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 $a, b \in R$, $ab = ba$.

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