Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 23, 2020

Supplementary Problems.

1. Let R be a commutative ring; an ideal P of R is said to be a prime ideal of R if $ab \in P$, $a, b \in R$ implies that $a \in P$ or $b \in P$. Prove that P is a prime ideal of R if and only if R/P is an integral domain.

Proof. Note that

$$[ab \in P \implies a \in P \text{ or } b \in P]$$

is equivalent to

$$[(a+P)(b+P) = ab + P = P \implies a + P = P \text{ or } b + P = P].$$

Therefore, P is a prime ideal if and only if R/P is an integral domain. □

2. Let R be a commutative ring with unit element; prove that every maximal ideal of R is a prime ideal.

Proof. Let M be a maximal ideal of R. Then R/M is a field, and hence an integral domain. Therefore, by Problem 1, M is a prime ideal. □

3. Give an example of a ring in which some prime ideal is not a maximal ideal.

Solution. The trivial ideal (0) is a prime ideal, but not maximal. □

4. If R is a finite commutative ring (i.e., has only a finite number of elements) with unit element, prove that every prime ideal of R is a maximal ideal of R.

Proof. Let P be a prime ideal of R. Then R/P is an integral domain. Since R is finite, R/P is also finite. Since every finite integral domain is a field, R/P is a field. Now it follows that P is maximal. □

5. If F is a field, prove that $F[x]$ is isomorphic to $F[t]$.

Proof. Let $\phi : F[x] \to F[t]$ be a mapping defined as

$$\phi(f(x)) = \phi(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 t + \cdots a_n t^n = f(t).$$

Clearly it is an onto isomorphism from $F[x]$ to $F[t]$. $\square$

6. Find all the automorphisms σ of $F[x]$ with the property that $\sigma(f) = f$ for every $f \in F$.

Proof. Suppose σ is an automorphism of $F[x]$ such that $\sigma(f) = f$ for every $f \in F$. Then σ is determined by the image of x. That is, the polynomial $\sigma(x)$. Since $F[\sigma(x)] \subset F[x]$. For this mapping to be surjective, $\sigma(x)$ cannot have degree of larger than 2. So, we are left with the case $\sigma(x) = ax + b$ where $a \neq 0, b \in F$. This is surjective, as $g(x) = (x-b)/a$ will do the inverse map and hence, $F[\sigma(x)] = F[x]$. Therefore, σ's mapping x to $ax + b$, $a \neq 0, b \in F$ are the automorphisms of $F[x]$. $\square$

7. If R is a commutative ring, let $N = \{x \in R : x^n = 0 \text{ for some integer } n\}$. Prove
a) N is an ideal of R.

Proof. This is exactly the lemma introduced in Problem 7, Section 3.11. $\square$

b) In $\overline{R} = R/N$ if $\overline{x}^m = 0$ for some m then $\overline{x} = 0$.

Proof. Suppose $\overline{x}^m = 0$ for some m. Equivalently, $x^m \in N$. Now by the definition of N, $(x^m)^n = 0$ for some n. Consequently, $(x^m)^n = x^{mn} = 0$ which implies that $x \in N \iff \overline{x} = 0$. $\square$

8. Let R be a commutative ring and suppose that A is an ideal of R. Let $N(A) = \{x \in R : x^n \in A \text{ for some integer } n\}$. Prove
a) $N(A)$ is an ideal of R which contains A.

Proof. $N(A)$ clearly contains A. Let $x, y \in N(A)$. Suppose m and n are the integers satisfying $x^m, y^n \in A$. As A being an ideal of R,

$$\begin{aligned}(x+y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} = (y^{m+n} + xy^{m+n-1} + \cdots + x^{m-1}y^{n+1} \\ &\quad + x^m y^n + x^{m+1}y^{n-1} + \cdots + x^{m+n-1}y + x^{m+n}) \\ &= y^m y^n + (xy^{m-1})y^n + \cdots + (x^{m-1}y)y^m + x^m y^n + \\ &\quad + x^m(xy^{n-1}) + \cdots + x^m(x^{n-1}y) + x^m x^n \in A\end{aligned}$$

so that $x + y \in N(A)$. Also, $(-x)^{2m} = x^{2m} = x^m x^m \in A$ so that $-x \in N(A)$. Further, for any $r \in R$, $(rx)^m = r^m x^m \in A$. Thus, $N(A)$ is an ideal of R. $\square$

b) $N(N(A)) = N(A)$.

