MATH6302 - Modern Algebra
Homework 8

Joel Sleeba

December 6, 2024

1. Let x be a nilpotent element of the commutative ring R.
   (a) Prove that x is either zero or a zero-divisor.
   (b) Prove that rx is nilpotent for all $r \in R$.
   (c) Prove that $1 + x$ is a unit of R.
   (d) Deduce that the sum of a unit and a nilpotent element is a unit in R.

   Solution:

   (a) Let $x \in R$, be nilpotent, ($x^n = 0$) and R be commutative. If $x \neq 0$, then x^{n-1} is not zero (assuming n to be the smallest $n \in \mathbb{N}$ such that $x^n = 0$) but $x^{n-1}x = x^n = 0$, which shows that x is a zero divisor.

   (b) By the commutativity of R, we get

   $$(rx)^n = r^n x^n = r^n 0 = 0$$

   which shows that rx is nilpotent.

   (c) We claim that $(1 + x)^{-1} = 1 - x + x^2 - x^3 \ldots x^{n-1}$. To see this, notice that

   $$(1+x)(1-x+x^2-x^3 \ldots x^{n-1}) = (1-x+x^2-x^3 \ldots x^{n-1})+x(1-x+x^2-x^3 \ldots x^{n-1}) = 1$$

   (d) Let $a \in R$ be a unit and $x \in R$ be nilpotent with $x^n = 0$. Then $a^{-1}x$ is again nilpotent. Then, by the previous part, we see that $(1 + a^{-1}x)$ is a unit. Thus $a(1 + a^{-1}x) = a + x$ is a unit.

2. A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

Solution: Let $a \in R$. then $a+a = (a+a)^2 = a^2+a^2+a^2+a^2 = a+a+a+a$ forces $a+a=0$ i.e $a = -a$ for all $a \in R$. Therefore showing $ab = ba$ is equivalent to showing $ab+ba = 0$ for any $a, b \in R$.

$$\begin{aligned} a+b = (a+b)^2 &= a^2+ab+ba+b^2 \\ &= a+b+ab+ba \end{aligned}$$

gives $ab+ba = 0$ and hence we're done.

3. Let X be any non-empty set and let $\mathcal{P}(X)$ be the power set of X. Define addition and multiplication in $\mathcal{P}(X)$ as

$$A+B = A\Delta B, \quad A \cdot B = A \cap B$$

   (a) Show that $\mathcal{P}(X)$ is a ring under these operations.

   (b) Prove that $\mathcal{P}(X)$ is a unital commutative Boolean ring.

   Solution:

   (a) We have already verified in the first assignment that $(\mathcal{P}, \Delta)$ is an Abelian group. Notice that since $A \cap B \subset X$ for each $A, B \in \mathcal{P}(X)$, $\cap$ is a binary operation. Associativity of $\cap$ follows since $(A \cap B) \cap C = A \cap B \cap C = A \cap (B \cap C)$. Moreover $A \cap B = B \cap A$. Hence we just need to verify that $\cap$ distributes over Δ.

$$\begin{aligned} (A\Delta B) \cap C &= ((A \setminus B) \cup (B \setminus A)) \cap C \\ &= ((A \setminus B) \cap C) \ \cup \ ((B \setminus A) \cap C) \\ &= ((A \cap C) \setminus (B \cap C)) \ \cup \ ((B \cap C) \ (A \cap C)) \\ &= (A \cap C)\Delta(B \cap C) \end{aligned}$$

   Hence $(\mathcal{P}, \Delta, \cap)$ is a commutative ring.

   (b) Since we've already shows that $\cap$ is commutative, we'll just verify the rest. Notice that for any $A \in \mathcal{P}(X)$, we have $A \cap X = A = X \cap A$, hence X acts as the multiplicative identity making the ring unital. Moreover $A \cap A = A$ shows that it is a Boolean ring.

4. Decide which of the following are ideals of the ring $\mathbb{Z}[x]$

   (a) Set of all polynomials whose constant term is a multiple of 3.

   (b) Set of all polynomials whose coefficient of x^2 is a multiple of 3.

(c) Set of all polynomials whose constant term, coefficient of x, and coefficient of x^2 are 0.

(d) $\mathbb{Z}[x^2]$.

(e) Set of polynomials whose coefficients sum to zero.

(f) Set of polynomials $p(x)$ such that $p'(0) = 0$.

Solution:

(a) The zero polynomial $\mathbf{0}$, which is the additive identity will not be in the collection. Therefore it won't be a subring, hence not an ideal.

(b) Consider $3x^2 + 1$ in the collection and $x^2 \in \mathbb{Z}[x]$. Then $x^2(3x^2 + 1) = 3x^4 + x^2$ is not in the collection. Hence it is not an ideal.

