Binary Quadratic Forms

Sivmeng HUN

August 19, 2023

Chapter 1

Gaussian Integers and Sum of Two Squares

1.1 Gaussian Integers

We denote $\mathbb{Z}[i] = \{p + iq : p, q \in \mathbb{Z}\}$ the set of Gaussian integers. For $x = p + qi$, we define the norm $N(x) = p^2 + q^2$. It turns out that this norm satisfy Euclidean algorithm.

For $x, y \in \mathbb{Z}[i]$ we say $x \mid y$ if there is an $u \in \mathbb{Z}[i]$ such that $xu = y$. By a *unit* in $\mathbb{Z}[i]$ we mean those elements that divides 1, i.e. they are those that have multiplicative inverse. Lastly, we say u, v are associates if $u \mid v$ and $v \mid u$. We denote it by $u \sim v$.

One might ask: How many units are there in $\mathbb{Z}[i]$? This is answered in Exercise 1.2.3 in Lehman's book which we will give a full proof here.

Proposition 0.1 *(Ex 1.2.3, p. 26) Let u, v, w be Gaussian integers, then the following are true:*

- *If v divides w in $\mathbb{Z}[i]$, then $N(v)$ divides $N(w)$ in $\mathbb{Z}$*
- *u is a unit if and only if $N(u) = 1$*
- *If $v \sim w$ in $\mathbb{Z}[i]$, then $N(v) = N(w)$.*

Proof. Let $u, v, w \in \mathbb{Z}[i]$.

- Suppose that $v \mid w$, then $vu = w$ for some u. Taking the norm from both sides, we have $N(v)N(u) = N(vu) = N(w)$. Thus $N(v) \mid N(w)$. However, the converse isn't always true. Take for instance $v = 2 + i$ and $w = 3 + i$. It's easy to see that $v \nmid w$ but $N(v) \mid N(w)$.
- Let u be a unit. By definition, $u \mid 1$ thus $N(u) \mid 1$ in $\mathbb{Z}$. We conclude that $N(u) = 1$. Conversely, suppose that $u = p + qi$ and $N(u) = 1$. Thus $p^2 + q^2 = 1$. This means that $(p, q) = (\pm 1, 0), (0, \pm 1)$. It's easy to prove that each of the four possibilities of $p + qi$ has inverse, i.e. u is a unit.
- Suppose that $v \sim u$, i.e. $v \mid u$ and $u \mid v$. Hence $N(v) \mid N(u)$ and $N(u) \mid N(v)$ in $\mathbb{Z}$. Therefore $N(u) = N(v)$. The converse isn't always

true. For example take $v = 7 + i$ and $w = 5 + 5i$. It's easy to see that v and w aren't associates, but $N(v) = N(u) = 50$.

$\square$

This shows that in $\mathbb{Z}[i]$ there are precisely four units namely $1, -1, i, -i$.

Unique Factorization into Irreducibles

In $\mathbb{Z}[i]$, by *reducible* element we mean a non-zero, non-unit element that can be written as products of non-unit elements in $\mathbb{Z}[i]$. Otherwise we call them *irreducible* elements.

Proposition 0.2 *(Ex 1.2.8, p. 27) Let w be a reducible Gaussian integer. Then w can be written in some way as a product of irreducible elements in $\mathbb{Z}[i]$.*

Proof. We prove by contradiction. Suppose that there are reducibles that can't be written as product of irreducibles, and let w be one of them with the smallest norm. Since w is reducible, then we can write $w = ab$ where a, b are non-unit. Taking norm from both sides, we obtain that $N(a), N(b) < N(w)$. Moreover neither a nor b can be irreducibles since we would have $w = ab$ product of irreducibles.

Without loss of generality, assume that the factor a is reducible. Hence $a =: \prod a_i$ must be product of irreducibles, if not, a would have the same property of w, yet with a smaller norm. Therefore b must also be reducible as well. Arguing as the above, we conclude that $b =: \prod b_j$ is product of irreducibles. But that would be a contradiction because now $w = \prod a_i \cdot \prod b_j$ is product of irreducibles. $\square$

The above proposition shows the existence of such factorizations. It says that every non-unit element of $\mathbb{Z}[i]$ is either irreducible or product of irreducibles. Next, we prove the uniqueness of such factorization up to multiplication by units.

