210C HOMEWORK 1

KIM, SUNGJIN

Problem1.
(a) Since $E \subset \mathfrak{p} \Longleftrightarrow I \subset \mathfrak{p}$, we have $V(E) = V(I)$. Since $\mathfrak{p}$ is a prime ideal, $x^n \in \mathfrak{p}$ for some $n \geq 1$ if and only if $x \in \mathfrak{p}$, i.e. $I \subset \mathfrak{p} \Longleftrightarrow \sqrt{I} \subset \mathfrak{p}$. Thus, it follows that $V(I) = V(\sqrt{I})$.

(b) $V(\{0\}) = \{\mathfrak{p} \in \mathrm{Spec}(A) | 0 \in \mathfrak{p}\} = \mathrm{Spec}(A)$, and there is no prime ideal that contains 1, so $V(\{1\}) = \emptyset$.

(c) $\cup_{i \in A} E_i \subset \mathfrak{p} \Longleftrightarrow E_i \subset \mathfrak{p}$ for all $i \in A$. Thus, $V(\cup_{i \in A} E_i) = \cap_{i \in A} V(E_i)$.

(d) The proof is just the same as (c), $\sum_{i \in A} I_i \subset \mathfrak{p} \Longleftrightarrow I_i \subset \mathfrak{p}$ for all $i \in A$. Thus, $V(\sum_{i \in A} I_i) = \cap_{i \in A} V(I_i)$.

(e) Note that $V(IJ) \supset V(I \cap J) \supset V(I) \cup V(J)$, since $IJ \subset I \cap J$. In fact, $V(IJ) = V(I) \cup V(J)$ follows from the property of prime ideals, namely, $\mathfrak{p} \supset IJ \Longleftrightarrow \mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$. Hence, $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

(f) Consider $\mathcal{C} = \{V(I) | I \text{ is an ideal in } A\}$. By (b), $\mathcal{C}$ contains $\mathrm{Spec}(A)$ and $\emptyset$. Also, $\mathcal{C}$ contains arbitrary intersection by (d), and finite union by (e). Hence, $V(I)$ form the closed subsets of a topology on $\mathrm{Spec}(A)$.

(g) First note that $f^{-1}(\mathfrak{q})$ does not contain 1, otherwise $\mathfrak{q}$ would contain 1. Then for $a, b \in A$,

$$\begin{aligned} ab \in f^{-1}(\mathfrak{q}) &\Longleftrightarrow f(ab) \in \mathfrak{q} \\ &\Longleftrightarrow f(a)f(b) \in \mathfrak{q} \\ &\Longleftrightarrow f(a) \in \mathfrak{q} \text{ or } f(b) \in \mathfrak{q} \\ &\Longleftrightarrow a \in f^{-1}(\mathfrak{q}) \text{ or } b \in f^{-1}(\mathfrak{q}). \end{aligned}$$

Hence $f^{-1}(\mathfrak{q})$ is a prime ideal in A.

(h) For a commutative ring A, Spec(-):$A \mapsto \mathrm{Spec}(A)$. For a ring homomorphism $f : A \longrightarrow B$, $\mathrm{Spec}(f)$:$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ defined by $\mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$. Let $f : A \longrightarrow B$, $g : B \longrightarrow C$, be ring homomorphisms and $\mathfrak{q} \in \mathrm{Spec}(C)$, then we have $(gf)^{-1}(\mathfrak{q}) = f^{-1}(g^{-1}(\mathfrak{q}))$. Thus, $\mathrm{Spec}(g \circ f) = \mathrm{Spec}(f) \circ \mathrm{Spec}(g)$. It is clear that $1_A : A \longrightarrow A$ gives $\mathrm{Spec}(1_A) = 1_{\mathrm{Spec}(A)}$. Hence $\mathrm{Spec}(-)$ is a contravariant functor from commutative rings to topological spaces.

(i) Consider the inclusion $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, (0) is a maximal ideal in $\mathbb{Q}$, since $\mathbb{Q}$ is a field. However $i^{-1}((0)) = (0) \subset \mathbb{Z}$ is not a maximal ideal in $\mathbb{Z}$ since (0) is contained in an ideal $2\mathbb{Z}$ in $\mathbb{Z}$.

Problem2.
(a) $\mathrm{Spec}(A) - (D(s) \cap D(t)) = V(sA) \cup V(tA) = V(stA)$ by problem1(e). Thus, $V(stA) = \mathrm{Spec}(A) - D(st)$ implies the result $D(s) \cap D(t) = D(st)$.

(b) The statement is equivalent to $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$. Suppose first that a is nilpotent, then $a^n \in \mathfrak{p}$ for some $n \geq 1$ for any prime ideal $\mathfrak{p}$. This implies $a \in \mathfrak{p}$, thus $\sqrt{(0)} \subset \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$. For the other direction, suppose that a is not nilpotent. Then $S = \{a^n | n \geq 0\}$ form a multiplicative subset of A not containing 0. We have $S^{-1}A \neq 0$, so $\mathrm{Spec}(S^{-1}A) \neq \emptyset$. Thus there is a prime ideal in A which does not intersect S, in particular, does not contain a.

