Rings and Modules

Trishan Mondal

Assignment-2

§ Problem 1

(Parts of Ex. 1.18 on page 10 of A − M)
If $f : A \to B$ is a ring homomorphism and I_1, I_2 are ideals in A and J_1, J_2 are ideals in B, give examples to show that the following containments can be strict:

$$(I_1 \cap I_2)^e \subset I_1^e \cap I_2^e; (I_1 : I_2)^e \subset I_1^e : I_2^e;$$
$$J_1^c + J_2^c \subset (J_1 + J_2)^c ; (J_1 : J_2)^c \subset J_1^c : J_2^c.$$

Solution.

- $\underline{(\mathbf{I_1} \cap \mathbf{I_2})^\mathbf{e} \subset \mathbf{I_1^e} \cap \mathbf{I_2^e}}$: Let, $f : \mathbb{Z}[X, Y] \to \mathbb{Z}$ a homomorphism that maps $f(X) = 10$ and $f(Y) = 14$ (Such a homomorphism always exist, because we can map any polynomial $f(X, Y) = \sum a_{ij} X^i Y^j \mapsto \sum a_{ij}(10)^i(14)^j$ This is clearly a homomorphism).

  Now consider, (X) and (Y). Here, $(X)^e = (10)$ and $(Y)^e = (14)$ so, $(X)^e \cap (Y)^e = (70)$ but $(X) \cap (Y) = (XY)$ so, $((X) \cap (Y))^e = (XY)^e = (140) \subset (70)$.

- $\underline{(\mathbf{I_1} : \mathbf{I_2})^\mathbf{e} \subset \mathbf{I_1^e} : \mathbf{I_2^e}}$: Consider, $f : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$. defined as, $f(x) = (x, 0)$. Take, $I_1 = \mathbb{Z}$ and $I_2 = \{0\}$. Then,

  $$I_1 : I_2 = \mathbb{Z} \Rightarrow (I_1 : I_2)^e = (\mathbb{Z} \times \{0\}).$$

  Now, $I_1^e = \mathbb{Z}\times\{0\}$ and $I_2^e = \{(0, 0)\}$ So, $I_1^e : I_2^e = \mathbb{Z}\times\mathbb{Z}$. From here we can see that, $\mathbb{Z}\times\{0\} \subset \mathbb{Z}\times\mathbb{Z}$.

- $\underline{\mathbf{J_1^c} + \mathbf{J_2^c} \subset (\mathbf{J_1} + \mathbf{J_2})^\mathbf{c}}$: Let, $\pi : \mathbb{Z}[x, y] \to \mathbb{Z}[x, y]/(x+y-1)$. Here, π is the natural projection map onto the quotient Ring. Let, $\bar{X}, \bar{Y}$ be the residue class of x and y in $\mathbb{Z}[x, y]/(x+y-1)$ respectively. Notice that,

  $$(\bar{X})^c = \pi^{-1}((\bar{X})) = (x)$$
  $$(\bar{Y})^c = \pi^{-1}((\bar{Y})) = (y).$$

  Now, $(\bar{X}) + (\bar{Y})$ in $\mathbb{Z}[x, y]/(x + y - 1)$ contains unity (as $\bar{X} + \bar{Y} = 1$ in the given Ring). So, $((\bar{X}) + (\bar{Y}))^c = (1)^c = \mathbb{Z}[x, y]/(x + y - 1)$.

- $\underline{(\mathbf{J_1} : \mathbf{J_2})^\mathbf{c} \subset \mathbf{J_1^c} : \mathbf{J_2^c}}$: Let, $f : \mathbb{Z} \to \mathbb{Z}[X], J_1 = \{0\}, J_2 = (X)$, . Now, $J_1^c = \{0\}$. So, $J_2^c = \{0\}$ which means $J_1^c : J_2^c = \mathbb{Z}$. but

  $$J_1 : J_2 = \{0\} \Longrightarrow (J_1 : J_2)^c = \{0\}$$

■

§ Problem 2

(Ex. 18, Chapter 1 of Atiyah-Macdonald)
For a ring A, the set X of all prime ideals of A is called the (prime) spectrum of A. It is a topological space where the closed sets are, by definition, the sets of the form $V(E) := \{$ all prime ideals of A containing $E\}$ for any subset E of A. For instance $V(\{0\}) = X$ and $V(\{1\}) = \emptyset$. Assume the properties mentioned in exercises 15 and 17 which describe this topological space; this is called the Zariski topology on X.
For psychological reasons, it is convenient to think of a point of X as x, but think of it as an ideal $\mathfrak{p}_x$, since x is really a prime ideal of A. Prove:
(a) $V(\mathfrak{p}_x) = \overline{\{x\}}$
(b) $\mathfrak{p}_x \subseteq \mathfrak{p}_y$ iff $y \in \overline{\{x\}}$
(c) X is a T_0-space; that is, given any two distinct points in X, at least one of them has an open neighbourhood not containing the other point.