Proof. Clearly $N(A) \subset N(N(A))$. Suppose $x \in N(N(A))$. Then $x^n \in N(A)$ for some n. Further, $(x^n)^m \in A$ for some m. Since $x^{nm} = (x^n)^m$, $x \in N(A)$. Therefore, $N(N(A)) \subset N(A)$ so that $N(N(A)) = N(A)$. □

9. If n is an integer, let J_n be the ring of integers mod n. Describe N for J_n in terms of n.

Proof. Let the prime factorization of n be $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. We claim that $N(A) = (p_1 p_2 \cdots p_k)$. Suppose $x \in (p_1 p_2 \cdots p_k)$. Then $x = bp_1 p_2 \cdots p_k$. Let $a = \max\{a_1, a_2, \cdots a_k\}$. Then $x^a = (bp_1 p_2 \cdots p_k)^a$ and since $n \mid (bp_1 p_2 \cdots p_k)^a$, $n \mid x^a \iff x^a = 0$ in J_n. Now conversely, assume that $x \in N(A)$. That is, $x^m = 0$ for some integer m. If $x = 0$, it is done. If $x \neq 0$, assume that $p_1 p_2 \cdots p_k \nmid x$ for the sake of contradiction. Consequently, there exists a prime p_i such that $p_i \nmid x$. Hence, $p_i \nmid x^m$ for all positive integer m and hence $n \nmid x^m$, $x^m \neq 0$. But this is a contradiction. Hence it is must that $p_1 p_2 \cdots p_k \mid x$ and hence,$x \in (p_1 p_2 \cdots p_k)$. □

10. If A and B are ideals in a ring R such that $A \cap B = (0)$, prove that for every $a \in A$, $b \in B$, $ab = 0$.

Proof. Note that $ab \in A \cap B$, as A and B are ideals of R. Therefore, $ab = 0$. □

11. If R is a ring, let $Z(R) = \{x \in R : yx = xy \text{ all } y \in R\}$. Prove that $Z(R)$ is a subring of R.

Proof. Choose $a, b \in Z(R)$. Then $(a + (-b))y = ay + (-b)y = ya + y(-b) = y(a + (-b))$ for all $y \in R$. Hence $a + b \in Z(R)$. Also, $(ab)y = a(by) = a(yb) = (ay)b = (ya)b = y(ab)$ so that $xy \in Z(R)$. These shows that $Z(R)$ is a subring of R. □

12. If R is a division ring, prove that $Z(R)$ is a field.

Proof. It is trivial that $Z(R)$ is commutative. Hence $Z(R)$ is a commutative division ring, and hence a field. □

13. Find a polynomial of degree 3 irreducible over the ring of integers, J_3, mod 3. Use it to construct a field having 27 elements.

Solution. Let $p(x) = x^3 - x - 1$. It is clearly an irreducible polynomial of degree 3 in J_3. Consequently, $J_3[x]/(p(x))$ is a field, with 27 elements. □

14. Construct a field having 625 elements.

Solution. Let $p(x) = x^5 - x - 1$. If it had a quadratic factor $f(x)$, then $J_5[x]/(f(x)) \simeq J_{25}$ so that

$$w^5 = w + 1, \quad w = w^{25} = (w + 1)^5 = w^5 + 1 = w + 2,$$

which is a contradiction. Therefore, $p(x)$ is irreducible in J_5. Now consider the field $J_5[x]/(p(x))$. Then it is a field, with $5^4 = 625$ elements. $\square$

15. If F is a field and $p(x) \in F[x]$, prove that in the ring

$$R = \frac{F[x]}{(p(x))},$$

N(Nilradical of R) is (0) if and only if $p(x)$ is not divisible by the square of any polynomial.

Proof. Suppose $N = (0)$. For the sake of contradiction, assume that $p(x)$ is divisible by some square of a non-costant polynomial $t(x)$. Then $t(x)^2 d(x) = p(x)$ for some $d(x) \in F[x]$. Note that $t(x)d(x)$ is not in $(p(x))$. But since $(t(x)d(x))^2 \in (p(x))$, $t(x)d(x) \in N$ which contradicts the fact that $N = (0)$.
Conversely, assume that $p(x)$ is not divisible by the square of any polynomial. With the fact that $F[x]$ is an UFD, $p(x)$ can be expressed as product of unique irreducible polynomials(upto associates), which are all distinct. Consider $t(x)$ which is not in $(p(x))$. Then $t(x)$ must be missing an irreducible factor of $p(x)$. Consequently, $t(x)^n$ cannot contain that missing factor for any n. Thus, $t(x)^n \notin (p(x))$ for all n. Therefore, $N = (0)$. $\square$

