Shidhesh Supekar

50/50

Algebra HW 10

1 $\eta \subset A$ consist of all nilpotent elements. To show.

$$\eta = \bigcap_{\substack{P \subset A \\ \text{prime ideal}}} P$$

Pf: $\eta \subseteq \bigcap_{\substack{P \subset A \\ \text{prime ideal}}} P$: Let $a \in \eta \Rightarrow \exists\, k \in \mathbb{N}$ s.t

$a^k = 0 \in P \quad \forall\, P \subseteq A$ p-prime ideal.

Now $a \cdot a^{k-1} \in P \Rightarrow$ either $a \in P$ or $a^{k-1} \in P$

If $a \in P$ we are done, if $a^{k-1} \in P$, continue this.

As k is finite, this process will terminate giving

$a \in P$. $\Rightarrow \eta \subseteq \bigcap P$

To show $\bigcap P \subseteq \eta$. Let $a \in \bigcap_{P: \text{prime ideal}} P$ but $a \notin \eta$.

$\Rightarrow S := \{ a, a^2, a^3, \ldots \}$ As $a \notin \eta$

$0 \notin S$ and S is also closed under multiplication. By Problem 4, maximal ideal P_S which does not intersect S is prime.

But $a \in \bigcap_{P: \text{prime}} P \Rightarrow a \in P_S$ contradicting $S \cap P_S = \emptyset$.

Hence, $a \in \eta$.

Pf for Pblm 4.

Let P_S be the maximal ideal among ideals which do not intersect S. [Zorn's lemma guarantees existence of such an ideal. Let $a, b \in R$, $ab \in P_S$ Let

$a \notin P_S$, $b \notin P_S \Rightarrow P_S \subsetneq (P_S, a)$ and $P_S \subsetneq (P_S, b)$.

But as P_S is maximal ideal $S \cap (P_S, a) \neq \emptyset$

and $S \cap (P_S, b) \neq \emptyset \Rightarrow$

$P_1 + ax = s$, $P_2 + by = t$ $\quad s, t \in S$

$\Rightarrow P_1(P_2 + by) + P_2 ax + abxy = st$ $\quad P_1, P_2 \in P_S$, $x, y \in R$.

How LHS $\in P_S$ and RHS $\in S$ contradicting

$P_S \cap S = \phi$. Hence, P_S is prime ideal.

3. $n \in A$ nilpotent $u \in A$ a unit. To show $(u+n)$ is again a unit.

Pf $(u+n)\, u^{-1}(1 - u^{-1}n + (u^{-1}n)^2 + \cdots (-1)^{k-1}(u^{-1}n)^{k-1})$ [$k \in \mathbb{N}$ s.t $n^k = 0$]

$= (1 + u^{-1}n)(1 - u^{-1}n + (u^{-1}n)^2 + \cdots (-1)^{k-1}(u^{-1}n)^{k-1})$

$= 1 + u^{-1}n - u^{-1}n - (u^{-1}n)^2 + (u^{-1}n)^2 + \cdots (-1)^{k-1}(u^{-1}n)^{k-1} + \underbrace{(-1)^{k-1}(u^{-1}n)^k}_{=0}$

$= 1$

$\Rightarrow u+n$ have multiplicative inverse $\Rightarrow u+n$ is a unit. ✓

6. Let $A = \mathbb{Z}$, $B = \mathbb{Q}$. $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. $f: \mathbb{Z} \to \mathbb{Q}$

However $n \mapsto n$ is a ring homomorphism.

$b := \langle f(p\mathbb{Z}) \rangle = \mathbb{Q}$ since $\mathbb{Q}$ is a field.

Hence b is not a prime ideal of $\mathbb{Q}$. ✓

9. $J := \{x \in A \mid \forall y \in A \;\; 1 - xy \text{ is a unit}\}$.

To prove J is an ideal and $J = \bigcap_{m \subset A} m$

m : maximal.

Pf : J is an ideal If $a, b \in J$, $y \in A$

$1 - (a+b)xy = 1 - ay - by$

$= (1-ay)[1 - (1-ay)^{-1}by]$ [$\because a \in J$]

$= (1-ay)(1 - b(1-ay)^{-1}y]$

$= (1-ay)(1-by')$ is a unit

as $(1-ay), (1-by')$ are units.

Let $r \in A$ $ra \in J$ as $1 - ray = 1 - a\underbrace{ry}_{\in A} \in$ units.

Hence, J is an ideal.

To show $J = \bigcap_{m:\text{maximal}} m$

Let $a \in J$ and M be any maximal ideal.

If $a \in M \Rightarrow \exists\ r \in A$ s.t $m' + ar = 1$ $m' \in M$.

$\Rightarrow \underbrace{1 - ar}_{\text{unit}} = m' \in M$ contradicting M to be maximal.

