Rings and modules - Problem set 2 solutions

Solved on Tuesday 26.09

Problem 1. Let $R = (R, +, \cdot)$ be a ring. For $r, s \in R$, define

$$r \circ s \coloneqq sr.$$

Show that $R^{\mathrm{op}} = (R, +, \circ)$ is a ring, called the *opposite ring* of R.

Solution. Clearly R^{op} is an additive group since addition in R^{op} is the same. Let $r, s, t \in R^{\mathrm{op}}$. Using associativity of multiplication in R, we have

$$r \circ (s \circ t) = r \circ (ts) = (ts)r = t(sr) = t(r \circ s) = (r \circ s) \circ t,$$

and so multiplication in R^{op} is associative too. Furthermore, we have

$$r \circ (s + t) = (s + t)r = sr + tr = r \circ s + r \circ t$$

and

$$(r + s) \circ t = t(r + s) = tr + ts = r \circ t + s \circ t,$$

which shows distributivity of $\circ$ with respect to addition in R^{op}. Hence R^{op} is a ring.

Problem 2. (Exercise 10.2.7 in the book.) Let F be a field and R be a ring. Let $\phi : F \to R$ be a ring homomorphism. Show that $\phi = 0$ or ϕ is injective.

Solution. The kernel $\operatorname{Ker} \phi$ of ϕ is an ideal of F. Since F is a field, the only ideals of F are (0) and F by Problem 3. If $\operatorname{Ker} \phi = (0)$, then ϕ is injective by Proposition 4.2(7). If $\operatorname{Ker} \phi = F$ then $\phi = 0$.

Problem 3. (Exercises 10.1.1 and 10.1.2 in the book) Let R be a unital ring.

(a) Show that R is a division ring if and and only if the only right (or left) ideals in R are the trivial ideals (0) and R.

(b) Assume that R is also commutative. Show that R is a field if and only if the only two-sided ideals in R are the trivial ideals $\{0\}$ and R.

Solution.

(a) Assume first that R is a division ring and let I be an ideal in R. Assume that $I \neq (0)$ and let $a \in I \setminus \{0\}$. Then a is a unit since R is a division ring. Therefore, for every $r \in R$ we have that $r = ra^{-1}a \in I$. We conclude that $R \subseteq I$ and so $R = I$.

Assume now that the only ideals of R are (0) and R. Let $r \in R \setminus \{0\}$. Consider the right ideal rR. Since R is unital, we have that $rR = \{rs \mid s \in R\}$. Hence $r = r1 \in rR$ and so $rR \neq (0)$. Therefore, we have that $rR = R$. Hence $1 \in R = rR$ and so there exists $s \in R$ with $rs = 1$. This shows that r is a unit and so we conclude that R is a division ring.

(b) Assume first that R is a field. Then R is a division ring and so it follows by part (a) that the only right ideals in R are (0) and R. But right and two-sided ideals coincide since R is commutative, and so this direction is proved.

Assume now that the only two-sided ideals in R are (0) and R. Since R is commutative, these are the only right ideals in R as well. Hence by part (a) we conclude that R is a division ring. Since R is also commutative, we obtain that R is a field.

Problem 4. (a) Let $n, m \in \mathbb{Z}$. Show that $(n) \subseteq (m)$ if and only if m divides n.

(b) (Exercise 10.1.4 in the book.) Find all ideals in $\mathbb{Z}/(10)$.

Solution.

(a) Assume that $(n) \subseteq (m)$. Then $n \in (n)$ implies that $n \in (m) = m\mathbb{Z}$ and so $n = mk$ for some $k \in \mathbb{Z}$. In particular m divides n.

Assume now that m divides n. Then $n = mk$ for some $k \in \mathbb{Z}$. In particular $n \in (m)$ and so $(n) \subseteq (m)$, since (n) is the smallest ideal containing n and (m) is an ideal containing n.

(b) By Corollary 4.6 we have that every ideal of $\mathbb{Z}/(10)$ is of the form $I/(10)$, where I is an ideal of $\mathbb{Z}$ containing (10). Since $\mathbb{Z}$ is a PID, ideals of $\mathbb{Z}$ are of the form (n) for an integer $n \in \mathbb{Z}$. Since $(n) = (-n)$ we may assume that $n \geq 0$. Hence ideals of $\mathbb{Z}/(10)$ are of the form $(n)/(10)$ where $(10) \subseteq (n)$ and $n > 0$. By part (a) we have that $(10) \subseteq (n)$ if and only if n divides 10. Since the positive divisors of 10 are $1, 2, 5, 10$, we conclude that the ideals of $\mathbb{Z}/(10)$ are $(1)/(10) = \mathbb{Z}/(10)$, $(2)/(10)$, $(5)/(10)$ and $(10)/(10) = (0)$.

Problem 5. (Exercise 10.3.4 in the book.) Let R be a unital ring and $e \in R$ be an idempotent. Show that $eR \oplus (1-e)R$ is a direct sum of right ideals and that $eR \oplus (1-e)R = R$.

Solution. We have that eR and $(1-e)R$ are right ideals. Hence $eR + (1-e)R$ is an ideal in R. Let $r \in R$. Then

$$r = 1r = (e + 1 - e)r = er + (1-e)r \in eR + (1-e)R$$

and so $R \subseteq eR + (1-e)R$. We conclude that $R = eR + (1-e)R$. It remains to show that the sum is direct. For this it is enough to show that $(eR) \cap ((1-e)R) = (0)$. Let $r \in (eR) \cap ((1-e)R)$. Then $r = es$ and $r = (1-e)t$ for some $s, t \in R$. Then $es = (1-e)t$. Then $e = e^2$ gives

$$es = e^2 s = e(1-e)t = (e - e^2)t = (e-e)t = 0,$$

and so $es = 0$. Hence $r = es = 0$ and so $(eR) \cap ((1-e)R) = (0)$, which concludes the proof.

Problem 6. (Exercise 10.4.3 in the book.) Prove that the ideal (X^4+4) is not a prime ideal in the polynomial ring $\mathbb{Q}[X]$.

