Math250aHw3

Trustin Nguyen

September 11, 2023

Exercise 1: Prove that the ring of integers, $\mathbb{Z}$, is a principal ideal domain. (Hint: Use the Euclidean algorithm, which uses "division with remainder" in $\mathbb{Z}$ to compute the single generator of an ideal in the ring of integers defined by two integers $(a, b) \subseteq \mathbb{Z}$.)

Proof. Consider the ideal generated by $d_1, s = (d_1, s)$ where $d_1, s \neq 0, 1$ and such that $d_1 \neq s$. Also remove the case where $d_1 \mid s$ or $s \mid d_1$. Then we have that wlog, $d_1 < s$. So by the division algorithm, we have

$$s = d_1 q_1 + d_2$$

for some $q_1 \in \mathbb{Z}$ and $d_2 < d_1$. Since $d_2 < d_1$, we apply the same process:

$$d_1 = d_2 q_2 + d_3$$

We continue this process until it stops, which we know it will because the remainder becomes smaller every time. The process stops when $d_n \mid d_{n-1}$:

$$d_{n-1} = d_n q_n$$

But observe now that

$$d_{n-2} = d_{n-1} q_{n-1} + d_n$$

or if we substitute $d_n q_n = d_{n-1}$:

$$d_{n-2} = d_n q_n q_{n-1} + d_n$$

so $d_n \mid d_{n-2}$. By backwards strong induction, we continue this process and conclude that $d_n \mid s, d_1$. We also conclude that $d_n \in (d_1, s)$ because the Euclidean algorithm was carried out within our ideal (d_1, s). Finally, we can conclude that since $d_n \mid s, d_1$, then $(s, d_1) \subseteq (d_n)$. Therefore, we have a double inclusion and the ideals are equal, showing that all ideals are generated by a single element. □

Exercise 2: Let $\mathbb{Q}$ be the field of rational numbers. Use the fact that $\mathbb{Q}[x]$ is a principal ideal domain to show that $\mathbb{Q}[x]/(x^2+1)$ is a field. (You don't need to find the formula for division to do this.) Show that

$$\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[i] := \{a + bi : a, b \in \mathbb{Q}, i^2 = -1\}$$

by finding the ring homomorphism that carries a vector space basis of the first ring to a vector space basis of the second. Inside $\mathbb{Q}[i]$ is the ring of *Gaussian integers*, defined as a subring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Proof. Consider the evaluation map of $\mathbb{Q}[x]$ at i which goes to $\mathbb{Q}[i]$

$$\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[i]$$
$$\varphi(p(x)) := p(i)$$

This is a homomorphism. Notice that $(x^2+1) \subseteq \ker\varphi$. Now suppose that our ideal $\ker\varphi$ was also generated by another element f:

$$(x^2+1, f) \subseteq \ker\varphi$$

Since $\mathbb{Q}[x]$ is a PID, we can say that it is generated by a single element: (g), so for $h_1, h_2 \in \mathbb{Q}[x]$,

$$\begin{aligned} gh_1 &= x^2+1 \\ gh_2 &= f \end{aligned}$$

But we know that x^2+1 is irreducible in $\mathbb{Q}[x]$. Therefore, g is either a unit or x^2+1. It cannot be a unit. So g is x^2+1 meaning that $(x^2+1) \mid f$. So $(x^2+1, f) = (x^2+1)$. Therefore, $\ker\varphi = (x^2+1)$. Notice that φ is also surjective. Therefore, $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}[i]$. Now to show that $\mathbb{Q}[i]$ has inverses for every element except 0, suppose that $a+bi \in \mathbb{Q}[i]$ where a, b are not both zero. Then

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{Q}[i]$$

So inverses map to inverses and therefore, $\mathbb{Q}[x]/(x^2+1)$ is a field. □

Exercise 3: Define the *Norm* of any complex number $a+bi$ to be $N(a+bi) := a^2+b^2$. In the complex plane, show that every complex number differs from some Gaussian integer by a complex number whose norm is $\leqslant 1/2$.

