

MATH 310: HOMEWORK 9

- (1) Find all the invertible elements in $\mathbb{Z}_2[x]/(x^4 + x^2 + 1)$.
- (2) Find all the monic quadratic irreducible polynomials in $\mathbb{Z}_3[x]$.
- (3) For each monic quadratic irreducible polynomial $f(x) \in \mathbb{Z}_3[x]$, let $I = (f(x))$ and find the multiplicative inverse of $x + I$ in the field $\mathbb{Z}_3[x]/I$.
- (4) Consider the following function:

$$N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$$

$$N(a + bi) = a^2 + b^2$$

Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$. Now find all the invertible elements of $\mathbb{Z}[i]$.

- (5) Let $p \in \mathbb{Z}$ be a prime. Prove that:

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$$

Use this fact to give an example of a non-zero prime ideal which is not a maximal ideal.

Theorem. $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. First, let's recall some facts about the division algorithm in \mathbb{Z} . If $a, b \in \mathbb{Z}$ and $b \neq 0$, then:

$$a = bq + r, \quad 0 \leq r < b, \quad \text{i.e.} \quad \frac{a}{b} = q + \frac{r}{b}$$

In other words, q is the closest integer to the left of $\frac{a}{b}$ on the number line. What about the closest integer to the right?

$$\frac{a}{b} = q + 1 + \frac{r}{b} - 1 = q + 1 + \frac{r - b}{b}, \quad \text{i.e.} \quad a = (q + 1)b + (r - b)$$

Note that either $r \leq \frac{b}{2}$ or $r > \frac{b}{2}$. In the second case: $r - b > -\frac{b}{2}$. In other words, we have the modified division algorithm:

$$a = q'b + r', \quad |r'| \leq \frac{b}{2}$$

Now define:

$$N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0} \\ N(a + bi) = a^2 + b^2$$

We need to show that for any $\alpha, \beta \in \mathbb{Z}[i]$ where $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r$$

and $N(r) < N(\beta)$ or $r = 0$.

Let $\alpha = a + bi$ and $\beta = c + di$, where $a, b, c, d \in \mathbb{Z}$. Since $\mathbb{Z}[i]$ is a subring of \mathbb{C} , we have:

$$\frac{\alpha}{\beta} = \frac{(a + bi)(c - di)}{N(\beta)} = \frac{ac + bd}{N(\beta)} + \frac{i(bc - ad)}{N(\beta)}$$

By the division algorithm in \mathbb{Z} , we have:

$$ac + bd = N(\beta)q_1 + r_1$$

$$bc - ad = N(\beta)q_2 + r_2$$

where $|r_1|$ and $|r_2| \leq \frac{N(\beta)}{2}$. Then:

$$\frac{\alpha}{\beta} = q_1 + \frac{r_1}{N(\beta)} + iq_2 + \frac{ir_2}{N(\beta)} \implies \alpha = \beta(q_1 + iq_2) + \frac{\beta(r_1 + ir_2)}{N(\beta)}$$

Let $q = q_1 + iq_2$ and:

$$r = \frac{\beta(r_1 + ir_2)}{N(\beta)}$$

Now:

$$N(r) = N(\beta)N\left(\frac{r_1 + ir_2}{N(\beta)}\right) = N(\beta)\left(\frac{r_1^2}{N(\beta)^2} + \frac{r_2^2}{N(\beta)^2}\right) = \frac{r_1^2 + r_2^2}{N(\beta)}$$

We have r_1^2 and $r_2^2 \leq \frac{N(\beta)^2}{4}$, so that:

$$N(r) \leq \frac{N(\beta)^2 + N(\beta)^2}{4N(\beta)} = \frac{N(\beta)}{2}$$

□