Solution. Assume to a contradiction that $(X^4 + 4)$ is a prime ideal in $\mathbb{Q}[X]$. We have

$$(X^2 + 2X + 2)(X^2 - 2X + 2) = X^4 + 4 \in (X^4 + 4),$$

and since $\mathbb{Q}[X]$ is a commutative ring and (X^4+4) is a prime ideal, we conclude that $X^2+2X+2 \in (X^4+4)$ or $X^2-2X+2 \in (X^4+4)$ by Theorem 6.8. Assume that $X^2+2X+2 \in (X^4+4)$. Then $X^2+2X+2 = (X^4+4)p(X)$ for some polynomial $p(X) \in \mathbb{Q}[X]$. Clearly $p(X) \neq 0$. Then

$$2 = \deg(X^2 + 2X + 2) = \deg((X^4 + 4)p(X)) = \deg(X^4 + 4) + \deg(p(X)) \geq 4,$$

which is a contradiction. Similarly we reach a contradiction if we assume that $X^2 - 2X + 2 \in (X^4 + 4)$. Hence we conclude that $(X^4 + 4)$ is a prime ideal in $\mathbb{Q}[X]$.

Problem 7. Let R be a commutative ring and I an ideal in R. Show that R/I is an integral domain if and only if I is a prime ideal.

Solution. We use the equivalent characterization for a prime ideal in a commutative ring coming from Theorem 6.8, that is, an ideal I is prime if for all $r, s \in R$ we have that if $rs \in I$, then $r \in I$ or $s \in I$.

Assume first that R/I is an integral domain and we show that I is a prime ideal. Let $r, s \in R$ with $rs \in I$. Then in R/I we have

$$(r + I)(s + I) = rs + I = 0 + I.$$

Since R/I is an integral domain, we have that $r + I = 0 + I$ or $s + I = 0 + I$ in R/I or equivalently $r \in I$ or $s \in I$. Hence I is a prime ideal in R.

Assume now that I is a prime ideal in R and we show that R/I is an integral domain. Let $r+I, s+I \in R/I$ and assume that $(r + I)(s + I) = 0 + I$. Since $(r + I)(s + I) = rs + I$, we conclude that $rs + I = 0 + I$ and so $rs \in I$. Since I is a prime ideal in a commutative ring, we have that $r \in I$ or $s \in I$. But then $r + I = 0 + I$ or $s + I = 0 + I$ and so R/I is an integral domain.

Problem 8. (Third isomorphism theorem for rings.) Let R be a ring. Let I and J be ideals in R such that $I \subseteq J$. Show that the quotient ring $(R/I)/(J/I)$ is isomorphic to the quotient ring R/J. *(Hint: use the first isomorphism theorem for rings.)*

Solution. We define a map $f : R/I \to R/J$ by $f(r+I) = r+J$ for every $r+I \in R/I$. We claim that f is well-defined. Indeed, if $r+I = s+I$ for $r+I, s+I \in R/I$, then $r-s \in I \subseteq J$ and so $r-s \in J$. Then $r+J = s+J$ and so

$$f(r+I) = r+J = s+J = f(s),$$

as required. Moreover, we claim that f is a ring homomorphism. Indeed, for any $r+I, s+I \in R/I$ we have

$$f((r+I)+(s+I)) = f((r+s)+I) = (r+s)+J = (r+J)+(s+J) = f(r+I)+f(s+I),$$

and

$$f((r+I)(s+I)) = f(rs+I) = rs+J = (r+J)(s+J) = f(r+I)f(s+I),$$

as required. We also claim that f is surjective. Indeed, let $r+J \in R/J$. Then $r \in R$ and so $r+I \in R/I$. Then $f(r+I) = r+J$, showing surjectivity of f. Hence $\operatorname{Im} f = R/J$. Finally, we claim that $\operatorname{Ker} f = J/I$. Indeed, let $a+I \in \operatorname{Ker} f$. Then $f(a+I) = 0+J$ and so $a+J = 0+J$. Hence $a \in J$ and so $a+I \in J/I$. This shows that $\operatorname{Ker} f \subseteq J/I$. For the other inclusion, let $a+I \in J/I$. Then $a \in J$ and $f(a+I) = a+J = 0+J$. Hence $a+I \in \operatorname{Ker} f$ and so we conclude that $\operatorname{Ker} f = J/I$. But then by the first isomorphism theorem for rings (Theorem 4.4) we conclude that

$$(R/I)/(J/I) = (R/J)/(\operatorname{Ker} f) \cong \operatorname{Im} f = R/J,$$

as required.

Problem 9. (Second isomorphism theorem for rings.) Let R be a ring. Let S be a subring of R and let I be an ideal in R. Show that the following hold.

(a) The sum $S+I \coloneqq \{s+a \mid a \in S, a \in I\}$ is a subring of R.

(b) The intersection $S \cap I$ is an ideal in S.

(c) The quotient rings $S/(S \cap I)$ and $(S+I)/I$ are isomorphic.

(Hint: use the first isomorphism theorem for rings.)

Solution.

(a) Since I is an ideal in R, it is also a subring of R. Since the sum of two subrings is a subring, we conclude that $S+I$ is a subring of R.

(b) Since $0 \in S \cap I$, we have that $S \cap I \neq \varnothing$. Let $a, b \in S \cap I$ and $s \in S$. Then $a, b \in S$ and $a, b \in I$ and so $a-b \in S$ and $a-b \in I$ since S and I are subrings. Hence $a-b \in S \cap I$. Moreover, since $a \in S$ and $s \in S$ we have that $sa \in S$ and since $a \in I$ and $s \in R$ we have that $sa \in I$. Hence $sa \in S \cap I$ and $S \cap I$ is a left ideal of S. Similarly it is also a right ideal of S and so $S \cap I$ is a two-sided ideal of S.

(c) Clearly $I \subseteq S+I \subseteq R$ and since I is an ideal of R, it follows that I is an ideal of $S+I$. Hence $(S+I)/I$ is well-defined. We define a map $f : S \to (S+I)/I$ by $f(s) = s+I$ for every $s \in S$. We claim that f is a ring homomorphism. Indeed, for any $s, t \in S$ we have

$$f(s+t) = (s+t)+I = (s+I)+(t+I) = f(s)+f(t),$$

and

$$f(st) = st+I = (s+J)(t+J) = f(s)f(t),$$

as required. We also claim that f is surjective. Indeed, let $(s+a)+I \in (S+I)/I$ for some $s \in S$ and $a \in I$. Then $(s+a)+I = s+I$ since $s+a-s = a \in I$. Hence $f(s) = s+I = (s+a)+I$ showing surjectivity of f. Hence $\operatorname{Im} f = R/J$. Finally, we claim that $\operatorname{Ker} f = S \cap I$. Indeed, let $s \in \S \cap I$. Then $s \in I$ and $f(s) = s+I = 0+I$. This shows that $S \cap I \subseteq \operatorname{Ker} f$. Now let $s \in \operatorname{Ker} f$. Then $f(s) = 0+I$

and $f(s) = s + I$ imply that $s + I = 0 + I$. Hence $s \in I$ and since $s \in S$ we have that $s \in S \cap I$. This shows that $\operatorname{Ker} f \subseteq \cap I$. But then by the first isomorphism theorem for rings (Theorem 4.4) we conclude that

$$S/(S \cap I) = S/(\operatorname{Ker} f) \cong \operatorname{Im} f = (S + I)/I,$$

as required.

