Note for Gaussian Integer and Multiplicative Norm

Date: May 21 Made by Eric

Definition

Definition 1. *An element $a + bi$ of $\mathbb{Z}[i]$ is a **Gaussian Integer**, the norm $N(\alpha)$ of a Gaussian Integer $\alpha = a + bi$ is defined by $N(\alpha) = a^2 + b^2$*

Lemma 1. $N(\alpha) = 0 \iff \alpha = 0$

Lemma 2. $N(\alpha\beta) = N(\alpha)N(\beta)$

Definition 2. *Let D be an integral domain. A **multiplicative norm** N on D is a function mapping D to $\mathbb{Z}$ that satisfy*

$$N(\alpha) = 0 \iff \alpha = 0 \tag{1}$$

and

$$\forall(\alpha, \beta) \in D^2, N(\alpha\beta) = N(\alpha)N(\beta) \tag{2}$$

Notice that multiplicative norm and Euclidean norm are completely two different concept, while the former map element into negative integer and the latter does not. The only "relationship" between them is that if a norm mapping non-zero element to non-negative integer satisfy the second condition of multiplicative, it immediately satisfy the second condition of Eucliden norm.

Theorems

Theorem 3. *The set of Gaussian Integer $\mathbb{Z}[i]$ form an Euclidean domain if we define $\nu(\alpha) = N(\alpha)$ for all non-zero elements.*

Proof. We first need to show $\mathbb{Z}[i]$ is an integral domain. Obviously $\mathbb{Z}[i]$ is a commutative ring with unity, we only need to show $\mathbb{Z}[i]$ contain no zero divisor. Observe that $\alpha\beta = 0 \implies N(\alpha\beta) = 0 \implies N(\alpha)N(\beta) = 0 \implies N(\alpha) = 0$ or $N(\beta) = 0 \implies \alpha = 0$ or $\beta = 0$.

It remains to show that for all α and non-zero β in $\mathbb{Z}[i]$, there exists $q, r \in \mathbb{Z}[i]$ such that $\alpha = q\beta + r$ and $\nu(r) < \nu(B)$ or $r = 0$ and that for all non-zero α, β in $\mathbb{Z}[i]$, we have $\nu(\alpha) \leq \nu(\alpha\beta)$.

Arbitrarily pick α and non-zero β from $\mathbb{Z}[i]$, and let q be the Gaussian integer closest to $\frac{\alpha}{\beta}$. If $\alpha - \beta q = 0$, then we let $r = 0$, the proof is over. So, we only have to consider the case $\alpha - \beta q \neq 0$. Let $r = \alpha - \beta q \neq 0$.

Because q is the closest Gaussian integer to $\frac{\alpha}{\beta}$, we know

$$|q - \frac{\alpha}{\beta}| < \frac{\sqrt{2}}{2} \tag{3}$$

and further

$$|\beta||q - \frac{\alpha}{\beta}| = \frac{\sqrt{2}}{2}|\beta| \tag{4}$$

that is

$$|r| = |\beta q - \alpha| = |\beta||q - \frac{\alpha}{\beta}| = \frac{\sqrt{2}}{2}|\beta| \tag{5}$$

then

$$\sqrt{N(r)} < \frac{\sqrt{2}}{2}\sqrt{N(\beta)} \tag{6}$$

and

$$\nu(r) = N(r) < \frac{1}{2}N(\beta) < N(\beta) = \nu(\beta) \text{ (done)} \tag{7}$$

Arbitrarily pick non-zero α, β from $\mathbb{Z}[i]$. Because β is non-zero, we can deduce $1 \leq N(\beta)$, and further observe

$$\nu(\alpha) = N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta) = \nu(\alpha\beta) \text{ (done)} \tag{8}$$

■

Lemma 4. *Let D be an integral domain and equipped D with a multiplicative norm N, then*

$$\forall u \in [u], N(u) = \pm 1 \textit{ and } N(1) = 1 \tag{9}$$

Proof.

$$N(1) = N(1 * 1) = N(1)^2 \implies N(1) = 1 \tag{10}$$

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}) \implies N(u) = \pm 1 \tag{11}$$

■

Notice that every integral domain equipped with multiplicative norm maps units to 1, but not every element of every integral domain equipped with multiplicative norm mapped to 1 is a unit. An example is $\mathbb{Z}[x]$ and $N(f(x)) = 2^{deg(f(x))}$, where $N(0)$ is defined to be 0. We can see $N(23) = 1$

Theorem 5. ***(Fermat's*** $p = a^2 + b^2$ ***Theorem)*** *Let p be an odd prime in $\mathbb{Z}$. Then*

$$p = a^2 + b^2 \textit{ for some integer } a, b \iff p \equiv_4 1$$

Proof. $(\longrightarrow)$

Because p is odd, WOLG, we can suppose a is odd and b is even. Express a, b in the form $a = 2n + 1$ and $b = 2m$, and observe $p = 4n^2 + 4m^2 + 4n + 1$, which implies $p \equiv_4 1$.

