Algebraic Properties of the Gaussian Integers

Matt McCarthy

April 2016

Theorem. *The Gaussian Integers, denoted $\mathbb{Z}(i)$, form a Euclidean domain.*

1 Background

Before we can talk about Euclidean domains, we first need to introduce the definition of a ring.

Definition 1 (Ring)**.** Let R be a nonempty set, and let $+ : R^2 \to R$ and $\cdot : R^2 \to R$ be binary operations on R. Then we say R is a *ring* if all of the following hold.

1. The structure $(R, +)$ is an abelian group whose identity we denote as 0.
2. For any $a, b, c \in R$, $a(bc) = (ab)c$ (Multiplicative Associativity).
3. For any $a, b, c \in R$, $a(b + c) = ab + ac$ (Left Distributivity).
4. For any $a, b, c \in R$, $(a + b)c = ac + bc$ (Right Distributivity).

If one says R is a ring, we imply that there exists some addition and some multiplication operators which we denote as $a + b$ and ab respectively.

Definition 2 (Ring with Unity)**.** Let R be a ring. Then R is a *ring with unity* if there exists a $1 \in R$ such that for any $a \in R$, $a \cdot 1 = 1 \cdot a = a$. If such a 1 exists, we call it the *unity*.

Definition 3 (Commutative Ring)**.** Let R be a ring. Then we say R is *commutative* if for any $a, b \in R$, $ab = ba$.

The integers, denoted $\mathbb{Z}$, are a commutative ring with unity because they satisfy all of the above properties under the usual addition and multiplication. Another helpful definition is that of a subring.

Definition 4 (Subring)**.** Let R be a ring and let S be a nonempty subset of R. Then S is a *subring* of R if $(S, +, \cdot)$ is also a ring.

Furthermore, we have a test which makes it easier to show a subset is a subring.

Proposition 1 (Subring Test)**.** *Let R be a ring, and let $S \subseteq R$ be nonempty. Then S is a subring of R if and only if for any $a, b \in S$, $a - b$ and ab are also in S.*

Now we need a few more definitions and then we can proceed to proving the theorem. First, we need to define what a zero divisor is.

Definition 5 (Zero Divisor)**.** Let R be a ring and let $a \in R$ be nonzero. We say a is a *zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$.

An example of a zero divisor is 2 in $\mathbb{Z}_6$, since $2 \cdot 3 \equiv 0 \mod 6$. An important property of zero divisors is that they cannot be inverted. Thus, if our ring has no zero divisors it is fairly nice; in fact it is nice enough that we name it.

Definition 6 (Integral Domain)**.** Let R be a commutative ring with unity. Then we say R is an *integral domain* if R has no zero-divisors.

We call these structures integral domains, because they behave like the integers. That is there is a unity, multiplication commutes, and we can multiply any nonzero elements together to get another nonzero element.

Next we will define one of the strongest structures in algebra, the field.

Definition 7 (Field)**.** Let $\mathbb{F}$ be a commutative ring with unity. Then $\mathbb{F}$ is a *field*, if for each $a \in \mathbb{F} \setminus \{0\}$, there exists a $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$.

One field that we will use in our proof is the complex numbers, denoted $\mathbb{C}$. Lastly, we define Euclidean domains.

Definition 8 (Euclidean Domain)**.** Let R be an integral domain. Then we say R is a *Euclidean domain* if there exists a function $d : R \to (\mathbb{Z}^+ \cup \{0\})$ such that

1. for any $x, y \in R \setminus \{0\}$, $d(xy) \geq d(x)$,
2. and there exist $q, r \in R$ where $x = yq + r$ with $r = 0$ or $d(r) < d(y)$.

Any such d is called a *measure*.

Essentially, Euclidean domains are rings where the division algorithm works.

2 Solution

To start, we define $\mathbb{Z}(i)$, the Gaussian Integers.

Definition 9 (Gaussian Integers)**.** The *Gaussian Integers* are

$$\mathbb{Z}(i) = \{a + bi | a, b \in \mathbb{Z}\}.$$

We first need to show that $\mathbb{Z}(i)$ is an integral domain.