Problem 10. (Exam December 2011, problem 3.) Let R be a unital ring. Show that every proper left ideal I in R is contained in a maximal left ideal of R.

Solution. Let $I \subseteq R$ be a left ideal with $I \neq R$. Set

$$S = \{J \text{ left ideal in } R \mid I \subseteq J \text{ and } J \neq R\}.$$

Since $I \in S$, we have that $S \neq \varnothing$. We claim that $(S, \subseteq)$ is a poset. Clearly for any $J \in S$ we have $J \subseteq J$ and so $\subseteq$ is reflexive. For $J, J' \in S$ we have that $J \subseteq J'$ and $J' \subseteq J$ imply that $J = J'$ and so $\subseteq$ is antisymmetric. Finally for $J, J', J'' \in S$ we have that $J \subseteq J'$ and $J' \subseteq J''$ and so $J \subseteq J''$.

Now let C be a nonempty chain in S, that is a nonempty subset $C \subseteq S$ such that for all $J, J' \in C$ one of $J \subseteq J'$ and $J' \subseteq J$ holds. We claim that

$$U = \bigcup_{J \in C} J$$

is a left ideal in R. Since $C \neq \varnothing$, we have that $U \neq \varnothing$. Let $a, b \in U$ and $r \in R$. Then there exist $J_1, J_2 \in C$ such that $a \in J_1$ and $b \in J_2$. Since C is a chain, one of $J_1 \subseteq J_2$ and $J_2 \subseteq J_1$ holds. Without loss of generality we assume that $J_1 \subseteq J_2$. Then $a, b \in J_2$ and so

- $a - b \in J_2 \subseteq U$ implies $a - b \in U$, and
- $ra \in J_2 \subseteq U$ implies $ra \in U$.

Hence U is a left ideal in R. Since $I \subseteq J$ for all $J \in C$, we have that $I \subseteq U$. Since $J \neq R$ for all $J \in C$, we have that $1 \notin J$ for all $J \in C$ (since if 1 belongs to a left ideal then $r = r1$ belongs to that ideal for all $r \in R$). Hence $1 \notin U$ either, and so $U \neq R$. Therefore $U \in S$ and U is an upper bound of C by construction. By Zorn's lemma there exists a maximal element $M \in S$. Since $I \subseteq M$, it is enough to show that M is a maximal left ideal. Assume $M \subseteq N$ for some left ideal N of R with $N \neq R$. Then $I \subseteq M \subseteq N$ implies that $N \in S$ and so $M = N$ since M is a maximal element. Therefore M is a maximal left ideal of R containing I, as required.

Problem 11. (Exercise 10.2.4 in the book.) Let R be a commutative ring. Let N be the set of all nilpotent elements in R.

(a) Show that N is a nil ideal.

(b) Show that the ring R/N has no nonzero nilpotent elements.

(c) Give an example to show that if R is not commutative, then N is not necessarily an ideal.

Solution.

(a) Since the ring is commutative, it can easily be seen that for any $r, s \in R$ and any $n > 0$ we have

$$(r + s)^n = \sum_{k=0}^{n} r^k s^{n-k}. \tag{1}$$

Clearly $0 \in N$ and so $N \neq \varnothing$. Now let $a, b \in N$. Then a and b are nilpotent, so there exist $x, y > 0$ such that $a^x = 0$ and $b^y = 0$. Let $0 \leq k \leq x + y - 1$. We claim that $a^k b^{x+y-k} = 0$. If $k \geq x$, then indeed $a^k = 0$ since $a^x = 0$. If $k < x$, then $x + y - k \geq y$ and so $b^y = 0$. Hence indeed $a^k b^{x+y-k} = 0$. Now using (1) we have that

$$(a + b)^{x+y} = \sum_{k=0}^{x+y} a^k b^{x+y-k} = \sum_{k=0}^{x+y} 0 = 0,$$

and so $a+b \in N$. Moreover, for any $r \in R$, we have that

$$(ra)^x = r^x a^x = r^x 0 = 0,$$

where in the first equality we used that R is commutative. Hence $ra \in N$ and so N is a left ideal. Since R is commutative, we conclude that N is a two-sided ideal. Moreover, it is a nil ideal by definition.

(b) Let $r+N \in R/N$ be nilpotent and we show that $r+N = 0+N$. Since $r+N$ is nilpotent, there exists some $x > 0$ such that $(r+N)^x = 0+N$. Since $(r+N)^x = r^x + N$, we conclude that $r^x + N = 0 + N$ and so $r^x \in N$. Hence r^x is nilpotent in R. Hence there exists some $y > 0$ such that $(r^x)^y = 0$. Since $0 = (r^x)^y = r^{xy}$, we conclude that r is also nilpotent. Hence $r \in N$ and so $r + N = 0 + N$ as required.

(c) Let $R = M_2(\mathbb{C})$. Let $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Then $A^2 = 0$ and $B^2 = 0$ and so $A, B \in N$. However, $A + B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and a direct computation shows that for $n > 0$ we have

$$(A+B)^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \text{if } n \text{ is odd,} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \text{if } n \text{ is even.} \end{cases}$$

Hence $A + B \notin N$ and so N is not an ideal.

Problem 12. Let R be a ring.

(a) For $a, b \in R$ we define

$$aRb \coloneqq \{arb + nab \mid r \in R, n \in \mathbb{Z}\},$$

that is

$$aRb = \{xb \mid x \in aR\} \text{ and } aRb = \{ay \mid y \in Rb\}.$$

Show that a two-sided ideal P in R is prime, if and only if it satisfies the condition

$$aRb \subseteq P \text{ implies that } a \in P \text{ or } b \in P. \tag{2}$$

(Hint: for showing that P prime implies (2) let $aRb \subseteq P$ and consider the product of the two-sided ideals $(a)(b)$. Show that $(a)(b) \subseteq P$ by considering how a term of $(a)(b)$ looks like and using both the assumptions that $aRb \subseteq P$ and that P is a two-sided ideal.)

