Name——————————————, ID ————————

 © copyright Ayman Badawi 2017

HW ONE: MTH 420, Spring 2018

Ayman Badawi

QUESTION 1. Let R be a commutative ring, I be an ideal of R (it is possible that $I = R$), and $A = R(+)I$. Define + and $\cdot$ on A as following:
$(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac, ad + bc)$. Then $(A, +, .)$ is a commutative ring (do not show that)

(i) Show that $1_A = (1_R, 0_R)$ (it is clear that $0_A = (0_R, 0_R)$) **Trivial, no comments**

(ii) Let P be a prime ideal of A. Show that $P = L(+)I = \{(a, b) \mid a \in L \text{ and } b \in I\}$ for some prime ideal L of R.

Solution: First we show that $P = L(+)I$ for some proper ideal L of R. Let $L = \{a \in R \mid (a, i) \in P$ for some $i \in I\}$. We show that L is an ideal of R. Let $x, y \in L$. We show $x - y \in L$. Since $x, y \in L$, we have $(x, a), (y, b) \in P$ for some $a, b \in I$. Since P is an ideal of A, $(x, a) - (y, b) = (x - y, a - b) \in P$. Thus $x - y \in L$. Let $x \in L$ and $r \in R$. We show $rx \in L$. Since $x \in L$, we have $(x, c) \in P$ for some $c \in I$. Since P is an ideal of A, $(r, 0)(x, c) = (rx, rc) \in P$. Thus $rx \in L$. Thus L is an ideal of R. It is clear that $P \subseteq L(+)I$. We show $L(+)I \subseteq P$. First we show that $0(+)I \subseteq P$. Let $(0, i) \in 0(+)I$. Then $(0, i)^2 = (0, 0) \in P$. Since P is prime, $(0, i) \in P$ (This is the first time we used the hypothesis that P is prime). Thus $0(+)I \subseteq P$. Now let $(a, b) \in L(+)I$. We show $(a, b) \in P$. Since $a \in L$, we have $(a, v) \in P$ for some $v \in I$. Since I is an ideal of R, there exists $w \in I$ such that $v + w = b$. Hence $(a, v) + (0, w) = (a, v + w) = (a, b) \in P$. Thus $P = L(+)I$. Since P is prime, $P \neq A$. Thus L is a proper ideal of R. We show L is a prime ideal of R. Assume $xy \in L$ for some $x, y \in R$. We show that $x \in L$ or $y \in L$. Since $xy \in L$, we have $(x, s)(y, d) = (xy, sy + xd) \in P = L(+)I$ for some $s, d \in I$. Since P is prime, we have $(x, s) \in P$ or $(y, d) \in P$. Thus $x \in L$ or $y \in L$.

(iii) If M is a maximal ideal of A? can you determine the form of M? i.e., see (ii)

Solution: Since M is a maximal ideal of A, M is a prime ideal of A. Hence $M = L(+)I$ for some prime ideal L of R. We show that L is a maximal ideal of R. Pick $r \in R \setminus L$. We show that $rx + h = 1$ for some $x \in R$ and $h \in L$. Since $r \notin L$, $(r, 0) \notin M$. Since M is a maximal ideal of A, we have $(1, 0) = (r, 0)(x, f) + (h, k)$ for some $x \in R, h \in L$, and $f, k \in I$. Thus $1 = rx + h$. Hence L is a maximal ideal of R.

(iv) Let $U(A)$ be the set of all units of A (i.e., set of all invertible elements of A). Show that $U(A) = U(R)(+)I$.

Solution: Let $(v, k) \in U(A)$. Then $(u, k)(d, v) = (1, 0) \in A$ for some $(v, d) \in A$. Thus $d = u^{-1}$ in R. Thus $U(A) \subseteq U(R)(+)I$. Now Let $x \in U(R)$ and $i \in I$. We show $(x, i) \in U(A)$. We need to construct an element $h \in A$ such that $(x, i)h = (1, 0)$. Let $h = (x^{-1}, -ix^{-2})$. Note that $-ix^{-2} \in I$ since I is an ideal. Now $(x, i)h = (x, i)(x^{-1}, -ix^{-2}) = (1, 0)$. Thus $(x, i) \in U(A)$, and hence $U(A) = U(R)(+)I$.