Solution.

- (a) $V(\mathfrak{p}_x)$ contains x and is closed. Thus $V(\mathfrak{p}_x) \supseteq \overline{\{x\}}$. We can assume, $\overline{\{x\}} = V(E)$ for some subset E. Then $V(\mathfrak{p}_x) \subseteq V(E)$ implies $\mathfrak{p}_x \supseteq E$. So,for any other prime ideal $\mathfrak{p}$ containing $\mathfrak{p}_x$, it contains E, hence $V(\mathfrak{p}_x) \subseteq V(E) = \overline{\{x\}}$. ■
- (b) If $y \in \overline{\{x\}}$, then $y \in V(\mathfrak{p}_x)$ by part(a). This means $\mathfrak{p}_y$ contains $\mathfrak{p}_x$. Conversely, if $\mathfrak{p}_y$ contains $\mathfrak{p}_x$, then $\mathfrak{p}_y \in V(\mathfrak{p}_x) = \overline{\{x\}}$ by part(a). ■
- (c) If x, y are distinct point of X, then either $\mathfrak{p}_x$ contained in $\mathfrak{p}_y$ or $\mathfrak{p}_y$ contained in $\mathfrak{p}_x$. Without loss of generality, assume $\mathfrak{p}_x \subsetneq \mathfrak{p}_y$. Then, $y \notin \overline{\{x\}}$. Thus, $X \backslash \overline{\{x\}}$ is an open set containing y but not x. ■

§ Problem 3

(a). Let (A, δ) be a Euclidean domain; that is, δ is a Euclidean function on the domain A. Then, prove that the quotient and remainder are unique if and only if $\delta(a+b) \leq \max(\delta(a), \delta(b))$ for all $a, b, a+b \neq 0$.

(b). Let $d : A\backslash\{0\} \to \{0, 1, \cdots\}$ be a function (where A is a domain) satisfying only the second property of a Euclidean function; viz., for each $a, b \neq 0$, there exist $q, r \in A$ with $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$. Show that (A, δ) is a Euclidean domain, where $\delta(a) := \min\{d(ab) : b \neq 0\}$. In other words, δ satisfies both the properties of a Euclidean function.

(c). In $\mathbf{Z}[\sqrt{-7}]$, for each $k \geq 2$, show that there is an element which is a product of $2k, 2k+1, \cdots, 3k$ irreducible elements at the same time.

Solution.

(a) Assume remainder and quotient are unique but $\delta(a+b) > \delta(a), \delta(b)$ for some $a, b \neq 0$ then the two divisions

$$b = 0(a+b) + b$$
$$b = 1(a+b) - a$$

are well defined , as $\delta(b), \delta(-a) < \delta(a+b)$ and give different quotients and remainders. This is a contradiction !

Conversely, let $a = qb + r = q'b + r'$ with q, q' different or r, r' different.(So, $\delta(b) > \delta(r'), \delta(r)$). Which imples $(q - q')\, b = r - r'$. Now,

$$\begin{aligned} \delta(b) &\leq \delta(r - r') \\ &\leq \max\{\delta(r), \delta(-r')\} \\ &= \max\{\delta(r), \delta(r')\} \\ &< \delta(b) \end{aligned}$$

This gives us a contradiction. ■

(b) For nonzero a and b in A we have

$$\delta(ab) = \min\{d(abc) : c \neq 0\} \geq \min\{d(ac) : c \neq 0\} = \delta(a)$$

