problem session 5, part 3

9,11 p 166; 20 p 167

Section 6.3

9 p166 R is an integral domain, $p \in R$, $p \neq 0_R$

The principal ideal (p) is prime.

Prove that whenever $p = cd$, then c or d is a unit in R.

Pf

$cd = p \in (p)$ because $1_R \in R$.

The ideal is prime, therefore $c \in (p)$ or $d \in (p)$

If $c \in (p)$, then $\underline{d \text{ is a unit}}$ ← To prove.

$c \in (p)$ means that $c = pr$, with $r \in R$.

We rewrite $p = cd$ as $p = prd$

$$p - prd = 0_R$$

$$p(1_R - rd) = 0_R$$ Since R is an integral domain

$$p = 0_R \text{ or } 1_R - rd = 0_R$$

As $p \neq 0_R$ (given), we conclude that $rd = 1_R$, therefor $\underline{d \text{ is a unit}}$.

20 p167 Find an ideal in $\mathbb{Z}\times\mathbb{Z}$ which is prime but not maximal.

Solution

Recall: $\mathbb{Z}\times\mathbb{Z} = \{(a,b) \mid a,b \in \mathbb{Z}\}$ - commutative ring with identity $(1,1) = 1_{\mathbb{Z}\times\mathbb{Z}}$

$(a,b)+(c,d) = (a+c, b+d)$

$(a,b)(c,d) = (ac, bd)$

- not an integral domain:

$(1,0)(0,1) = (0,0) = 0_{\mathbb{Z}\times\mathbb{Z}}$

Consider the map

$$\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto a$$

Easy to check: this map is a surjective homomorphism

The kernel $K = \{(0,b) \mid b \in \mathbb{Z}\}$ is an ideal by Th 6.10

The First Isomorphism Theorem (Th 6.13) allows us to conclude that

$$\mathbb{Z}\times\mathbb{Z}/K \simeq \mathbb{Z} \leftarrow \text{is an integral domain, but not a field}$$

The ideal K is prime by Th 6.14, but not maximal by Th 6.15

11 p166 Show that the principal ideal $(x-1)$ in $\mathbb{Z}[x]$ is prime but not maximal.

Pf As in the previous problem, that will follow from

$$\mathbb{Z}[x]/(x-1) \simeq \mathbb{Z}$$

Parallel to

$$\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$$

Example 7 p164

Consider the map

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}$$
$$f \longmapsto f(1)$$

This is a ring homomorphism because

$$\mathbb{Q}[x] \longrightarrow \mathbb{Q}$$
$$f \longmapsto f(1)$$

$\mathbb{Q}$ is a field

is a ring homomorphism.

The map is surjective (constant polynomials already do the job)

Wanted: the kernel is $(x-1) \subset \mathbb{Z}[x]$ (suffices by the First Isomorphism Theorem)

The kernel is $K = \{ f \in \mathbb{Z}[x] \mid f(1) = 0 \}$

Clearly, $K \supseteq (x-1)$ $\Big\}$ If $f = (x-1)q$, $q \in \mathbb{Z}[x]$, then $f(1) = 0$

We need $K \subseteq (x-1)$, in other words,

$f(1)=0$ implies $\underline{f=(x-1)q \text{ with } q \in \mathbb{Z}[x]}$

Remainder Thm (Th 4.15) $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$

$f=(x-1)q+f(1)$, and since $f(1)=0$, we have

$\underline{f=(x-1)q \text{ with } q \in \mathbb{Q}[x]}$.

We want to prove that if $f \in \mathbb{Z}[x]$, then $\underline{q \in \mathbb{Z}[x]}$

Let $q = a_0 + \dots + a_n x^n \in \mathbb{Q}[x]$

Expand $(x-1)q \in \mathbb{Z}[x]$:

$$(x-1)q = -a_0 + (a_0-a_1)x + (a_1-a_2)x^2 + \dots + (a_{n-1}-a_n)x^n + a_n x^n \in \mathbb{Z}[x]$$

$a_0 \in \mathbb{Z}$

$a_0 - a_1 \in \mathbb{Z}$ implies $a_1 \in \mathbb{Z}$

$a_1 - a_2 \in \mathbb{Z}$ implies $a_2 \in \mathbb{Z}$

...

$a_{n-2} - a_{n-1} \in \mathbb{Z}$ implies $a_{n-1} \in \mathbb{Z}$

$a_n \in \mathbb{Z}$

In fact, $q \in \mathbb{Z}[x]$