Proposition 0.3 *Every Gaussian integer that is neither zero nor a unit can be wrriten uniquely as a product of irreducibles, aside from the order of the factors and multiplication by units.*

Proof. Again we prove by contradiction, and assume that w is an element of smallest norm that can be written in two distinct ways a products of irreducibles. We may write $w = u_1 \cdot u_2 \cdots u_k$ and $w = z_1 \cdot z_2 \cdots z_\ell$ and we may assume $\ell \geq k$. Since u_1 is irreducible, then it has to divide exactly one of the z_i, and by rearranging the terms, we may without loss of generality assume that $u_1 \mid z_1$. Thus we can write $z_1 = u_1 a_1$ for some non-zero a_i. We claim that a_1 has to be a unit, otherwise a_1 is either irreducible or product of one. But then z_1 would have two distinct factorizations namely z_1 and $u_1 a_1$. Since $N(z_1) < N(w)$, that would be a contradiction.

We conclude that $u_2 \cdots u_k = a_1 \cdot (z_2 \cdots z_\ell)$. Since a_1 is unit, then $u_2 \nmid a_1$. Arguing as above, we may assume that $u_2 \mid z_2$ and $z_2 = u_2 a_2$ where a_2 is a unit. Continuing this fashion, we obtain

$$1 = a_1 a_2 \cdots a_k \cdot (z_{k+1} \cdots z_\ell)$$

This tells us that the rest of the z_i's are unit, and we would get a contradiction because the factorization $\prod u_i$ and $\prod z_i$ are unique up to unit multiples and rearranging the terms. $\square$

This tells us that the ring $\mathbb{Z}[i]$ is a UFD domain.

Classification of Irreducibles

In Lehman's book we have the following result: If $N(z)$ is prime, then z is irreducible in $\mathbb{Z}[i]$. Moreover If z is irreducible, then $z \mid p$ for some prime $p \in \mathbb{N}$. So if we can factorize p into into irreducibles in $\mathbb{Z}[i]$, we would have a way to classify all the irreducibles. This is made clear with the following theorem

---

Theorem 1 *Let $p \in \mathbb{N}$ be a prime number. Then*

$$p \text{ is reducible} \iff p \equiv 1 \pmod 4.$$

Moreover in proving the above theorem we obtain that if p is reducible, then its factorization is $p = z \cdot \overline{z}$ where z and $\overline{z}$ are both irreducibles. Now we can start classifying as follows: let $z \in \mathbb{Z}[i]$ be any irreducible and u is any unit. Then there is some prime $p \in \mathbb{N}$ such that $z \mid p$. There are three cases:

- Case $p = 2$: we have $(1+i)(1-i) = 2$, and $(1+i) \sim (1-i)$. Moreover $1+i$ is irreducible since $N(1+i)$ is prime. Therefore $\boxed{z = (1+i)u}$.
- Case $p \equiv 1 \pmod 4$: As mentioned above, we conclude that $p = (q + ri)(q - ri)$. Multiplication by units, we might assume that $q > r > 0$. Because both $(q+ri)$ and $(q-ri)$ are irreducibles, and they aren't associate of each other, this yields $\boxed{z = (q+ri)u \text{ or } z = (q-ri)u}$.
- Case $p \equiv 3 \pmod 4$: The above theorem tells us that p is irreducible in $\mathbb{Z}[i]$, therefore $\boxed{z = p}$.

We summarize these result in the following theorem

Theorem 2 *The irreducibles in $\mathbb{Z}[i]$ consists precisely of the following elements and their associates:*

- *p, where $p \equiv 3 \pmod 4$ is a prime*
- *$q + ri$ and $q - ri$, where $q^2 + r^2 \equiv 1 \pmod 4$ is a prime ($q > r$)*
- $1 + i$