(v) Convince me that $Z(A) = Z(R)(+)I$.

Let $(a, c) \in Z(A)$ and we may assume that $(a, c) \neq (0, 0)$. Hence there is $(f, h) \in A$ such that $(a, c)(f, h) = (0, 0)$. Thus $a \in Z(R)$. Hence $Z(A) \subseteq Z(R)(+)I$. Now we show $Z(R)(+)I \subseteq Z(A)$. Let $i \in I$ such that $i \neq 0$. Since $(0, i)(0, i) = (0, 0)$, we conclude that $(0, i) \in Z(A)$. Thus $0(+)I \subseteq Z(A)$. Assume $a \in Z(R)$ and $i \in I$ such that $a \neq 0$. We show that $(a, i) \in Z(A)$. We need to construct an element $h \in Z(A)$ such that $(a, i)h = (0, 0)$ and $h \neq (0, 0)$. Since $a \in Z(R)$ and $a \neq 0$, there exists $b \in Z(R)$ such that $b \neq 0$ and $ab = 0$. Now suppose $bk = 0$ for every $k \in I$. Then $(a, i)(b, 0) = (0, 0)$ and $(a, i) \in Z(A)$. Assume that $bm \neq 0$ for some $m \in I$. Then $m \neq 0$. Then $(a, i)(0, bm) = (0, abm) = (0, 0)$ (since $ab = 0$). Tthus $(a, i) \in Z(A)$. Done

(vi) Let $N(A) = \{x \in A \mid x^n = (0, 0)\}$. Convince me that $N(A)$ is never an empty set. Can you describe $N(A)$? (see (ii))

claim: $N(A) = N(R)(+)I$. Let $(x, i) \in N(A)$. It is clear that $x \in Ni(R)$. Thus $N(A) \subseteq N(R)(+)I$. Assume that $(a, i) \in N(R)(+)I$. We show that $(a, i) \in N(A)$. By induction, we see that $(a, i)^n = (a^n, na^{n-1}i)$ for every $n \geq 2$. Since $(a, i) \in N(R)(+)I$, we conclude that $a \in N(R)$ and there is a positive integer $m \geq 2$ such that $a^m = 0$. Hence $(a, i)^{m+1} = (a^{m+1}, (m + 1)a^m i) = (0, 0)$. Thus $(a, i) \in N(A)$. Done

QUESTION 2. Let $A = Z_{36}(+)6Z_{36}$. (note $6Z_{36}$ is the ideal of Z_{36} generated by 6) Then in view of question (1) find the following

(i) All prime ideals of A

(ii) All maximal ideals of A

(iii) $U(A)$

(iv) $Z(A)$

(v) $N(A)$

Solution Trivial calculations using the results in Question one. All of you got it right

QUESTION 3. Choose $n \geq 1$ distinct prime numbers in Z, say $p_1, ..., p_n$. Let $D = \{a/b \in Q \mid a \in Z, b \in Z^*$ and $p_i \nmid b$ for every $1 \leq i \leq n\}$.(Hint: note that if v, k are positive integers in Z, then $gcd(v, k) = c_1 v + c_2 k$ for some $c_1, c_2 \in Z)$

(i) Prove that $(D, +, \cdot)$ is a subring of Q with identity $1 = 1_Q$. Here $+$ and $\cdot$ are the normal operation on Q

Solution: By construction of D using the normal addition and multiplication, it is clear that $x - y \in D$ and $xy \in D$. Done

(ii) Prove that D has exactly n distinct maximal ideal.

