

A closer look into a well-known quotient ring

by Manjil Saikia - Sunday, February 26, 2012

<https://gonitsora.com/a-closer-look-into-a-well-known-quotient-ring/>

The ring $Z[i] = \{a+ib : a, b \in Z, i^2 = -1\}$ is quite a well-known ring in Algebra. Further, being a principal ideal domain, every ideal of $Z[i]$ is generated by a single element say $a+ib \in Z[i]$ and so can be taken in the form $\langle a+ib \rangle = \{(x+iy)(a+ib) : x, y \in Z\}$.

We now consider the quotient ring $Z[i]/\langle a+ib \rangle = \{(x+iy)/(a+ib) : x, y \in Z\}$ and try to look for a precise way of representing the elements in it. First we suppose that a and b are both non zero. The quantities $d = \gcd(a, b)$ and $N = (a^2 + b^2)/\gcd(a, b)$ deserve special attention in the discussion.

Result A: - An integer $n \in \langle a+ib \rangle$ if and only if $n \in \langle (a^2 + b^2)/\gcd(a, b) \rangle$.

Proof: - Since $d = \gcd(a, b)$, we can write $a+ib = d(p+iq)$, where $\gcd(p, q) = 1$.

Now let $n \in \langle a+ib \rangle$. This implies that $n = (a+ib)(x+iy)$ for some $x+iy \in Z[i]$.

$\Rightarrow n = d(p+iq)(x+iy)$, which gives $py = -qx \Rightarrow p|qx$ and $q|py$. (“|” means divides.)

And since $\gcd(p, q) = 1$, so $p|x$ and $q|y$ which means that x/p and y/q are integers.

Also, $py = -qx \Rightarrow x/p = -y/q = k$ say, where $k \in Z$.

Thus we get $n = d(p+iq)(kp-ikq)$

$\Rightarrow n = d(p^2 + q^2)(k+i0)$ which shows that $n \in \langle d(p^2 + q^2) \rangle$.

But $d(p^2 + q^2) = \{(dp)^2 + (dq)^2\}/d = (a^2 + b^2)/\gcd(a, b) = N$.

Hence, $n \in \langle N \rangle$.

Conversely if $n \in \langle N \rangle$ then by using the relation $a^2 + b^2 = (a+ib)(a-ib)$ it can be easily shown that $n \in \langle a+ib \rangle$.

Therefore $n \in \langle a+ib \rangle$ if and only if $n \in \langle (a^2 + b^2)/\gcd(a, b) \rangle$.

Result B: - For any $n \in Z$, $n \in \langle a+ib \rangle$ if and only if $n \in \langle N \rangle$.

Proof: - Similar to above.

Observation: -

- 1) Since $1, 2, \dots, N-1$ do not belong to $\langle a+ib \rangle$ so it is clear that the elements $0+\langle a+ib \rangle, 1+\langle a+ib \rangle, \dots, (N-1)+\langle a+ib \rangle$ of $\mathbb{Z}[i]/\langle a+ib \rangle$ are distinct.
- 2) Since $a^2+b^2=(a+ib)(a-ib)$ so it is to be noted that $\langle N \rangle \subseteq \langle a+ib \rangle$.
- 3) If $n \in \mathbb{Z}$ then by division algorithm, there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < N$ such that $n=Nq+r$. Since $n-r=Nq \in \langle a+ib \rangle$ so $n+\langle a+ib \rangle = r+\langle a+ib \rangle$.

Thus any element of the form $n+\langle a+ib \rangle$, where $n \in \mathbb{Z}$, can be reduced to the form $r+\langle a+ib \rangle$ for a unique integer r satisfying $0 \leq r < N$.

The following result is further more generalized:

Result C:- $\mathbb{Z}[i]/\langle a+ib \rangle = \{r+is+\langle a+ib \rangle : r, s \in \mathbb{Z} \text{ and } 0 \leq r < N \text{ and } 0 \leq s < d\}$.

Proof: - The proof is a just a simple application of a well- known property of GCD.