(b) (Exercise 10.4.6 in the book.) Let R be a ring and P be a prime (two-sided) ideal in R such that the quotient ring R/P has no nonzero nilpotent elements. Show that R/P is an integral domain.

Solution.

(a) Assume first that (2) holds. We show that P is a prime ideal. Let I and J be ideals such that $IJ \subseteq P$ and we need to show that $I \subseteq P$ or $J \subseteq P$. If $I \subseteq P$, then we are done. Assume that $I \nsubseteq P$. Then there exists $a \in I$ such that $a \notin P$. Let $b \in J$. For any $r \in R$, since I is an ideal, we have that $ar \in I$, and since $b \in J$ we obtain that $arb \in IJ$. For any $n \in \mathbb{Z}$, and since $a \in I$ and $b \in J$ we have that $nab \in IJ$. Hence $arb + nab \in IJ$ for any $r \in R$ and any $n \in \mathbb{Z}$ and so $aRb \subseteq IJ \subseteq P$. By (2) we conclude that $a \in P$ or $b \in P$. Since we have $a \notin P$ we conclude that $b \in p$. But b was an arbitrary element in J, we have shown that $J \subseteq P$, as required.

Assume now that P is a prime ideal and we show that (2) holds. Assume then that $aRb \subseteq P$ and we need to show that $a \in P$ or $b \in P$. Consider the ideals

$$(a) = RaR = \left\{ \sum_{k \in K} r_k a s_k + ra + as + na \mid |K| < \infty, r, s, r_k, s_k \in R, n \in \mathbb{Z} \right\},$$

$$(b) = RbR = \left\{ \sum_{k' \in K'} r'_k b s'_k + r'b + bs' + n'b \mid |K'| < \infty, r', s', r'_k, s'_k \in R, n' \in \mathbb{Z} \right\}.$$

Consider their product $(a)(b)$. By the description of (a) and (b) above we have that elements in $(a)(b)$ are sums of terms of the form

$$rasr'bs', rasr'b, rasbs', n'rasb, rar'bs', rar'b, rabs', n'rab, asr'bs', asr'b, asbs', n'asb, nar'bs', nar'b, nabs', nn'ab.$$

Each of these elements belongs to P. Indeed, for example $rasr'bs'$ is of the form $ratbs$ where $t = sr' \in R$. Then $atb \in aRb \subseteq P$, and since P is an ideal, we have that $ratbs' \in P$ as well. Therefore we conclude that $(a)(b) \subseteq P$. Since P is a prime ideal, we obtain that $(a) \subseteq P$ or $(b) \subseteq P$. In particular $a \in P$ or $b \in P$, as required.

(b) We use part (a). Let $\overline{a}, \overline{b} \in R/P$ be such that $\overline{a}\overline{b} = 0$. We need to show that $\overline{a} = 0$ or $\overline{b} = 0$. Let $r \in R$. Then

$$(\overline{bra})^2 = \overline{brabra} = \overline{brabra} = \overline{br(ab)ra} = \overline{br0ra} = 0,$$

and

$$(\overline{ba})^2 = \overline{baba} = \overline{baba} = \overline{b(ab)a} = \overline{b0a} = 0.$$

Hence $\overline{bra}$ and $\overline{ba}$ are nilpotent. By assumption we obtain that $\overline{bra} = 0$ and $\overline{ba} = 0$. Hence $bra \in P$ and $ba \in P$. Since r was arbitrary, we obtain that $bra \in P$ for any $r \in R$. Since P is an ideal, and $ba \in P$ we obtain that $nba \in P$ for any $n \in \mathbb{Z}$. Hence we conclude that $bra + nba \in P$ for any $r \in R$ and any $n \in \mathbb{Z}$ and so $bRa \subseteq P$. Since P is a prime ideal, by part (a) we conclude that $b \in P$ or $a \in P$. But then $\overline{b} = 0$ or $\overline{a} = 0$, as required.

Problem 13. (Exam December 2010, problem 2.) Let $A = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right) \in M_3(\mathbb{Z}_2)$. Define $\psi : \mathbb{Z}_2[X] \to M_3(\mathbb{Z}_2)$ by

$$\psi(f(x)) = a_0 I_3 + a_1 A + a_2 A^2 + \cdots + a_m A^m,$$

for $f(x) = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m \in \mathbb{Z}_2[X]$ and where $I_3 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

(a) Show that ψ is a ring homomorphism.

(b) Find the kernel $\operatorname{Ker}\psi$ of ψ, and show that the image of ψ, denoted by $\operatorname{Im}\psi$, is a subring of $M_3(\mathbb{Z}_2)$ and a field with 8 elements.

(c) Let $F = \operatorname{Im}\psi$. Why is $M_3(\mathbb{Z}_2)$ not an algebra over F, when the action of the subring F on $M_3(\mathbb{Z}_2)$ is the natural one? Find a field k such that $M_3(\mathbb{Z}_2)$ is an algebra over k, and compute the dimension of $M_3(\mathbb{Z}_2)$ as a vector space over k.

Solution.

(a) Let

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$
$$g(X) = b_0 + b_1 X + b_2 X^2 + \cdots + b_l X^l$$

be two elements of $\mathbb{Z}_2[X]$. Without loss of generality we assume that $m \leq l$. We have

$$\begin{aligned}
\psi(f(X) + g(X)) &= \psi((a_0 + a_1 X + \cdots + a_m X^m) + (b_0 + b_1 X + \cdots + b_l X^l)) \\
&= \psi((a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_m + b_m)X^m + b_{m+1}X^{m+1} + \cdots + b_l X^l) \\
&= (a_0 + b_0)I_3 + (a_1 + b_1)A + \cdots + (a_m + b_m)A^m + b_{m+1}A^{m+1} + \cdots + b_l A^l \\
&= (a_0 I_3 + a_1 A + \cdots + a_m A^m) + (b_0 I_3 + b_1 A + \cdots + b_l A^l) \\
&= \psi(a_0 + a_1 X + \cdots + a_m X^m) + \psi(b_0 + b_1 X + \cdots + b_l X^l) \\
&= \psi(f(X)) + \psi(g(X)),
\end{aligned}$$

and by setting $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ we have

$$\begin{aligned}\psi(f(X)g(X)) &= \psi((a_0 + a_1X + \cdots + a_mX^m)(b_0 + b_1X + \cdots + b_lX^l)) \\ &= \psi(c_0 + c_1X + \cdots + c_{m+l}X^{m+l}) \\ &= c_0I_3 + c_1A + \cdots + c_{m+l}A^{m+l} \\ &= (a_0 + a_1A + \cdots + a_mA^m)(b_0 + b_1A + \cdots + b_lA^l) \\ &= \psi(a_0 + a_1X + \cdots + a_mX^m)\psi(b_0 + b_1X + \cdots + b_lX^l) \\ &= \psi(f(X))\psi(g(X)).\end{aligned}$$

Hence ψ is a ring homomorphism.