Solution: First note that $Z \subset D \subset Q$. Also note that when we write $x = a/b \in D$, then it is understood that $p_i \nmid b$ for every $1 \leq i \leq n$. For each $1 \leq i \leq n$. We show that $p_i D$ is a maximal ideal of D. Since $p_i D = span\{p_i\}$ it is trivial that $p_i D$ is an ideal. We show that $p_i D \neq D$. Suppose that $p_i x = 1 in D$ for some $x \in D$. Then $x = 1/p_i \notin D$, a contradiction (note that D consists of elements of the form a/b where $a, b in Z$ and $p_i \nmid b$ for every $1 \leq i \leq n$). Thus $p_i D$ is a proper ideal of D. Assume $\frac{a}{b}$ (written in reduced form)$\in D \setminus p_i D$. We show that $x\frac{a}{b} + y = 1$ for some $x \in D$ and $y \in p_i D$. Since $\frac{a}{b} \notin p_i D$, we conclude that $p_i \nmid a$. Thus $gcd(a, p_i) = 1$. Hence $1 = hp_i + ka$ for some $h, k \in Z$. Thus $b = bhp_i + bka$. Hence $1 = \frac{b}{b} = \frac{bhp_i}{b} + \frac{bka}{b}$. Let $y = \frac{bhp_i}{b}$. Then $y \in p_i D$. Let $x = bk$. Then $bk \in D$. Thus $1 = x\frac{a}{b} + y$ as desired. Hence $p_i D$ is a maximal ideal of D for every $1 \leq i \leq n$. Hence D has at least n maximal ideals. Now we show that D will not have more than n maximal ideals. Suppose that M is a maximal ideal of D and $M \neq p_i D$ for every $1 \leq i \leq n$. Then there exists an $x = a/b \in M$ such that $x \notin p_i D$ for every $1 \leq i \leq n$. Hence $a \neq 0$ and $p_i \nmid a$ for every $1 \leq i \leq n$. Hence $b/a \in D$. Since $(a/b)(b/a) = 1 in D$, we conclude that $x = a/b$ is a unit of D, a contradiction (since proper ideals do not contain units). Thus D has exactly n maximal ideals.

(iii) Say $M_1, ..., M_n$ are the maximal ideals of D, and let $J(D) = \cap_{i=1}^{n} M_i$. Find $J(D)$

Solution: By the proof of (ii), each $M_i = p_i D$ for every $1 \leq i \leq n$. Hence $J(D) = M_1 \cap M_2 \cap \cdots \cap M_n = p_1 p_2 \cdots p_n D = span\{p_1 p_2 \cdots p_n\}$.

(iv) Prove that $u + m$ is a unit of D for every $m \in J(D)$ and for every $u \in U(D)$.

Solution Let $u = a/b$ be a unit in D. Hence $a \neq 0$ and $(a/b)(b/a) = 1$ in D, and thus $b/a \in D$. Thus $p_i \nmid a$ for every $1 \leq i \leq n$. Also note that since $u = a/b \in D$, we conclude that $p_i \nmid b$ for every $1 \leq i \leq n$. Let $m \in J(D)$. Them $m = \frac{p_1 p_2 \cdots p_n h}{d}$, for some $h/d \in D$ (note that $p_i \nmid d$ for every $1 \leq i \leq n$). Now $u + m = \frac{a}{b} + \frac{p_1 p_2 \cdots p_n h}{d} = \frac{da + bp_1 p_2 \cdots p_n h}{bd}$. Now note that $p_i \nmid da + bp_1 p_2 \cdots p_n h$ for every $1 \leq i \leq n$ (because $p_i \mid bp_1 p_2 \cdots p_n h$ and $p_i \nmid ab$ for every $1 \leq i \leq n$). Thus $W = \frac{bd}{da + bp_1 p_2 \cdots p_n h} \in D$. Hence (u + m)w = 1 in D. Thus $u + m$ is a unit of D.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com