Proof. Suppose that $a+bi \in \mathbb{C}$. Consider $x+yi \in \mathbb{Z}[i]$. We want to find an x, y such that

$$N(a+bi-(x+yi)) \leqslant \frac{1}{2}$$

Observe that the norm is

$$(a-x)^2+(b-y)^2$$

Consider the decimal part of a given by $0 \leqslant a - \lfloor a \rfloor \leqslant 1$. If $a - \lfloor a \rfloor > \frac{1}{2}$, let $x = \lfloor a \rfloor + 1$, otherwise, $x = \lfloor a \rfloor$. Notice that now, $|a-x| \leqslant \frac{1}{2}$. Therefore, $(a-x)^2 \leqslant \frac{1}{4}$. Repeat the same thing for $b-y$ and we get

$$N(a+bi-(x+yi)) \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

which concludes the proof. □

Exercise 4: Show that $N((a+bi)(c+di)) = N(a+bi)N(c+di)$.

Proof. Just expand:

$$\begin{aligned} N((a+bi)(c+di)) &= N(ac-bd+(ad+bc)i) \\ &= (ac-bd)^2+(ad+bc)^2 \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\ &= (ac)^2 + (ad)^2 + (bd)^2 + (bc)^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(a+bi)N(c+di) \end{aligned}$$

so we are done. □

Exercise 5: Show that $\mathbb{Z}[i]$ is a *Euclidean ring* with norm N, in the sense that given Gaussian integers $a + bi$ and $c + di$, there is a Gaussian integer $e + fi$ such that

$$a + bi = (c + di)(e + fi) + \varepsilon$$

where ε is a Gaussian integer and $N(\varepsilon) < N(c + di)$. (Hint: approximate the result of dividing in the field $\mathbb{Q}[i]$. You don't need to find a formula for division to do this.)

Proof. Consider division over the field of fractions $\mathbb{Q}[i]$. We want to find a $z \in \mathbb{Z}[i]$ such that

$$\frac{a + bi}{c + di} - z = r$$

where our remainder r has a norm less than $c + di$. Notice that $\frac{a+bi}{c+di} \in \mathbb{Q}[i]$, so by the previous problem, we have that there is a z such that

$$N\left(\frac{a + bi}{c + di} - z\right) = N(r) \leqslant \frac{1}{2}$$

Now we solve for $a + bi$:

$$\begin{aligned} \frac{a + bi}{c + di} - z &= r \\ \frac{a + bi}{c + di} &= z + r \\ a + bi &= (c + di)z + r(c + di) \end{aligned}$$

We see that $\varepsilon = r(c + di)$, so therefore, $N(\varepsilon) = N(r)N(c + di)$, but since $N(r) < 1$, we have $N(\varepsilon) < N(c + di)$. □

Exercise 6: Imitate the Euclidean algorithm to prove that $\mathbb{Z}[i]$ is a principal ideal domain.

Proof. Consider the ideal generated by $d_1, s = (d_1, s)$ with $d_1, s \in \mathbb{Z}[i]$ and where $d_1, s \neq 0, 1$ such that $d_1 \neq s$. Also remove the case where $d_1 \mid s$ or $s \mid d_1$. Then we have that wlog, $N(d_1) < N(s)$. So by the division algorithm, we have

$$s = d_1 q_1 + d_2$$

for some $q_1 \in \mathbb{Z}$ and $N(d_2) < N(d_1)$. Since $N(d_2) < N(d_1)$, we apply the same process:

$$d_1 = d_2 q_2 + d_3$$

We continue this process until it stops, which we know it will because $N(d_i) < N(d_{i-1})$. The process stops when $d_n \mid d_{n-1}$:

$$d_{n-1} = d_n q_n$$

But observe now that

$$d_{n-2} = d_{n-1} q_{n-1} + d_n$$

or if we substitute $d_n q_n = d_{n-1}$:

$$d_{n-2} = d_n q_n q_{n-1} + d_n$$

so $d_n \mid d_{n-2}$. By backwards strong induction, we continue this process and conclude that $d_n \mid s, d_1$. We also conclude that $d_n \in (d_1, s)$ because the Euclidean algorithm was carried out within our ideal (d_1, s). Finally, we can conclude that since $d_n \mid s, d_1$, then $(s, d_1) \subseteq (d_n)$. Therefore, we have a double inclusion and the ideals are equal, showing that all ideals are generated by a single element. □