])$ only if $\ker(g) \subset \ker(f)$ and $g(z) \mid f(z)$ for all $z \in \mathbb{Z}[i], z \notin \ker(g)$.

Proof. If $f = gh$ for some $h \in C(\mathbb{Z}[i])$, then $g(a) = 0$ implies $f(a) = g(a)h(a) = 0$ and $g(z)$ divides $g(z)h(z) = f(z)$ if $z \in \mathbb{Z}[i]$ and $g(z) \neq 0$. □

We have found a necessary condition for $g \mid f$ and we then state a sufficient condition.

Lemma 18. Let $f, g \in C(\mathbb{Z}[i])$. If $\ker(g)$ is empty and $g(z)$ divides $f(z)$ for all $z \in \mathbb{Z}[i]$, then g divides f.

Proof. $\ker(g)$ is empty, so $\dfrac{f}{g}$ must be continuous. $g(z)$ divides $f(z)$ for all $z \in \mathbb{Z}[i]$, so $\dfrac{f}{g}$ is integer-valued. $f = \dfrac{f}{g}g$ where $\dfrac{f}{g} \in C(\mathbb{Z}[i])$, so g divides f. □

With this we can again construct a strictly increasing chain of principal ideals.

Proposition 20. $C(\mathbb{Z}[i])$ does not satisfy the ascending chain condition on principal ideals.

Proof. Let $f_0, f_1, \cdots : \mathbb{R} \to \mathbb{R}$ with the following:

$$f_0(x) = 2, f_n(x) = \begin{cases} 2 & \text{for } x \leq 0 \text{ or } x \geq n+1 \\ 2-x & \text{for } 0 < x < 1 \\ 1 & \text{for } 1 \leq x \leq n \\ x-n+1 & \text{for } n < x < n+1 \end{cases} \quad \text{for } n = 1, 2, \ldots$$

We extend these functions to $g_0, g_1, \cdots : \mathbb{C} \to \mathbb{C}$ by taking $g_n(x) = f_n(\mathrm{Re}(x))$. For each n, $g_n \in C(\mathbb{Z}[i])$ and $g_n \mid g_{n-1}$. The chain of principal ideals $(g_0) \subset (g_1) \subset \ldots$ is non-terminating. □

Corollary 5. $C(\mathbb{Z}[i])$ is not Noetherian.

Lemma 19. Any function with non-empty kernel is not irreducible.

Proof. Let $f \in C(\mathbb{Z}[i])$ with $f(a) = 0$. Let $g(x) = \left|\sqrt{f(x)}\right|$ for $|f(x)| < 1$ and $g(x) = 1$ otherwise. Let $h(x) = 0$ for $f(x) = 0$ and $h(x) = \dfrac{f(x)}{g(x)}$ otherwise. g and h are continuous and integer-valued and $g(a) = h(a) = 0$, so g and h are non-units in $C(\mathbb{Z}[i])$. Thus $f = gh$ is not irreducible. □

Lemma 20. Let $f \in C(\mathbb{Z}[i])$. If $f(z)$ is composite in $\mathbb{Z}[i]$ for some $z \in \mathbb{Z}$, then f is not irreducible.

Proof. Let p be a proper factor of $f(z)$, i.e. p is not a unit or an associate of $f(z)$. Assume without loss of generality that $\mathrm{Re}(p) > 0$. Let $g(x) = |x - z|(1 - p) + p$ for $|x - z| < 1$ and $g(x) = 1$ otherwise. g is continuous, integer-valued and not a unit. Moreover, g divides f and g is not an associate of f since $g(z) = p$ is a proper factor of $f(z)$. So f is not irreducible. □

Lemma 21. Let $f \in C(\mathbb{Z}[i])$. If $f(a)$ and $f(b)$ are not units for distinct $a, b \in \mathbb{Z}[i]$, then f is not irreducible.

Proof. Let r be an associate of $f(a)$ with $\mathrm{Re}(r) > 0$. Let $g(x) = |x - a|(1 - r) + r$ for $|x - a| < 1$ and $g(x) = 1$ otherwise. $g, \dfrac{f}{g} \in C(\mathbb{Z}[i])$ where $g(a)$ and $\dfrac{f}{g}(b)$ are non-units. So f is not irreducible. □

Proposition 21. The irreducibles of this ring are functions with empty kernel which map one Gaussian integer to a Gaussian prime and all other Gaussian integers to the units $\{1, -1, i, -i\}$.

Proof. By **Lemmas 19, 20 and 21**, any irreducible f must have an empty kernel and if $f(a), f(b)$ are non-units for some $a, b \in \mathbb{Z}[i]$, then $a = b$ and $f(a)$ is a Gaussian prime. Moreover, since any irreducible must not be a unit, such a always exists.

On the other hand, if f has empty kernel and for some $a \in \mathbb{Z}[i]$, $f(a)$ is a Gaussian prime and $f(\mathbb{Z}[i] \setminus \{a\}) \subset \{1, -1, i, -i\}$. Now suppose $f = gh$. Then $\ker(g) = \ker(h) = \ker(f) = \emptyset$. Moreover, since $f(a)$ is prime, one of $g(a)$ and $h(a)$ is a unit and the other is an associate of $f(a)$. It follows that one of g and h is a unit and the other is an associate of f. f is irreducible. □

Proposition 22. $C(\mathbb{Z}[i])$ is not a unique factorization domain.

Proof. If f is the finite product of some irreducibles in $C(\mathbb{Z}[i])$, then $f(\mathbb{Z}[i] \setminus S) \subset \{1, -1, i, -i\}$ for some finite set S. Non-zero non-unit constant functions cannot be expressed as a finite product of irreducibles and so no unique factorization exists. It follows that $C(\mathbb{Z}[i])$ is not a UFD. □

References

[1] Artin, M. *Algebra*. Prentice-Hall, 1991
[2] Herstein, I.N. *Topics in Algebra*. John Wiley and Sons, 1975
[3] Fraleigh, J.B. *A First Course in Abstract Algebra*. Addison Wesley, 2003
[4] Cahen, P.J. and Chabert, J.L. *What You Should Know About Integer-Valued Polynomials*. The American Mathematical Monthly, 2016
[5] Marcus, D.A. *Number Fields*. Springer-Verlag, 1977
[6] Burkill, J.C. *A First Course in Mathematical Analysis*. Cambridge University Press, 1978

REVIEWERS' COMMENTS

This paper studied integer-valued polynomials, by which the author means a polynomial f whose values on the set of integers are integers, i.e. $f(\mathbb{Z}) \subset \mathbb{Z}$. The main goal of the paper was to study the algebraic properties of the ring of such polynomials, and also extend the results by replacing $\mathbb{Z}$ by $\mathbb{Z}[i]$, addressing several issues about whether the ring of (Gaussian) integer-valued polynomials is Noetherian, integrally closed, GCD or not. Reviewers think that the author has a good commend on ring theory.