We take any element $x+iy+\langle a+ib \rangle$ of $\mathbb{Z}[i]/\langle a+ib \rangle$. By division algorithm, we can write $y=qd+s$ where $q, s \in \mathbb{Z}, 0 \leq s < d$. Again since $d=\gcd(a,b)$ so there exist $u, v \in \mathbb{Z}$ such that $d=au+bv$. And it is easy to see that $d=(a+ib)(u-iv)-i(bu-av)$ which gives

$$x+iy+\langle a+ib \rangle = (x+qbu-qav)+is+iq(a+ib)(u-iv)+\langle a+ib \rangle$$

$$= (Nw+r)+is+\langle a+ib \rangle, \text{ where } 0 \leq r < N, \text{ (division algorithm)}$$

$$= r+is+\langle a+ib \rangle \text{ where } 0 \leq r < N, 0 \leq s < d \text{ (since } Nw \in \langle a+ib \rangle \text{)}$$

Hence the result

Result D: - The elements in the set in RHS of D are distinct.

Proof: - Let $A = \{r+is+\langle a+ib \rangle : r, s \in \mathbb{Z} \text{ and } 0 \leq r < N \text{ and } 0 \leq s < d\}$

Let $x_1+iy_1+\langle a+ib \rangle$ and $x_2+iy_2+\langle a+ib \rangle$ be any two members of A .

Since $0 \leq y_1, y_2 < d$ and $0 \leq x_1, x_2 < N$ a simple observation reveals that

1) x_1-x_2 cannot be a non-zero multiple of N and

2) y_1-y_2 cannot be a non-zero multiple of d .

The above members will be equal if $(x_1+iy_1)-(x_2+iy_2) \in \langle a+ib \rangle$

i.e. if $(x_1-x_2)+i(y_1-y_2) \in \langle a+ib \rangle$

$$\Rightarrow (x_1 - x_2) + i(y_1 - y_2) = (a + ib)(m + in) \text{ for some } m, n \in \mathbb{Z}$$

$$\Rightarrow (x_1 - x_2) = am - bn \text{ and } (y_1 - y_2) = bm + an$$

$$\Rightarrow d \mid (x_1 - x_2) \text{ and } d \mid (y_1 - y_2) \text{ since } d = \gcd(a, b)$$

i.e. $y_1 - y_2$ is a multiple of d , but by (1) above $y_1 - y_2 = 0$ i.e. $y_1 = y_2$

We thus have $x_1 - x_2 \in \langle a + ib \rangle$ which in turn implies that $x_1 - x_2$ is a multiple of d but by (2) above, the only possibility is $x_1 - x_2 = 0$ i.e. $x_1 = x_2$. Thus the elements are distinct.

Conclusion:- From the above results it is clear that

$$1) \mathbb{Z}[i] / \langle a + ib \rangle = \{ r + is + \langle a + ib \rangle : r, s \in \mathbb{Z} \text{ and } 0 \leq r < N \text{ and } 0 \leq s < d \}$$

2) $\mathbb{Z}[i] / \langle a + ib \rangle$ contains exactly the above $N \times d = a^2 + b^2$ elements.

$$3) \text{ If } \gcd(a, b) = 1, \text{ then } \mathbb{Z}[i] / \langle a + ib \rangle = \{ x + \langle a + ib \rangle : 0 \leq x < a^2 + b^2 \}$$

which is isomorphic to the ring $\mathbb{Z}_{a^2 + b^2}$ of integers modulo $a^2 + b^2$.

4) Further if $a^2 + b^2$ is prime then $\mathbb{Z}[i] / \langle a + ib \rangle$ is a field and so $\langle a + ib \rangle$ is maximal.

5) Another way of representing $\mathbb{Z}[i] / \langle a + ib \rangle$ is

$$\mathbb{Z}[i] / \langle a + ib \rangle = \{ r + is + \langle a + ib \rangle : r, s \in \mathbb{Z} \text{ and } 0 \leq r < d \text{ and } 0 \leq s < N \}$$

6) It can be proved that the same result holds for the case when one of a or b is zero. In this case we can take $\gcd(a, 0) = \text{mod}(a)$ and $\gcd(b, 0) = \text{mod}(b)$.

There may be other better ways of representing the elements of $\mathbb{Z}[i] / \langle a + ib \rangle$

We can try looking for other such smarter ways !!

- Debashish Sharma, Junior Research Fellow, Dept. of Mathematics, NIT Silchar.

PDF generated from <https://gonitsora.com/a-closer-look-into-a-well-known-quotient-ring/>.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.