For any divisior a of x we must have $\delta(a) \leq \delta(x)$. Now, we will show A admits division with remainder with respect to δ. Pick a and b in A with $b \neq 0$. Set $\delta(b) = d(bc)$ for some nonzero $c \in A$. Using division of a by bc (which is nonzero) in (R, d) there are q_0 and r_0 in A such that,

$$a = (bc)q_0 + r_0, \quad r_0 = 0 \text{ or } d(r_0) < d(bc).$$

Take, $q = cq_0$ and $r = r_0$, so $a = bq + r$. If $r_0 = 0$ nothing to show, so we may assume $r_0 \neq 0$. It's not hard to see $d(bc) = \delta(b)$ and $\delta(r) \leq d(r)$. Now, the condition $d(r) = d(r_0) < d(bc)$ implies $\delta(r) < \delta(b)$. Thus

$$a = bq + r, \quad r = 0 \text{ or } \delta(r) < \delta(b).$$

Hence δ satisfies both the properties of an Euclidian function. ■

(c) We have,

$$2 \cdot 2 \cdot 2 = (1 + \sqrt{-7})(1 - \sqrt{-7}).$$

Now,

$$\begin{aligned} (2 \cdot 2 \cdot 2)(2 \cdot 2 \cdot 2) &= (1 + \sqrt{-7})(1 - \sqrt{-7})(1 + \sqrt{-7})(1 - \sqrt{-7}) \\ &= (2 \cdot 2 \cdot 2)(1 + \sqrt{-7})(1 - \sqrt{-7}) \end{aligned}$$

For any $k \geqslant 2$ Consider,

$$2^{3k} = \underbrace{(2 \cdot 2 \cdot 2) \ldots (2 \cdot 2 \cdot 2)}_{\text{there are } k \text{ many brackets}}$$

Let, $1 \leq l \leq k$. Notice that,

$$(2 \cdot 2 \cdot 2) \ldots \underbrace{(2 \cdot 2 \cdot 2) \cdots (2 \cdot 2 \cdot 2)}_{l \text{ many are there}} = (2 \cdot 2 \cdot 2) \ldots \left\{(1 + \sqrt{-7})(1 - \sqrt{-7})\right\} \ldots \left\{(1 + \sqrt{-7})(1 - \sqrt{-7})\right\}$$

So, then are $(3k - 3l + 2l) = 3k - l$ elements in the above product. If we vary l from 1 to k, we will get, 2^{3k} as product of $2k, \ldots, 3k$ elements at the sametime for $k \geq 2$. It is not hard to see that, 2, $(1 + \sqrt{-7}), (1 - \sqrt{-7})$ are irreducible in $\mathbb{Z}[\sqrt{-7}]$. ■

§ Problem 4

Show that a prime p is congruent to 1 or 3 mod 8 if, and only if, it is expressible as $x^2 + 2y^2$.

Solution. From the quadratic reciprocity theorem, we know for any odd prime p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

So, $\left(\frac{-2}{p}\right) = (-1)^{\frac{(p+5)(p-1)}{8}}$. If $p \equiv 1, 3(\text{mod}8)$ We must have $\left(-\frac{2}{p}\right) = 1$. So, there is $a \in \mathbb{N}$ such that,

$$a^2 \equiv -2(\text{mod}p).$$

$\therefore p \mid 2 + a^2$. If we look on $\mathbb{Z}[\sqrt{2}i]$,

$$p \mid (a + \sqrt{2}i)(a - \sqrt{2}i).$$

Since,$p \nmid a, p \nmid 1$ we have,

$$p \nmid a + \sqrt{2}i, p \nmid a - \sqrt{2}i.$$

So, p is not a prime in $\mathbb{Z}[\sqrt{2}i]$.(This is because $\mathbb{Z}[\sqrt{2}i$ is E.D which automatically implies it's an U.F.D) i.e. p is not an irreducible. There exist some $a, b, c, d \in \mathbb{Z}$ such that,

$$p = (a + i\sqrt{2}b)(c + i\sqrt{2}d)$$
$$\Rightarrow p^2 = \left(a^2 + 2b^2\right)\left(c^2 + 2d^2\right).$$

If, $a^2 + 2b^2 = p^2$ then, $c^2 + 2d^2 = 1$. Which means $c = \pm 1, d = 0$. but then, $p = \pm(a + i\sqrt{2}b)$ which is not possible. Similarly, $a^2 + 2b^2 = 1$ and $c^2 + 2d^2 = p^2$ not possible. only possibility is,

$$p = c^2 + 2d^2 = a^2 + 2b^2$$

On other hand if $p = 2x^2 + y^2$ then $p \equiv 1, 3(\text{mod}8)$.This is because we can write every natural number as $4k + 2, 4k \pm 1, 4k$ so any perfect square is $1, 4, 0(\text{mod}8)$. Now since p is odd prime y must be odd so, $p \equiv 1, 3(\text{mod}8)$ according to when $x \equiv 1, 4, 0(\text{mod}8)$. And Hence we are done. ■

§ Problem 5

(a) Prove that $\mathbb{R}[X, Y]/\left(X^2 + Y^2 - 1\right)$ is not a UFD.
(b) Prove that $\mathbb{C}[X, Y]/\left(X^2 + Y^2 - 1\ \right)$ is a PID (and so, a UFD).

