113 Class Problems: Principal, Prime and Maximal Ideals

1. (a) Give an explicit description of all possible ideals of $\mathbb{Z}$. Hint: Consider the possible subgroups of a cyclic group.
   (b) If $(n) = (m) \subset \mathbb{Z}$ what must be true about n and m?
   (c) Let $m \in \mathbb{N}$. Using the definition, prove that that $(m) \subset \mathbb{Z}$ is a prime ideal if and only if m is prime.
   (d) Let $m \in \mathbb{N}$. Using the definition, prove that $(m) \subset \mathbb{Z}$ is maximal if and only if m is prime.
   This shows that prime and maximal ideals coincide in $\mathbb{Z}$.

Solutions:

a) Subgroups of cyclic groups are cyclic $\Rightarrow$ All possible ideals of $\mathbb{Z}$ are of form $(m) = m\mathbb{Z}$ for $m \in \mathbb{Z}$

b) $(n) = (m) \Leftrightarrow n | m$ <u>and</u> $m | n \Leftrightarrow n = \pm m$

c) Let m be prime.

Euclid's Lemma

$ab \in (m) \Rightarrow m | ab \Rightarrow m | a$ or $m | b \Rightarrow a \in (m)$ or $b \in (m)$

Assume (m) prime. Assum $m = ab$, $a, b \in \mathbb{N}$, $a, b < m$

Then $ab \in (m)$ but $a \notin (m)$ and $b \notin (m)$. Contradiction

Hence (m) prime $\Rightarrow$ m prime

d) Assume m prime and (m) not maximal. Then $\exists d \in \mathbb{N}$ such that $(m) \subsetneq (d) \subsetneq \mathbb{Z} \Rightarrow d \neq 1, d \neq m$ <u>and</u> $d | m$. Contradiction as m prime.

Assume (m) maximal. Let $d \in \mathbb{N}$ such that $d | m$

$\Rightarrow (m) \subset (d) \subset \mathbb{Z} \Rightarrow \begin{matrix} (m) = (d) \\ \text{or} \\ (d) = \mathbb{Z} \end{matrix} \Rightarrow \begin{matrix} m = d \\ \text{or} \\ 1 = d \end{matrix} \Rightarrow m$ prime

2. (a) Prove that $(x) \subset \mathbb{Z}[x]$ is a prime ideal. Is it maximal? Hint: Can you realise (x) as the kernel of some homomorphism?

(b) Let p be a prime and $(p, x) = \{f(x)p + g(x)x | f(x), g(x) \in \mathbb{Z}[x]\}$. This is the ideal generated by the set $\{p, x\}$ as described in question 7 of homework 5. Prove that $(p, x) \subset \mathbb{Z}[x]\}$ is maximal.

Solutions:

$\mathbb{Z}$ commutative so a homomorphism

a) $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$

$f(x) \longrightarrow f(0)$

$\mathrm{Ker}\,\phi = (x)$, $\mathrm{Im}\,\phi = \mathbb{Z}$

$\Rightarrow \mathbb{Z}[x]/(x) \cong \mathbb{Z}$ I.D. $\Rightarrow (x)$ prime

again a homomorphism

b) $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}$

$f(x) \longrightarrow [f(0)]_p$

constant term of $f(x)$ and p

$\mathrm{Ker}\,\phi = \{a_0 + .. + a_n x^n \mid a_i \in \mathbb{Z}, p \mid a_0\} = (p, x)$

$\mathrm{Im}\,\phi = \mathbb{Z}/p\mathbb{Z}$

field

$\Rightarrow \mathbb{Z}[x] / (p, x) \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow (p, x)$ maximal