(b) Let us first compute the powers of A. So we compute $A^2 = AA$, $A^3 = A^2A$ etc. (remember that we are working over $\mathbb{Z}_2$ so that $1 + 1 = 0$). We have

$$A^2 = \begin{pmatrix}0 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix},\ A^3 = \begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 1\\ 0 & 1 & 1\end{pmatrix},\ A^4 = \begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\end{pmatrix},$$

$$A^5 = \begin{pmatrix}1 & 1 & 1\\ 1 & 0 & 0\\ 1 & 1 & 0\end{pmatrix},\ A^6 = \begin{pmatrix}1 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix},\ A^7 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

that is $A^7 = I_3$ and so the powers of A repeat after that (i.e. $A^8 = A$, $A^9 = A^2$ etc.) Now let $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbb{Z}_2[X]$. Then we compute

$$\psi(f(X)) = a_0I_3 + a_1A + \cdots + a_6A^6 + a_7I_3 + a_8A + \cdots + a_{13}A^6 + a_{14}I_3 + \cdots + a_mA^m.$$

We may then rewrite the above as

$$\psi(f(X)) = (a_0 + a_7 + a_{14} + \cdots)I_3 + (a_1 + a_8 + a_{15} + \cdots)A + \cdots + (a_6 + a_{13} + a_{20} + \cdots)A^6. \tag{3}$$

To keep notation simple therefore, for $0 \leq i \leq 6$ let us set

$$\alpha_i = \sum_k a_{i+k}.$$

Of course, $a_{i+k} = 0$ for $i + k > m$ so the above sum is indeed finite. Notice also that $\alpha_0, \alpha_1, \ldots, \alpha_7$ are independent of each other since each of them is defined by completely different coefficients of the polynomial $f(X)$. Then we may use this notation and (3) to write

$$\begin{aligned}\psi(f(X)) &= \alpha_0I_3 + \alpha_1A + \alpha_2A^2 + \alpha_3A^3 + \alpha_4A^4 + \alpha_5A^5 + \alpha_6A^6 \\ &= \alpha_0\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right) + \alpha_1\left(\begin{smallmatrix}0&0&1\\1&0&1\\0&1&0\end{smallmatrix}\right) + \alpha_2\left(\begin{smallmatrix}0&1&0\\0&1&1\\1&0&1\end{smallmatrix}\right) + \alpha_3\left(\begin{smallmatrix}1&0&1\\1&1&1\\0&1&1\end{smallmatrix}\right) + \alpha_4\left(\begin{smallmatrix}0&1&1\\1&1&0\\1&1&1\end{smallmatrix}\right) + \alpha_5\left(\begin{smallmatrix}1&1&1\\1&0&0\\1&1&0\end{smallmatrix}\right) + \alpha_6\left(\begin{smallmatrix}1&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right) \\ &= \begin{pmatrix}\alpha_0 + \alpha_3 + \alpha_5 + \alpha_6 & \alpha_2 + \alpha_4 + \alpha_5 + \alpha_6 & \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5\\ \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5 & \alpha_0 + \alpha_2 + \alpha_3 + \alpha_4 & \alpha_1 + \alpha_2 + \alpha_3 + \alpha_6\\ \alpha_2 + \alpha_4 + \alpha_5 + \alpha_6 & \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5 & \alpha_0 + \alpha_2 + \alpha_3 + \alpha_4\end{pmatrix}.\end{aligned}$$

Notice that there are some repetitions in the entries of the matrix $\psi(f(X))$ above. In fact, if we set

$$\begin{aligned}\beta &\coloneqq \alpha_2 + \alpha_4 + \alpha_5 + \alpha_6,\\ \gamma &\coloneqq \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5,\\ \delta &\coloneqq \alpha_0 + \alpha_2 + \alpha_3 + \alpha_4,\end{aligned}$$

then we obtain

$$\psi(f(X)) = \begin{pmatrix}\beta + \delta & \beta & \gamma\\ \gamma & \delta & \beta + \gamma\\ \beta & \gamma & \delta\end{pmatrix}. \tag{4}$$

Now let us compute $\operatorname{Ker}\psi$. Assume that $f(X) \in \operatorname{Ker}\psi$ so that $\psi(f(X)) = 0$. By (4) we obtain that $\beta = \gamma = \delta = 0$. Hence we obtain the system of equations

$$\begin{aligned}\alpha_2 + \alpha_4 + \alpha_5 + \alpha_6 &= 0\\ \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5 &= 0\\ \alpha_0 + \alpha_2 + \alpha_3 + \alpha_4 &= 0\end{aligned}$$

As we have noted, the variables α_i are independent of each other. Hence we have three equations and seven unkowns, so we may let four of the variables, say $\alpha_0, \alpha_1, \alpha_2$ and α_6 be free. Then after some small manipulations to the system we obtain

$$\begin{aligned}\alpha_3 &= \alpha_1 + \alpha_2 + \alpha_6\\ \alpha_4 &= \alpha_0 + \alpha_1 + \alpha_6\\ \alpha_5 &= \alpha_0 + \alpha_1 + \alpha_2.\end{aligned}$$

Hence we conclude that the kernel of ψ is given by

$$\operatorname{Ker}\psi = \{f(X) = a_0 + a_1X + \cdots + a_mX^m \mid \alpha_3 = \alpha_1 + \alpha_2 + \alpha_6, \alpha_4 = \alpha_0 + \alpha_1 + \alpha_6, \alpha_5 = \alpha_0 + \alpha_1 + \alpha_2\}.$$