Solution.

(a) Let, $R = \mathbb{R}[X, Y]/\left(X^2 + Y^2 - 1\right)$. Notice that in. R, any element can be written as $p(X)+Y(q(X))$. where, $p(X)$ and $q(X) \in \mathbb{R}[X]$.Define a function, $d : A \to \mathbb{R}[X]$ as,

$$p(X) + Yq(X) \mapsto p^2 + q^2\left(X^2 - 1\right).$$

d is a Ring Homomorphism. Let,X is reducible in R. Then, $X = \tilde{p}(X)\tilde{q}(X)$ Here X is the residue class of x in R. Now, (Assume none of $\tilde{p}, \tilde{q}$ is unit).

$$\begin{aligned} d(X) &= d(\tilde{p})d(\tilde{q}) \\ &= d(a+bY)(d(c+dY)) \\ \Rightarrow X^2 &= \left(a^2 + b^2\left(X^2-1\right)\right)\left(c^2 + d^2\left(X^2-1\right)\right) \end{aligned}$$

$\mathbb{R}[X]$ is U.F.D. So, if $a^2 + b^2\left(X^2-1\right) = 1$ then, $a = \pm 1, b = 0$ which means $a+bY$ is unit. Similarly, $c^2 + d^2\left(X^2-1\right) \neq 1$. only possibility, $X = a^2 + b^2\left(X^2-1\right)$. That is also not possible. So, X is not reducible in R.

Claim: X does not divide $1 \pm Y$.

Proof. If $X \mid 1 - Y$ then, $\quad X(a+bY) = 1 - Y$.

$$\Rightarrow X^2\left(a^2 + b^2\left(X^2-1\right)\right) = X^2$$

$\Rightarrow a^2 = 1$ and $b = 0$ But, $X \cdot 1 \neq 1 - Y$. So, It's not possible. Similarly, $X \nmid 1 + Y$. □

In R we Can write, $X^2 = 1 - Y^2 = (1-Y)(1+Y)$.So, X^2 has two different factorization. Hence R is not U.F.D. ■

(b) Since, $\det\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \neq 0$. We Can write, $\mathbb{C}[X,Y] = \mathbb{C}[X+iY, X-iY]$. From here we can reduce the following,

$$\mathbb{C}[X,Y]/\left(X^2+Y^2-1\right) = \mathbb{C}[Z,\bar{Z}]/(Z\bar{Z}-1)$$

It is not hard to see that,**

$$\mathbb{C}[Z,\bar{Z}]/(Z\bar{Z}-1) \cong \mathbb{C}\left[Z, \frac{1}{Z}\right]$$

Claim: Let, A be a Commutative Ring. With unity. Let, S be a multiplicative set of A. Then, $S^{-1}A$ (localiZation of A at S) is PID if A is PID.

Proof. Let, $\pi_S : A \to S^{-1}A$ is natural projrction map. Every ideal I $\subseteq S^{-1}A$ satisfy, $I^{ce} = I$ Now, I^c is ideal in A so, I^c is principal. Let, $I^c = \langle a \rangle$ then, $I^{ce} = \langle \pi_s(a) \rangle$. □

Notice that, $\mathbb{C}\left[Z, \frac{1}{Z}\right]$ is localization of $\mathbb{C}[Z]$ at $\{1, Z, Z^2, \cdots\}$, so, $\mathbb{C}\left[Z, \frac{1}{Z}\right]$ is a PID. ■

• **Remark:** (**) Here $\bar{Z}$ is not conjugate of Z it's just an symbol for $X - iY$. If we define a map $\varphi : \mathbb{C}[Z,\bar{Z}] \to \mathbb{C}\left[Z, \frac{1}{Z}\right]$ that maps each polynomial $f(Z,\bar{Z}) \mapsto f\left(Z, \frac{1}{Z}\right)$. It's not hard to see that φ is an ring homomorphism. Now we will look at, Ker(φ) If, $f \in \mathbb{C}[Z,\bar{Z}]$ belongs to the kernal, then $\left(\bar{Z} - \frac{1}{Z}\right)$ must divides f since Z is prime in $\mathbb{C}[Z,\bar{Z}]$ we can say $(\bar{Z}Z - 1) \mid Zf$.Now by degree analysis of $Z\bar{Z} - 1$ we can show taht it;s irreducible. Since $\mathbb{C}[Z,\bar{Z}]$ is U.F.D we can sy $Z\bar{Z} - 1 \mid f$ (because $\deg Z < \deg Z\bar{Z} - 1$). Which immidiately implies Ker(φ) $= (\bar{Z}Z - 1)$ and hence the isomorphism follows.