(c) Since any sum and product of such polynomials will have their constant term, and coefficients of x, x^2 be 0, the collection is a subring. Moreover if $p(x) \neq \mathbf{0}$ is in the collection, then $p(x) = x^3 q(x)$ for $q(x) \in \mathbb{Z}[x]$. Then for any $r(x) \in \mathbb{Z}[x]$, $(rp)(x) = x^3 q(x) r(x)$, is again in the collection. Hence the collection is an ideal.

(d) Let $x^2 \in \mathbb{Z}[x^2]$. Then for $x \in \mathbb{Z}[x]$, $x \cdot x^2 = x^3 \notin \mathbb{Z}[x^2]$, shows that $\mathbb{Z}[x^2]$ is not an ideal.

(e) It is easy to verify that the collection given is a subroup of $\mathbb{Z}[x]$. The closure of the product on the collection will be evident once we verify the ideal condition.

Let $p(x) = \sum_{i=0}^{n} a_i x^i$, be a polynomial with $\sum_{i=0}^{n} a_i = 0$ and $q(x) = \sum_{j=0}^{m} b_j x^j$ be another polynomial in $\mathbb{Z}[x]$. Then

$$(qp)(x) = \sum_{j=0}^{m} \sum_{i=0}^{n} b_j a_i x^{i+j}$$

Then the sum of their co-efficients,

$$\sum_{j=0}^{m} \sum_{i=0}^{n} b_j a_i = \sum_{j=0}^{m} b_j \left(\sum_{i=0}^{n} a_n \right) = 0$$

shows that the collection is an ideal and hence proves the closure under multiplication too.

(f) Let $p(x) = x^2 + 1$ and $q(x) = x$. Then $p'(0) = 2 \times 0 = 0$. But $(pq)(x) = x^3 + x$ and $(pq)'(x) = 3x^2 + 1$ gives $(pq)'(0) = 1$. Hence the collection is not an ideal.

5. Prove that the ring $M_2(\mathbb{R})$ contains a subring isomorphism to $\mathbb{C}$.

   Solution: Consider the map $\phi : \mathbb{C} \to M_2(\mathbb{R})$ defined as

$$\phi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

   The fact that ϕ preserves addition follows easily from the matrix addition in $M_2(\mathbb{R})$. Hence we'll only verify the multiplicativity of the map.

$$\begin{aligned} \phi((a+ib)(p+iq)) &= \phi((ap-bq)+i(aq+bp)) \\ &= \begin{pmatrix} ap-bq & aq+bp \\ -aq-bp & ap-bq \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \\ &= \phi(a+ib)\phi(p+iq) \end{aligned}$$

   shows that ϕ is a ring homomorphism. Moreover we see that $\phi(a+ib) = \mathbf{0}$ if and only if $a = b = 0$. Hence ϕ is an injective ring homomorphism, which proves our assertion.

6. (a) Prove that the map $\phi : \mathbb{Z} \to R$ defined as $n \to n1_R$ is a ring homomorphism with kernel $n\mathbb{Z}$, where n is the characteristic of R.
   (b) Determine the characteristic of $\mathbb{Q}, \mathbb{Z}[x], \mathbb{Z}/n\mathbb{Z}$.
   (c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

   Solution:

   (a) Let $\phi : \mathbb{Z} \to R$ be the map given. Then

$$\phi(m+n) = (m+n)\mathbf{1} = m\mathbf{1} + n\mathbf{1} = \phi(m) + \phi(n)$$

   and

$$\phi(mn) = mn\mathbf{1} = (mn)(\mathbf{1} \cdot \mathbf{1}) = (m\mathbf{1}) \cdot (n\mathbf{1}) = \phi(m) \cdot \phi(n)$$

   shows that ϕ is a ring homomorphism.

   We'll show that $\mathrm{Ker}(\phi) = n\mathbb{Z}$, where n is the characteristic of R. Let $nk \in n\mathbb{Z}$, then

$$\phi(nk) = (nk)\mathbf{1} = (kn)\mathbf{1} = k(n\mathbf{1}) = k\mathbf{0} = 0$$

Conversely if $k \in \text{Ker}(\phi)$, then

$$\phi(k) = k\mathbf{1} = 0$$

which forces k to be a multiple of n. Thus we get $\text{Ker}(\phi) = n\mathbb{Z}$.