Finally, let us compute $\operatorname{Im}\psi$. By (4) we see that there are at most 8 possible values for $\psi(f(X))$, since β, γ and δ have two possibilities each, namely 0 or 1. Hence $\operatorname{Im}\psi$ has at most 8 elements. On the other hand, we have that $\psi(0) = 0$ and that $\psi(X^m) = A^m$ for any $m \geq 0$. Hence we have that $\{0, A, A^2, A^3, A^4, A^5, A^6, I_3\} \subseteq \operatorname{Im}\psi$ and so $\operatorname{Im}\psi$ has at least 8 elements. We conclude that

$$\operatorname{Im}\psi = \{0, A, A^2, A^3, A^4, A^5, A^6, I_3\}.$$

Moreover, $\operatorname{Im}\psi$ is a subring of $M_3(\mathbb{Z}_2)$ as it is the image of a ring homomorphism. Finally, it is also a field since $A^7 = I_3$, and so each of the matrices $A, A^2, A^3, A^4, A^5, A^6$ has an inverse, namely for $1 \leq k \leq 6$ we have

$$(A^k)^{-1} = A^{7-k}.$$

(c) The reason that $M_3(\mathbb{Z}_2)$ is not an algebra over F is that F is not included in the center of $M_3(\mathbb{Z}_2)$. Indeed, for $M_3(\mathbb{Z}_2)$ to be an F-algebra with the natural action, we need to have

$$X(MN) = M(XN)$$

for any $M, N \in M_3(\mathbb{Z}_2)$ and any $X \in F$. But taking for example $X = A$, $M = E_{11}$ and $N = I_3$ we see that

$$X(MN) = A(E_{11}I_3) = AE_{11} = \begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix} = \begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}$$

while

$$M(XN) = E_{11}(AI_3) = E_{11}A = \begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix} = \begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}.$$

To find a field k that makes $M_3(\mathbb{Z}_2)$ into a k-algebra, we can compute the center $Z(M_3(\mathbb{Z}_2))$ to be

$$Z(M_3(\mathbb{Z}_2)) = \left\{ \left(\begin{smallmatrix}a&0&0\\0&a&0\\0&0&a\end{smallmatrix}\right) \mid a \in Z(\mathbb{Z}_2) \right\}.$$

In fact, $\mathbb{Z}_2$ is a field itself and so $Z(\mathbb{Z}_2) = \mathbb{Z}_2$. Hence the center of $M_3(\mathbb{Z}_2)$ contains exactly two elements the zero matrix and the identity matrix and so it is isomorphic to $\mathbb{Z}_2$. Then $M_3(\mathbb{Z}_2)$ becomes a vector space over $\mathbb{Z}_2$ with scalar multiplication given by

$$aM = \begin{cases} M, & \text{if a=1,}\\ 0, & \text{if a=0,}\end{cases}$$

for all $M \in M_3(\mathbb{Z}_2)$. Then for all $M, N \in M_3(\mathbb{Z}_2)$ we have that

$$a(MN) = (aM)N = M(aN).$$

Indeed if $a = 0$, then the above expression is just 0 while if $a = 1$ the above expression is MN. Hence $M_3(\mathbb{Z}_2)$ is a $\mathbb{Z}_2$-algebra. The dimension of $M_3(\mathbb{Z}_2)$ as a vector space over $\mathbb{Z}_2$ is then 9, as in general the dimension of $M_n(k)$ as a vector space over the field k is n^2 (the matrices E_{ij} for $1 \leq i, j \leq n$ form a k-basis).

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 14. Let R be a ring.

(a) (Exercise 10.5.2 in the book.) Assume that R is commutative and let $I_1, \ldots, I_n$ be nil ideals in R. Show that $I_1 + \cdots + I_n$ is a nil ideal in R.

(b) (Exercise 10.5.1 in the book.) Let I and J be nilpotent ideals in R. Show that $I + J$ is a nilpotent ideal in R. *(Hint: a general element of $(I + J)^k$ for some $k \geq 1$ is a finite sum of terms of a specific form. Show that these terms are all zero for a big enough k.)*

Solution.

(a) By induction it is enough to show that $I_1 + I_2$ is a nil ideal in R. Let $z \in I_1 + I_2$. Then $z = a + b$ where $a \in I_1$ and $b \in I_2$. Since I_1 and I_2 are nil ideals, there exist $n, m > 0$ such that $a^n = 0$ and $b^m = 0$. Let $l = n + m - 1$. Then, since R is commutative, we may use (1) to obtain

$$z^l = (a + b)^l = \sum_{k=0}^{l} a^k b^{l-k}.$$

Let $0 \leq k \leq l$. If $k \geq n$, then $a^k = 0$ and so $a^k b^{l-k} = 0$. If $k < n$, then $l - k > l - n = m - 1$ and so $l - k \geq m$. Then $b^{l-k} = 0$ and so $a^k b^{l-k} = 0$. It follows that $a^k b^{l-k} = 0$ for all $0 \leq k \leq l$ and so $z^l = 0$. Hence z is nilpotent. Since z was an arbitrary element in $I_1 + I_2$, we conclude that $I_1 + I_2$ is a nil ideal.

(b) Since I and J are nilpotent, there exist $n \geq 0$ and $m \geq 0$ such that $I^n = 0$ and $J^m = 0$. Set $k = n+m-1$. Consider an element $z \in (I + J)^k$. By definition, it is a finite sum of terms of the form

$$z_1 z_2 \cdots z_k,$$

where $z_i \in I + J$. In particular, $z_i = a_i + b_i$ for some $a_i \in I$ and $b_i \in J$. Then the term $z_1 z_2 \cdots z_k$ can be computed as

$$z_1 z_2 \cdots z_k = (a_1 + b_1)(a_2 + b_2) \cdots (a_k + b_k).$$

By computing the above product using distributivity, we see that $z_1 z_2 \cdots z_k$ s a finite sum of terms of the form $x_1 x_2 \cdots x_k$, where each x_i is either equal to a_i or b_i. Now we have that $k = n + m - 1$. Therefore, in the product $x_1 x_2 \cdots x_k$ there are either at least n terms x_i with $x_i = a_i$ or there are at least m terms x_i with $x_i = b_i$. Both cases can be dealt with the same way, so let us assume that there are at least n terms x_i with $x_i = a_i$. Let us label these n terms as x_{i_1}, $x_{i_2}, \ldots x_{i_k}$ such that $i_1 < i_2 < \cdots < i_k$. In other words, we can write $x_1 x_2 \cdots x_k$ as

$$x_1 x_2 \cdots x_k = x_1 x_2 \cdots x_{i_1 - 1} \mathbf{x_{i_1}} x_{i_1+1} \cdots x_{i_2-1} \mathbf{x_{i_2}} x_{i_2+1} \cdots x_{i_n-1} \mathbf{x_{i_n}} x_{i_n+1} \cdots x_{k-1} x_k, \tag{5}$$