(c) If s is a unit, then clearly $s \notin \mathfrak{p}$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$. Thus, $D(s) = \mathrm{Spec}(A)$. Suppose that s is not a unit. Then there is a maximal ideal $\mathfrak{m}$ in A that contains sA. Since maximal ideal is prime, $\mathfrak{m} \notin D(s)$, so $D(s) \neq \mathrm{Spec}(A)$.

(d) We prove more general statement: Let I and J be two ideals in a ring A. Then $V(I) \subset V(J) \Longleftrightarrow J \subset \sqrt{I}$.
$\Leftarrow$) $V(I) = V(\sqrt{I}) \subset V(J)$.
$\Rightarrow$) $J \subset \bigcap_{\mathfrak{p} \supset J} \mathfrak{p} \subset \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \sqrt{I}$. The last equality follows from (b) applied to the ring A/I. Now apply this statement when $I = tA$, $J = sA$. Then the result follows.

(e) $D(s) = D(t)$ if and only if $sA \subset \sqrt{tA}$ and $tA \subset \sqrt{sA}$. This is in fact equivalent to $\sqrt{sA} = \sqrt{tA}$.

Problem3.
(a) The nonzero prime ideals in $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for some prime number $p \in \mathbb{Z}$. Thus, $\mathrm{Spec}(\mathbb{Z}) = \{(0)\} \cup \{p\mathbb{Z} |\ p \text{ is a prime number in } \mathbb{Z}\}$. Every ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Hence, we have $V(n\mathbb{Z}) = \{p\mathbb{Z} | p \text{ is a prime divisor of } n\}$ for nonzero, nonunit n, and we have $V(\mathbb{Z}) = \emptyset$, $V((0)) = \mathrm{Spec}(\mathbb{Z})$.

(b) Let P be a nonzero prime ideal in $A = \mathbb{Z}[X]$. Then the natural homomorphism $\mathbb{Z} \longrightarrow A/P$ has kernel $P \cap \mathbb{Z}$. This gives an embedding of $\mathbb{Z}/(P \cap \mathbb{Z})$ into A/P. Since A/P is an integral domain, so is $\mathbb{Z}/(P \cap \mathbb{Z})$. Thus, we have two cases

$$P \cap \mathbb{Z} = \begin{cases} p\mathbb{Z} & \text{for some prime } p \in \mathbb{Z} \\ (0) \end{cases}$$

(Case1) $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$:
By 3rd isomorphism theorem, we have

$$A/P \simeq \left(\mathbb{Z}/p\mathbb{Z}[X]\right) / (P/p\mathbb{Z}[X]).$$

In fact $\mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]$, and the LHS is an integral domain. It follows that $P/p\mathbb{Z}[X]$ is a prime ideal in $\mathbb{F}_p[X]$. Since $\mathbb{F}_p[X]$ is UFD, $P/p\mathbb{Z}[X] = (f(X))$ for some $f(X) \in \mathbb{F}_p[X]$ irreducible polynomial of degree ≥ 1 or $P/p\mathbb{Z}[X] = (0)$. Hence, in this case, we obtain $P = (p, f(X))$ or $P = p\mathbb{Z}[X]$ where f is irreducible mod p.
(Case2) $P \cap \mathbb{Z} = (0)$:
Consider the ideal $P\mathbb{Q}[X] \subset \mathbb{Q}[X]$, this is a proper prime ideal in $\mathbb{Q}[X]$. So,

$P\mathbb{Q}[X] = f(X)\mathbb{Q}[X]$ where f is irreducible over $\mathbb{Q}$. Further, we can assume that the polynomial f is primitive. We claim that $P = f(X)\mathbb{Z}[X]$. Suppose $h \in P$, $h = fg$ for some $g \in \mathbb{Q}[X]$. Taking content(Gauss lemma) on each side, we obtain $g \in \mathbb{Z}[X]$. Hence it follows that $P = f(X)\mathbb{Z}[X]$.
Now, we can write the result as follows:
Prime ideals P in $\mathbb{Z}[X]$ are one of the following forms:

$$P = \begin{cases} (0), & \\ (f(X)) & \text{for } f \in \mathbb{Z}[X] \text{ irreducible and primitive,} \\ (p) & \text{for some prime } p \in \mathbb{Z}, \\ (p, f(X)) & \text{for some prime } p \in \mathbb{Z}, \text{ and } f \text{ is irreducible mod } p. \end{cases} \tag{1}$$