(b) $\mathbb{Q}$ has characteristic 0, since $1 + 1 + \ldots 1 \neq 0$. For the same reason $\mathbb{Z}[x]$ also has characteristic 0. But $\underbrace{1 + 1 + \ldots 1}_{n \text{ times}} = 0$ in $\mathbb{Z}/n\mathbb{Z}[x]$. Hence $\mathbb{Z}/n\mathbb{Z}[x]$ has characteristic n.

(c) Let R be a ring of characteristic p, then for any $a \in R$, $pa = \underbrace{a + a + \ldots a}_{p \text{ times}} = a\underbrace{1 + 1 + \ldots 1}_{p \text{ times}} = a0 = 0$. Moreover, when R is a commutative ring,

$$(a+b)^p = \sum_{r=0}^{p} \frac{p!}{(p-r)!r!} a^{p-r} b^r = a^p + \sum_{r=1}^{p-1} \frac{p!}{(p-r)!r!} a^{p-r} b^r + b^p$$

Since p is a prime, $\frac{p!}{(p-r)!r!}$ is a multiple of p whenever $1 \leq r \leq p-1$. This is because all the numbers being multiplied together in the denominator is less than p and cannot factor out p. Hence we get that $(a+b)^p = a^p + b^p$.

7. Prove that an integral domain has characteristic p, where p is either a prime or 0.

Solution: Assume that R is an integral domain with characteristic $p \neq 0$. Then $p\mathbf{1} = 0$ for the multiplicative identity $\mathbf{1} \in R$. If p was not a prime, then $p = nk$ for $1 < n, k < p$. Then we'd get

$$p\mathbf{1} = (n\mathbf{1})(k\mathbf{1}) = 0$$

Since R is an integral domain this would force $n\mathbf{1} = 0$ or $k\mathbf{1} = 0$, which contradicts our assumption on the characteristic of R since $n, k < p$. Hence we see that p must be a prime.

8. Let R be a commutative ring. Prove that the set of all nilpotent elements form an ideal, called the *nilradical.*

Solution: Let I be the collection of all nilpotent elements of a commutative ring R. Let $a, b \in I$ with $a^n = b^m = 0$. Then

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n-i}{i} a^{m+n-i} b^i = \sum_{i=0}^{m+n} 0 = 0$$

shows that $a+b \in I$. If $r \in R$, then

$$(ar)^n = a^n r^n = 0$$

shows that $ar \in I$ for all $r \in R$, hence proving that I is an ideal.

9. Let I, J be ideals of R.
   (a) Prove that $I+J$ is the smallest ideal containing both I and J.
   (b) Prove that IJ is an ideal contained in $I \cap J$.
   (c) Give an example where $IJ \neq I \cap J$.
   (d) Prove that if R is commutative and $I+J=R$, then $IJ = I \cap J$.

Solution:

(a) Since I, J are subrings of R, being the ideals of R, we see that $I, J \subset I+J$ ($I = I + e_J$ and $J = e_I + J$). If $i+j, p+q \in I+J$, then $(i+j)+(p+q) = (i+p)+(j+q) \in I+J$. Moreover if $r \in R$ and $i+j \in I+J$, then

$$r(i+j) = ri + rj \in I+J$$

and

$$(i+j)r = ir + jr \in I+J$$

shows that $I+J$ is an ideal which contains I, J. Now if K is any other ideal that contain I, J, then being a subring, $K \ni i+j$ for all $i \in I, j \in J$. Hence $K \supset I+J$, which shows that $I+J$ is the smallest ideal that contain I, J.

(b) Let $\sum_{i=1}^n a_i b_i, \sum_{j=1}^m p_j q_j \in IJ$, where $a_i, p_j \in I$ and $b_i, q_j \in J$. Then

$$\sum_{i=1}^n a_i b_i + \sum_{j=1}^m p_j q_j \in IJ$$

by the definition of IJ. Moreover if $r \in R$, then

$$r\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (ra_i)b_i \in IJ$$

and

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)r = \sum_{i=1}^{n} a_i(b_i r) \in IJ$$

since I, J are ideals in R. Hence we see that IJ is an ideal of R.

Also for any $a_i \in I, b_i \in J$, $a_i b_i \in I \cap J$ since I, J are ideals. Thus we see that $IJ \subset I \cap J$.

(c) Let $I, J = (2) \subset \mathbb{Z}$. Then $I \cap J = (2)$. We claim that $IJ = (4)$. Since $4 = 2 \times 2$, we see that $4 \in IJ$. Thus $(4) \subset IJ$.

Conversely if $ij \in IJ$, then $i = 2k, j = 2m$ for $m, k \in \mathbb{Z}$. Thus $ij = 4mk \in (4)$. Thus all finite sums of elements ij where $i \in I, j \in J$ are also in (4). Thus we see that $IJ = (4) \neq (2) = I \cap J$.