where $x_{i_j} = a_{i_j} \in I$. Now we set

$$\begin{aligned}
y_1 &= \mathbf{x_{i_1}} x_{i_1+1} \cdots x_{i_2-1} = a_{i_1} x_{i_1+1} \cdots x_{i_2-1} \in I \\
y_2 &= \mathbf{x_{i_2}} x_{i_2+1} \cdots x_{i_3-1} = a_{i_2} x_{i_2+1} \cdots x_{i_3-1} \in I \\
&\vdots \\
y_{n-1} &= \mathbf{x_{i_{n-1}}} x_{i_{n-1}+1} \cdots x_{i_n-1} = a_{i_{n-1}} x_{i_{n-1}+1} \cdots x_{i_n-1} \in I \\
y_n &= \mathbf{x_{i_n}} x_{i_n+1} \cdots x_k = a_{i_n} x_{i_n+1} \cdots x_k \in I,
\end{aligned}$$

where each of the above elements is in I since it is the product of an element in I with an element in R and I is an ideal. Then by (5) that

$$x_1x_2\cdots x_k = x_1x_2\cdots x_{i_1-1}y_1y_2\cdots y_{n-1}y_n.$$

But $y_1y_2\cdots y_{n-1}y_n \in I^n$ since each of the elements is in I. Since $I^n = 0$ we conclude that $y_1y_2\cdots y_{n-1}y_n = 0$ and so $x_1x_2\cdots x_k = 0$. But then also $z_1z_2\cdots z_k = 0$ since $z_1z_2\cdots z_k$ is a finite sum of elements of the form $x_1x_2\cdots x_k$. Going further back, we obtain that $z = 0$ since z is a finite sum of elements of the form $z_1z_2\cdots z_k$. But z was an arbitrary element in $(I+J)^k$ and so $(I+J)^k = 0$ and the ideal $I+J$ is nilpotent, as required.

Problem 15. Let R be a unital ring. Let M be the set of all non-invertible elements in R. Show that the following are equivalent.

(a) The set M is an ideal.

(b) For every $r \in R$, either r or $1-r$ is a unit.

(Hint: to show that (b) implies (a), observe first that in any ring the product of two invertible elements is invertible, while the product of a non-invertible element with an invertible element in non-invertible.)

Rings for which these equivalent conditions hold are called *local*. Show also the following

(c) If R is a local unital ring with $0 \neq 1$, then R/M is a division ring.

(d) A commutative ring is local if and only if it has a unique maximal ideal (this holds also for non-commutative rings, but the proof is more involved.)

(e) (Exercise 10.2.19 in the book.) Show that the rings $\mathbb{Z}/(p^2)$ where p is a prime number and $F[[X]]$ where F is a field are local. *(In both cases use (d). For $\mathbb{Z}/(p^2)$ use the correspondence theorem to describe the ideals of $\mathbb{Z}/(p^2)$. For $F[[X]]$ show first that an element $f(X) = \sum_{i=0}^{\infty} a_iX^i$ of $F[[X]]$ is invertible if and only if $a_0 \neq 0$, and use this to show that any ideal of $F[[X]]$ is of the form (X^m) for some $m \geq 0$.)*

Solution. We start with some general observations about the product of invertible and non-invertible elements in any ring. First if $r, s \in R$ are invertible, then their product rs is also invertible with inverse $s^{-1}r^{-1}$. Hence the product of two invertible elements is invertible. Next we claim that the product of a non-invertible element with an invertible element is not invertible. Indeed, let $m, r \in R$ with m not invertible and r invertible, and assume to a contradiction that mr is invertible. Then there exists $s \in R$ with $mrs = 1$ and $smr = 1$. Since r is invertible, we can write the second equality as $sm = r^{-1}$ and then as $rsm = 1$. But then we have obtained that both $mrs = 1$ and $rsm = 1$ hold and so m is invertible, which contradicts our assumption. Similarly we can show that rm is not invertible. Hence we have seen that

- The product of two invertible elements in a unital ring is invertible. In particular, if r is invertible, then $-r = (-1)r$ is also invertible.
- The product of an invertible element with a non-invertible element in a unital ring is non-invertible.

We will use the above throughout.

We now start with the equivalence of (a), (b) and (c). Assume first that (a) holds, that is that M is an ideal, and we show that (b) holds. Assume towards a contradiction that there exists $r \in R$ such that neither r nor $1-r$ is a unit. Then $r, 1-r \in M$. Since M is an ideal, we obtain that $1 = r + (1-r) \in M$. But 1 is invertible and this contradicts the fact that M is the set of all non-invertible elements of R.

Assume now that (b) holds and we show that (a) holds. Clearly $0 \in M$ and so $M \neq \varnothing$. Next let $m, n \in M$ and we show that $m - n \in M$. Assume to a contradiction that $m - n \notin M$. Then $m - n$ is invertible and so there exists $r \in R$ with $r(m-n) = 1$ and $(m-n)r = 1$. In particular, r is invertible as well and so $-r$ also is. Then $r(m-n) = 1$ gives $rm - rn = 1$ or $rm = 1 + rn$ or $m = r^{-1}(1+rn)$. Since $-r$ is invertible, but n is not invertible (as $n \in M$), we conclude that $-rn$ is not invertible. By (b) we have then that $1 - (-rn) = 1 + rn$ is invertible. Then $m = r^{-1}(1+rn)$ is the product of two invertible elements and so it is invertible. But this contradicts $m \in M$. Hence $m - n \in M$.

Now let $m \in M$ and $r \in R$ be arbitrary and we show that $mr \in M$. In fact, if r is invertible, then we have already shown that $mr \in M$ since the product of a non-invertible element and an invertible element is non-invertible. Hence we may assume that r is also non-invertible. Assume to a contradiction that $mr \notin M$. Hence mr is invertible. Then mrm is not invertible, since it is the product of the invertible element mr and the non-invertible element m (as $m \in M$). By (b) we have that $1 - mrm$ is invertible. Then we write

$$1 - mrm = (mr)^{-1}(mr - m) = (mr)^{-1}m(r - 1) = (mr)^{-1}m(r - 1).$$

Now we have that $(mr)^{-1}$ is invertible and m is not invertible, and hence $(mr)^{-1}m$ is not invertible. Moreover, r is not invertible and so by (b) we obtain that $1 - r$ is invertible. It follows that $-(1 - r) = r - 1$ is also invertible. Hence the product $(mr)^{-1}m(r-1)$ is not invertible, as it is the product of a non-invertible element with an invertible element. Hence $1 - mrm = (mr)^{-1}m(r - 1)$ is not invertible. But we have seen already that $1 - mrm$ is invertible, and so we reach a contradiction. Therefore we conclude that $mr \in M$. Similarly we can show that $rm \in M$ and so we conclude that M is an ideal which shows (a).