§ Problem 6

Prove that the following are NOT UFDs:
$\mathbb{Z}[2i], \mathbb{Z}[\sqrt{8}], \mathbb{Z} + X\mathbb{Q}[X]$

Solution.

- In $\mathbb{Z}[2i]$, $2i$ is an irreducible element. Now, $4 = (2i) \times (-2i)$ so, $2i \mid 4$ but we can also write, $4 = 2 \times 2$. $2i \nmid 2$ in $\mathbb{Z}[2i]$. So $2i$ is an irreducible which is not prime. So, $\mathbb{Z}[2i]$ is not U.F.D.

- If 2 is reducible in $\mathbb{Z}[\sqrt{8}]$ then, $\exists a, b, c$ d $\in \mathbb{Z}$, with $a + b\sqrt{8}$, and $c + d\sqrt{8}$; not unit in $\mathbb{Z}[\sqrt{8}]$such that,

$$2 = (a + \sqrt{8}b)(c + \sqrt{8d})$$

Now, $4 = |(a^2 - 8b^2)\,(c^2 - 8d^2)|$, which implies $|a^2 - 8b^2| = |c^2 - 8d^2| = 2$, as $a + b\sqrt{8}$ and $c + d\sqrt{8}$ are not unit. So, $|a^2 - 8b^2| = 2$ is the requirement for this case. But,

$$\left|\frac{a^2}{2} - 4b^2\right| = 1$$
$$\Rightarrow \pm\frac{a^2}{2} + 1 = 4b^2$$

In this case, LHS is not even (as $2 \mid a \Rightarrow 4 \mid a^2$) and RHS always is even. So, 2 is irreducible in $\mathbb{Z}[\sqrt{8}]$. Now,

$$2 \mid (\sqrt{8} + 2)(\sqrt{8} - 2) = 4 = 2 \cdot 2$$
$$\text{but } 2 \nmid \sqrt{8} + 2, 2 \nmid \sqrt{8} - 2$$

So, 2 is not prime. i.e. $\mathbb{Z}[\sqrt{8}]$ is not a U.F.D.

- Let, $R = \mathbb{Z} + X\mathbb{Q}[X]$. Since R is a subring of an integral domain, R is an integral domain. We know only constant terms are unit in $\mathbb{Q}[x]$ and the only units in $\mathbb{Z}$ are ± 1. Thus the only units in R are ± 1.

  Notice that, $\pm p$ (where p is a prime integer), are irreducible in R. If $f = c + xg(x) \in R$, then $f = c\,(1 + c^{-1}xg(x))$ is reducible unless $c = \pm 1$. Therefore all irreducibles are $\pm p, \pm 1 + xg(x)$.

  We will show that x can't be factorized in terms of irreducible in R.If $x = (c + xg(x))(d + xh(x)) = cd + (ch_0 + dg_0)\,x + \cdots$. Since the degree of $x = 1$, the degrees of $g(x), h(x)$ are 0,1 in some order. We may assume $g(x) = c, h(x) = d + ex$. Then $x = c(d + ex) = cd + cex$. Either $c = 0$ or $d = 0$. But $c \neq 0$, so $d = 0$, whence $cex = 1$ and $ce = 1$.Which means c is unit in $\mathbb{Z}$. So, $x = (\pm 1)(\pm x)$. But we have shown that $\pm x$ are not irreducibles in R. Therefore, R is not a UFD. ■

• **Remark:** Let, $p \mid (c + xg(x))(d + xh(x)) = cd + xf(x)$. Then $p \mid cd$, so $p \mid c$ or $p \mid d$. Since p is a unit is $\mathbb{Q}, p \mid xg(x)$ and $p \mid xh(x)$. Therefore, p divides one of the factors and is prime. Similarly, if $1 + xf(x) \mid (c + xg(x))(d + xh(x)) = cd + xq(x)$, then the factorization holds in $\mathbb{Q}$ and here,$1 + xf(x)$ divides one of the factors and it is prime.
In this ring every irreducible is prime still ti's not a U.F.D. So this means the given ring is not even a Factorization Domain.