(d) Let R be unital, and commutative with $I + J = R$, and let $r \in I \cap J$. Since $I + J = R$ and $1 \in R$, we see that $1 = i + j$ for some $i \in I, j \in J$. Thus $r = r1 = ri + rj \in IJ$. Thus $I \cap J \subset IJ$.

10. Assume that R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors, then R is an integral domain.

Solution: Let $a, b \in \mathbb{R}$ such that $ab = 0 \in P$. Without loss of generality assume $a \in P$. Since we know that P contains no zero divisors, this forces $a = 0$. Hence we see that R is an integral domain.

11. Assume R is commutative. Let I, J are ideals of R and assume that P is a prime ideal of R that contains $I \cap J$. Prove that either I or J is contained in P.

Solution: Let $IJ \subset P$ and $I \not\subset P$. Then $\exists i_p \in I \setminus P$. Now for any $j \in J$,

$$i_p j \in IJ \subset P$$

forces $j \in P$, by the primality of P. Hence $J \subset P$.

12. Let I be the ideal $(2, x)$ of $\mathbb{Z}[x]$. Prove that I^2 contains elements which are not of the form ab for any $a, b \in I$.

    Solution: Let $x \in I, y \in J$. Then $x = \sum_{i=1}^{n} r_i a_i, y = \sum_{j=1}^{m} s_i b_i$ for $r_i, s_j \in R$. This shows that

$$xy = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_i a_i)(s_i b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_i a_i s_i) b_j = \sum_{i=1}^{n} \sum_{j=1}^{m} k_i a_i b_j$$

    for $k_i \in R$, since I is an ideal of R. Since we have shown that for any $x \in I, y \in J$, xy is a R-combination of elements $a_i b_j$, we see that any element of IJ must also be such. Thus we are done.

13. Prove that if R is an integral domain, then (x) is a prime ideal in $R[x]$. Prove that (x) is a maximal ideal if and only if R is a field.

    Solution: Let $I = (x)$, be the principal ideal generated by $x \in R[[x]]$. Let $p = \sum_{i=0}^{n} a_i x^i, q = \sum_{j=0}^{m} b_j x^j \in R[[x]]$. Then

$$pq = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} = \sum_{k=0}^{m+n} c_k x^k$$

    where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

    We notice that $pq \in I$ if and only if $c_0 = a_0 b_0 = 0$. Since R is an integral domain, this forces either a_0 or b_0 to be zero. Without loss of generality, assume $a_0 = 0$. Then

$$p = \sum_{i=1}^{n} a_i x^i = x\Big(\sum_{i=0}^{n-1} a_i x^i\Big) \in I$$

    Thus we see that I is a prime ideal.

    Now assume that I is a maximal ideal. Then $R[[x]]/I$ must be a field. We'll show that $R[[x]]/I \cong R$. Consider the map

$$\phi : R[[x]] \to R : p \to p(0)$$

    where 0 is the additive identity of R. Then by way addition and multiplication is defined in $R[[x]]$, we see that ϕ is a ring homomorphism. Moreover if $p = \sum_{i=1}^{n} a_i x^i \in I$, then $p(0) = 0$ shows that $I \subset \mathrm{Ker}(\phi)$. Maximality of I forces $I = \mathrm{Ker}(\phi)$, since ϕ is a non trivial ring homomorphism. Then by the first isomorphism therom, we get $R[[x]]/I \cong R$. Hence we see that R is a field.

14. Let R be a commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

Solution: Let P be a prime ideal of a finite unital commutative ring R. Then consider R/P, the collection of all additive cosets of P. Let $r + P \in R/P$. Since R/P is finite $r^n+P = (r+P)^n = (r+P)^m = r^m+P$ for some $n > m \in \mathbb{N}$. This forces $r^n - r^m = r^m(r^{n-m} - 1) \in P$. Now there can be two choices, either $r^m \in P$ or $r^{m-n} - 1 \in P$.

For the former case if $r^m \in P$, since $r^m = rr^{m-1} \in P$, by an induction argument, we see that $r \in P$. Then $r + P = P$ is the zero element in R/P.

In the latter case, if $r^{n-m} - 1 \in P$, we get $r^{n-m} + P = 1 + P$, and thus

$$\begin{aligned}
(r + P)(r + P)^{n-m-1} &= r^{n-m} + P \\
&= 1 + P \\
&= r^{n-m} + P \\
&= (r + P)^{n-m-1}(r + P)
\end{aligned}$$

Which shows that $r+P$ is invertible. Since $r+P$ was arbitrary, we have shown that every non-zero element of R/P is invertible making R/P a field. Thus P is maximal.