Now, we characterize the topology on Spec($\mathbb{Z}[X]$). Let $I \subset \mathbb{Z}[X]$ be a proper ideal. Consider $I \cap \mathbb{Z} = n\mathbb{Z}$, we have two cases,
(Case1) $I \cap \mathbb{Z} = n\mathbb{Z}$ with $n \neq 0, \pm 1$:
Let $\mathfrak{p} \in V(I)$, i.e. $\mathfrak{p}$ is a prime ideal containing I. Then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p|n$. Fix a prime $p|n$. The ideal $I + p\mathbb{Z}[X] \subset \mathbb{Z}[X]$ maps to some ideal $(f(X)) \subset \mathbb{F}_p[X]$ by reducing mod p, since $\mathbb{F}_p[X]$ is a PID. Let f_i be distinct irreducible factors of f in $\mathbb{F}_p[X]$ if deg(f)> 0 , and enumeration of all irreducible polynomials of $\mathbb{F}_p[X]$ with 0 if $f = 0$. Thus, we have $(f(X)) \subset (f_i(X)) \subset \mathbb{F}_p[X]$ for each i. Pulling back these ideals to $\mathbb{Z}[X]$, we obtain $I \subset I + p\mathbb{Z}[X] \subset (p, f_i(X)) \subset \mathbb{Z}[X]$ for each i. Hence, the result

$$\begin{aligned} V(I) = \{&(p, f_{p,i}) \mid p|n, (I + p\mathbb{Z}[X])/(p\mathbb{Z}[X]) = (f_p(X)) \subset \mathbb{F}_p[X], \deg(f_p) > 0, f_{p,i} \text{ are} \\ &\text{distinct irreducible factor of } f \text{ in } \mathbb{F}_p[X]\} \\ &\bigcup \{(p, f_{p,i}) \mid p|n, (I + p\mathbb{Z}[X])/(p\mathbb{Z}[X]) = (0) \subset \mathbb{F}_p[X], f_{p,i} \text{ are enumeration of} \\ &\text{all irreducible polynomials of } \mathbb{F}_p[X] \text{ with } 0\}. \end{aligned}$$

(Case2) $I \cap \mathbb{Z} = (0)$:
Consider $I\mathbb{Q}[X] = (f(X)) \subsetneq \mathbb{Q}[X]$ with f being primitive. Then we obtain $I = f(X)\mathbb{Z}[X]$ by Gauss lemma. Let f_i be distinct irreducible factors of f, and $\tau_i \in \mathbb{C}$ be the corresponding roots of f_i. For each i, we need to find primes p such that (p, f_i) become proper. To do this, we use Gauss lemma again so that we obtain the result:

$$(p, f_i) \text{ is proper } \iff \frac{1}{p} \notin \mathbb{Z}[\tau_i].$$

Hence, we have,

$$\begin{aligned} V(I) = \{&(p, f_{i,j}) \mid f_i|f, \frac{1}{p} \notin \mathbb{Z}[\tau_i], ((f_i) + p\mathbb{Z}[X])/(p\mathbb{Z}[X]) = (f_i(X) \text{ mod } p) \subset \mathbb{F}_p[X], \\ &\deg(f_i \text{ mod } p) > 0, f_{i,j} \text{ are distinct irreducible factor of } f_i \text{ in } \mathbb{F}_p[X]\} \\ &\bigcup \{(f_i) | \ f_i|f \text{ irreducible}\}. \end{aligned}$$

Problem4.
(a) We have a canonical isomorphism $0 = M \otimes_R (R/I) \simeq M/IM$. From this we obtain $M = IM$. By Nakayama lemma, there exists $a \in I$ such that $(1 - a)M = 0$.

Suppose $1-a$ is not unit, then it is contained in some maximal ideal $\mathfrak{m} \subset R$. However, $a \in I \subset \text{Rad}(R) \subset \mathfrak{m}$. So, it follows $(1-a)+a = 1 \in \mathfrak{m}$, which is impossible. Hence, $1-a$ is a unit, and $(1-a)M = M = 0$.

(b) We have $M/N = (IM+N)/N = I \cdot (M/N)$. Since $I \subset \text{Rad}(R)$, we can apply (a) to obtain $M/N = 0$. Hence, $M = N$.

(c) Since $k \otimes_R M = (R/\mathfrak{m}) \otimes_R M \simeq M/(\mathfrak{m}M) = 0$, we see that $M = \mathfrak{m}M$. We can apply (a) with $I = \mathfrak{m}$, and $\text{Rad}(R) = \mathfrak{m}$, since $\mathfrak{m}$ is the unique maximal ideal in R. Hence, we obtain by (a) that $M = 0$.

(d) Let $N = Rx_1 + \cdots + Rx_m$ be a R-submodule of M. We have $(\mathfrak{m}M+N)/(\mathfrak{m}M) \supset (R/\mathfrak{m})\overline{x_i}$ for all $i = 1, \cdots, m$. Thus, it follows that

$$M/\mathfrak{m}M \supset (\mathfrak{m}M+N)/(\mathfrak{m}M) \supset (R/\mathfrak{m})\overline{x_1} + \cdots + (R/\mathfrak{m})\overline{x_m} = M/\mathfrak{m}M.$$

This implies $M = \mathfrak{m}M + N$. Since $\text{Rad}(R) = \mathfrak{m}$, we can apply (b) to deduce that $M = N$.