$(\longleftarrow)$

From the fact that $\langle \mathbb{Z}_p^*, * \rangle$ is a cyclic group of a order divided by 4, we can pick an element α from $\mathbb{Z}_p^*$ that is of order 4 in the cyclic group $\langle \mathbb{Z}_p^*, * \rangle$. Notice $(\alpha^2)^2 \equiv_p$

$1 \implies \alpha^2 \equiv_p \pm 1$, and because α is of order 4, not 2, we deduce $\alpha^2 \equiv_p -1$; in other words, p divides $\alpha^2 + 1$.

We now show p is reducible. Notice that the fact that $\mathbb{Z}[i]$ is an UFD wouldn't change whether or not we strip its norm, so if we assume p is irreducible, then p is a prime. Because p divides $\alpha^2 + 1 = (\alpha - i)(\alpha + i)$, we deduce p divides $\alpha - i$ or p divides $\alpha + i$. WOLG, pick $a + bi$ such that $p(a + bi) = \alpha - i$. We immediately CaC from $pb = -1$, since $p > 1$. (done)

Because p is reducible, we can express p in the form $p = (a + bi)(c + di)$ where neither $a + bi$ nor $c + di$ are unit. Observe

$$N(p) = N(a + bi)N(c + di) \implies p^2 = (a^2 + b^2)(c^2 + d^2) \tag{12}$$

Notice that $\mathbb{Z}[i]$ is an UFD, so the Euclidean norm $N(x + yi) = x^2 + y^2$ only maps units to the smallest number of its range, which is $1 = N(1)$. Notice that $N(a + bi) = a^2 + b^2 = p^2$ or p or 1. Because $a + bi$ is not a unit, we deduce $N(a + bi) \neq 1$, and because $c + di$ is not a unit, we deduce $N(a + bi) \neq p^2$. Then, the deduction left us the desired $a^2 + b^2 = p$. ∎

Exercises

10.

10.(a)

Show that 2 is equal to the product of a unit and the square of an irreducible in $\mathbb{Z}[i]$

Proof.

$$2 = (-i)(1 + i)^2 \tag{13}$$

Notice $N(1 + i) = 2$, so if $1 + i = \alpha\beta$, we see $N(\alpha) = 1$ or $N(\beta) = 1$; that is α or β is an unit. ∎

10.(b)

Show that an odd prime p in $\mathbb{Z}$ is irreducible in $\mathbb{Z}[i]$ if and only if $p \equiv_4 3$

Proof. $(\longrightarrow)$

Assume $p \equiv_4 1$, we know $p = a^2 + b^2$ for some integer a, b. Then we see $p = (a + bi)(a - bi)$, where $p = N(a + bi) \neq 1 \neq N(a - bi) = p$ CaC

$(\longleftarrow)$

Assume p is reducible, and express p in the form $p = (a + bi)(c + di)$ where neither $a + bi$ nor $c + di$ are units. Then we can deduce $p^2 = N(p) = N(a +$

$bi)N(c+di) = (a^2+b^2)(c^2+d^2)$. By the fact that neither $a+bi$ not $c+di$ are units, we can further deduce $a^2+b^2 = p$, which implies $p \equiv_4 1$ CaC

■

15.

Let $\langle \alpha \rangle$ be a nonzero principal ideal in $\mathbb{Z}[i]$.

15.(a)

Show that $\mathbb{Z}[i]/\langle \alpha \rangle$ is a finite ring

15.(b)

Show that if π is an irreducible of $\mathbb{Z}[i]$, then $\mathbb{Z}[i]/\langle \pi \rangle$ is a field.

15.(c)

Find the order and characteristic of $\mathbb{Z}[i]/\langle 3 \rangle$ and $\mathbb{Z}[i]/\langle 1+i \rangle$ and $\mathbb{Z}[i]/\langle 1+2i \rangle$

16.

Let $n \in \mathbb{N}$ be square free, that is, not divisible by the square of any prime integer.

16.(a)

Show that the norm N of $\mathbb{Z}[i\sqrt{n}]$ defined by $N(a+bi\sqrt{n}) = a^2+nb^2$ is multiplicative.

16.(b)

Show that $N(\alpha) = 1 \iff \alpha$ is a unit of $\mathbb{Z}[i\sqrt{n}]$.

16.(c)

Show that $\mathbb{Z}[i\sqrt{n}]$ is atomic