(c) Assume first that R is local and we show that there exists a unique maximal ideal in R. In particular (a) holds and we have that M is an ideal. We claim that M is the unique maximal ideal in R. First let us show that M is maximal. Let I be a ideal in R such that $M \subsetneq I \subseteq R$ and we show that $I = R$. Since $M \subsetneq I$, there exists an element $a \in I$ such that $a \notin M$. In particular, a is invertible. Hence $1 = a^{-1}a \in I$ and so $I = R$ since I contains 1. Therefore M is maximal. Now let J be any maximal ideal in R. Since $J \neq R$, J does not contain any invertible element (otherwise, again $1 \in J$ which implies $J = R$). Hence J contains only non-invertible elements and so $J \subseteq M$. Since M is also an ideal with $M \neq R$, and by maximality of J, we conclude that $J = M$. Hence M is the unique maximal ideal in R.

Now assume that there exists a unique maximal ideal J in R and we show (a). Let $a \in R$ be a non-invertible element. Consider the ideal (a) generated by a. We have that

$$(a) = \{ra \mid r \in R\}.$$

We claim that (a) is a proper ideal of R. Indeed, assume to a contradiction that $(a) = R$ and so $1 \in (a)$. Then $1 = ra$ for some $r \in R$. Since R is commutative, we have $ar = 1$ and so a is invertible, which is a contradiction. Hence (a) is a proper ideal and so it is included in a maximal ideal in R by Theorem 7.4. Since by assumption there exists a unique maximal ideal J in R, we have that $(a) \subseteq J$. Hence $a \in J$ and since a was an arbitrary non-invertible element, we conclude that $M \subseteq J$. On the other hand, we have that J contains no invertible elements, since otherwise $1 \in J$ and $J = R$, contradicting maximality of J. Hence $J \subseteq M$. We have thus that $J = M$ and so M is an ideal.

(d) Now let us show that R/M is a division ring. Let $r + M \in R/M$ be a nonzero element. Then $r \notin M$ and so r is invertible in R. Hence there exists $r^{-1} \in R$. Then $(r + M)(r^{-1} + M) = rr^{-1} + M = 1 + M$ and $(r^{-1} + M)(r + M) = r^{-1}r + M = 1 + M$ and so $(r + M)^{-1} = r^{-1} + M$ and $r + M$ is invertible. Hence every nonzero element of R/M is invertible and so R/M is a division ring.

(e) The ring $\mathbb{Z}/(p^2)$ is commutative, hence by (d) it is enough to show that it has a unique maximal ideal. By Corollary 4.6 we have that ideals of $\mathbb{Z}/(p^2)$ are of the form $I/(p^2)$ where I is an ideal of $\mathbb{Z}$ containing p^2. Since $\mathbb{Z}$ is a PID, ideals in $\mathbb{Z}$ are of the form (n) for some $n \geq 0$. By Problem 4(a) we have that $(n) \subseteq (m)$ if and only if m divides n. Hence $(p^2) \subseteq (m)$ if and only if $m \mid p^2$ if and only if $m \in \{1, p, p^2\}$. We conclude that the ideals of $\mathbb{Z}/(p^2)$ are $(p^2)/(p^2) = (0)$, $(p)/(p^2) = \{0 + (p^2), p + (p^2), 2p + (p^2), \ldots, (p-1)p + (p^2)\}$ and $(1)/(p^2) = \mathbb{Z}/(p^2)$. Hence there exists a unique proper two-sided ideal of $\mathbb{Z}/(p^2)$, namely $(p)/(p^2)$, and so $\mathbb{Z}/(p^2)$ is a local ring.

The ring $F[[X]]$ is also commutative so we may use (d). We first show that an element $f(X) = \sum_{i=0}^{\infty} a_i X^i \in F[[X]]$ is invertible if and only if $a_0 \neq 0$. Assume first that $f(X)$ is invertible and let $g(X) = \sum_{i=0}^{\infty} b_i X^i$ be its inverse. Then $f(X)g(X) = 1$ and in particular $a_0 b_0 = 1$ which implies $a_0 \neq 0$. Assume now that $a_0 \neq 0$. Pick b_i such that

$$\begin{aligned} a_0 b_0 &= 1 \\ a_1 b_0 + a_0 b_1 &= 0 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 &= 0 \\ &\vdots \end{aligned}$$

Since at step 0 we only need to pick b_0, at step 1 we only need to pick b_1 etc., such a choice is possible. Then by construction $g(X) = \sum_{i=0}^{\infty} b_i X^i$ is an inverse of $f(X)$ and the claim is shown.

Now we claim that every ideal of $F[[X]]$ is of the form (X^m) for some $m \geq 0$. Let I be an ideal in $F[[X]]$. Let

$$m = \min\{m \geq 0 \mid \exists a_m X^m + a_{m+1} X^{m+1} + \cdots \in I, a_m \neq 0\}.$$

We claim that $I = (X^m)$. First let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in I$. Then by the definition of m we have that $a_0 = a_1 = \cdots = a_{m-1} = 0$. Hence $f(X) = \sum_{i=m}^{\infty} a_i X^i \in (X^m)$, which shows that $I \subseteq (X^m)$. Now we show that $(X^m) \subseteq I$. For this it is enough to show that $X^m \in I$. By assumption on m there exists $f(X) = \sum_{i=m}^{\infty} a_m X^i \in F[[X]]$ such that $a_m \neq 0$. Then $f(X) = X^m(a_m + a_{m+1}X + \cdots) = X^m g(X)$. But by the first part we have that $g(X)$ is invertible with inverse, say, $h(X)$. Since I is an ideal, we obtain that

$$X^m = X^m 1 = X^m(g(X)h(X)) = (X^m g(X))h(X) \in I,$$

as required. Hence we have shown that all ideals in $F[[X]]$ are of the form (X^m) for some $m \geq 0$. But then clearly we have a chain of inclusions $(X) \supseteq (X^2) \supseteq (X^3) \supseteq \cdots$, which shows that (X) is the unique maximal ideal in $F[[X]]$.