, Hence $a \in M$ $\forall$ M - maximal ideal.

i.e $J \subseteq \bigcap_{m:\text{maximal}} m$.

Let $a \in \bigcap_{m:\text{maxl}} m$ Let $x \in A$, if $1 - xa$ is not a unit, then ideal generated by $\langle 1 - xa \rangle$ is proper and contained in some maximal ideal $m_x \Rightarrow 1 - xa \in m_x$.

$\Rightarrow 1 \in m_x$ [as $a \in m_x$] Contradiction.

Hence. $1 - xa$ is a unit $\forall\ x \in A$.

$\Rightarrow a \in J$ ∎ ✓

11. $R : \mathbb{Z}[x]/(x^2+1)$

a) To show $\mathbb{Z}[x]/(x^2+1)$ is Principal ideal domain

Pf $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$ $\quad \mathbb{Z} \to \mathbb{Z}$

[Surjective map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ $\quad x \mapsto i$

$\ker \theta = (x^2+1)$]

Claim : $\mathbb{Z}[i]$ is Euclidean domain. Hence also a PID.

Define: $\theta : \mathbb{Z}[i] \to \mathbb{Z}^+$

$a + bi \mapsto a^2 + b^2 = (a+bi)(a-bi)$.

$\theta(xy) = \overline{xy}\, xy = x\bar{x}\, y\bar{y} = \theta(x)\,\theta(y)$.

~~Let $(a+bi) = (p+qi)\,x$~~

$a+bi \; ; \; p+qi \in \mathbb{Z}[i]$

$$\frac{a+bi}{p+qi} = \frac{(a+bi)(p-qi)}{p^2+q^2} \in \mathbb{Q}[i]$$

i.e $\frac{a+bi}{p+qi} = \alpha + \beta i \quad \alpha, \beta \in \mathbb{Q}$.

Let α', and β' be nearest integer to α, β respectively, i.e $|\alpha' - \alpha| \leq \frac{1}{2}$, $|\beta' - \beta| \leq \frac{1}{2}$

Let $r = [a+bi - (p+qi)(\alpha' + \beta' i)]$

then $\theta(r) = \theta(p+qi)\, \theta[\alpha + \beta i - \alpha' - \beta' i]$

$$= \theta(\beta+qi)\left[(\alpha-\alpha')^2 + (\beta-\beta')^2\right]$$

$$\leq \theta(p+qi)\left[\frac{1}{4} + \frac{1}{4}\right]$$

$$\leq \frac{\theta(p+qi)}{2} < \theta(p+qi).$$

Hence $\mathbb{Z}[i]$ satisfies euclidean algorithm with θ as it euclidean function.

$\Rightarrow \mathbb{Z}[i]$ is E.D. Hence a PID.

(b) $p \equiv 3 \bmod(4)$ prime To show $p\mathbb{Z}(i)$ is is prime ideal in $\mathbb{Z}[i]$.

Let $\alpha\beta \in p\mathbb{Z}[i]$.

$\Rightarrow \alpha\beta = p\alpha' \qquad \alpha' \in \mathbb{Z}[i]$.

$\Rightarrow \theta(\alpha\beta) = \theta(p\alpha') \Rightarrow \theta(\alpha)\theta(\beta) = p^2\,\theta(\alpha')$

$\Rightarrow p^2 \mid \theta(\alpha)\theta(\beta) \Rightarrow p \mid \theta(\alpha)$ or $p \mid \theta(\beta)$.

WLOG, Let $p \mid \Theta(\alpha)$

claim $\alpha \in p\mathbb{Z}[i]$.

Let $\alpha = a + bi \quad a, b \in \mathbb{Z}$.

$\Rightarrow p \mid a^2 + b^2$. Hence, either $p \mid a$ and $p \mid b$ [in which case we are done] or $p \nmid a$ and $p \nmid b$.

Let $p = 4k + 3 \quad k \in \mathbb{Z}$.

$a^2 + b^2 = 0 \bmod p$.

$\Rightarrow a^2 = -b^2 \bmod p$.

$\Rightarrow (a^2)^{2k+1} = (-b^2)^{2k+1} \bmod p$.

$\Rightarrow (a^{4k+2}) = -b^{4k+1} \bmod p$.

$\Rightarrow a^{p-1} = -b^{p-1} \bmod p$.

If $p \nmid a$ and $p \nmid b$ By Fermat's little theorem

$a^{p-1} = b^{p-1} = 1 \bmod p$.

$\Rightarrow 2a^{p-1} = 0 \bmod p \Rightarrow p \mid a$ contradiction.

Hence $p \mid a$ and $p \mid b \Rightarrow \alpha = a + bi \in p\mathbb{Z}[i]$.

$p\mathbb{Z}[i]$ is prime. ∎