Lemma 2. *$\mathbb{Z}(i)$ is an integral domain under standard complex addition and multiplication.*

Proof. We know that $\mathbb{C}$ is a field, therefore it is a commutative ring with identity and no zero divisors. Thus, it suffices to show that $\mathbb{Z}(i)$ is a subring of $\mathbb{C}$ that contains 1. Since $1, 0 \in \mathbb{Z}$, $1 + 0i = 1 \in \mathbb{Z}(i)$. Thus $\mathbb{Z}(i)$ is nonempty since it contains the unity. We now need to show that for any $z = a + bi, w = c + di \in \mathbb{Z}(i)$, $z - w, zw \in \mathbb{Z}(i)$. We know that $z - w = (a - c) + (b - d)i$ and $zw = (ac - bd) + (ad + bc)i$. Since $\mathbb{Z}$ is a ring, $a - c, b - d, ac - bd$, and $ad + bc$ are in $\mathbb{Z}$ by closure. Therefore, $z - w, zw \in \mathbb{Z}(i)$. Thus $\mathbb{Z}(i)$ is a commutative ring with unity that has no zero divisors. Hence, $\mathbb{Z}(i)$ is an integral domain. $\square$

Since $\mathbb{Z}(i)$ is an integral domain, we can embed it in what we call the *field of fractions*, otherwise known as $\mathbb{Q}(i)$. We will assume that $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$, which is true but requires a significant amount of background to show. The proof of the following theorem hinges upon the previous assumption.

Theorem 3. *$\mathbb{Z}(i)$ is a Euclidean domain.*

Proof. In order to show that an integral domain is a Euclidean domain, we need to propose a measure. We claim that $d : \mathbb{Z}(i) \to \mathbb{Z}^+ \cup \{0\}$ given by $d(z) = |z|^2$ is such a measure.

To start we need to show that for any $z, w \in \mathbb{Z}(i) \setminus \{0\}$, $d(zw) \geq d(z)$. We know that $d(zw) = |zw|^2$. However, from Euler's formula, we know that $|zw| = |z||w|$. Therefore, $d(zw) = |z|^2|w|^2$. Furthermore, by Euler's formula, the only element with modulus less than 1 in $\mathbb{Z}(i)$ is 0. Therefore, $d(zw) \geq |z|^2 = d(z)$.

Next, we need to find $q, r \in \mathbb{Z}(i)$ such that $z = wq + r$ where $r = 0$ or $d(r) < d(w)$. To do so, we embed $\mathbb{Z}(i)$ is $\mathbb{Q}(i)$ and consider z/w. We know $z/w = \alpha + \beta i$ with $\alpha, \beta \in \mathbb{Q}$. Let α', β' be the nearest integers to α and β respectively. Then $|\alpha - \alpha'| \leq 1/2$ and $|\beta - \beta'| \leq 1/2$. Furthermore,

$$\frac{z}{w} = \alpha - \alpha' + \alpha' + (\beta - \beta' + \beta')i = (\alpha' + \beta' i) + ((\alpha - \alpha') + (\beta - \beta')i).$$

Solving for z yields,

$$z = (\alpha' + \beta' i)w + ((\alpha - \alpha') + (\beta - \beta')i)w.$$

Since $\alpha', \beta' \in \mathbb{Z}$, we know that $\alpha' + \beta' i \in \mathbb{Z}(i)$. Thus,

$$((\alpha - \alpha') + (\beta - \beta')i)w = z - (\alpha' + \beta' i)w \in \mathbb{Z}(i)$$

by closure. Take $q = \alpha' + \beta' i$ and $r = ((\alpha - \alpha') + (\beta - \beta')i)w$. If $r = 0$, we are done, otherwise consider $d(r)$.

$$d(r) = |(\alpha - \alpha') + (\beta - \beta')i|^2 d(w) = (|\alpha - \alpha'|^2 + |\beta - \beta'|^2)d(w)$$

However, we know that $|\alpha - \alpha'| \leq 1/2$ and $|\beta - \beta'| \leq 1/2$. Therefore,

$$d(r) \leq \left(\frac{1}{4} + \frac{1}{4}\right) d(w) = \frac{1}{2} d(w) < d(w)$$

and d is a measure on $\mathbb{Z}(i)$. Thus $\mathbb{Z}(i)$ is Euclidean. $\square$