16. Prove that the polynomials $f(x) = 1 + x + x^3 + x^4$ is not irreducible over any field F.

Proof. It it easy to see that $f(x) = 1 + x + x^3(x+1) = (x^3+1)(x+1)$. Therefore, $f(x)$ is not irreducible over any field F. $\square$

17. Prove that the polynomial $f(x) = x^4 + 2x + 2$ is irreducible over the field of rational numbers.

Proof. Apply Eisenstein's Criterion. Let a_i denote the coefficients of x^i. Then $2 \nmid a_4, 2 \mid a_i, i \leq 3$ but $2^2 = 4 \nmid a_0 = 2$. Thus, given $f(x)$ is irreducible over $\mathbb{Q}$. $\square$

18. Prove that if F is a finite field, its characteristic must be a prime number p and F contains p^n elements for some integer. Prove further that if $a \in F$ then $a^{p^n} = a$.

Proof. Let m denote the number of elements in F. Then viewing F as a additive group, $m \cdot 1 = 0$. Hence F must be a field of finite characteristic, with p, a prime as its characteristic. Suppose m has another prime factor q other than p. Then by Cauchy's theorem, there is an element x of order q. Note that $(p, q) = 1$. Hence, $pr + qs = 1$ for some integers r and s. Consequently $x(pr + qs) = x \iff x = 0$, which is a contradiction. Hence, $m = p^n$ for some n. Now viewing $F^\times$ as a multiplicative group, $a^{p^n - 1} = 1$ so that $a^{p^n} = a$. $\square$

19. Prove that any nonzero ideal in the Gaussian integers $J[i]$ must contain some positive integers.

Proof. Let A be a nonzero ideal of $J[i]$. Say, $a + bi \in A$, where a and b are not both zero. Then $(a-bi)(a+bi) = a^2+b^2 \in A$ so that A contains a positive integer. Hence proved. $\square$

20. Prove that if R is a ring in which $a^4 = a$ for every $a \in R$ then R must be commutative.

Proof. Note that $(-x)^4 = x = -x$ so that $2x = 0$ for all $x \in R$. So expanding $(x + x^2)^2$, we have

$$(x + x^2)^2 = x^4 + 2x^3 + x^2 = x + x^2.$$

This shows that elements of the form $x + x^2$ is idempotent. We know that any idempotent elements are central elements. That is, they lie in $Z(R)$. Let $x = a + b$. Then

$$a(x + x^2) = (x + x^2)a \iff a^2b + a(b + b^2) = ba^2 + (b + b^2)a \iff a^2b = ba^2. \quad (1)$$

Since b was arbitrary, elements of the form x^2 also lies in $Z(R)$. Since $Z(R)$ being the subring of R, $a = (a+a^2)-a^2$ is also in $Z(R)$. Now a was arbitrary, and hence, $Z(R) = R$. Therefore, R is commutative. $\square$

21. Let R and R' be rings and ϕ a mapping from R into R' satisfying
a) $\phi(x + y) = \phi(x) + \phi(y)$ for every $x, y \in R$.
b) $\phi(xy) = \phi(x)\phi(y)$ or $\phi(y)\phi(x)$.
Prove that for all $a, b \in R$, $\phi(ab) = \phi(a)\phi(b)$ or that, for all $a, b \in R$, $\phi(ab) = \phi(b)\phi(a)$.

Proof. Let $a \in R$. We define W_a and U_a as follows:

$$W_a = \{x \in R : \phi(ax) = \phi(a)\phi(x)\}, \quad U_a = \{x \in R : \phi(ax) = \phi(x)\phi(a)\}.$$

It is easy to see that both W_a and U_a are additive subgroups of R and $R = W_a \cup U_a$, by the definition of ϕ. Since no group can be written as union of two subgroup, either $R = W_a$ or $R = U_a$. This is equivalent to $\phi(ab) = \phi(a)\phi(b)$ either $\phi(ab) = \phi(b)\phi(a)$, for every $a, b \in R$. $\square$

22. Let R be a ring with a unit element 1, in which $(ab)^2 = a^2b^2$ for all $a, b \in R$. Prove that R must be commutative.

Proof. We compute $((1+a)b)^2$, $(a(1+b))^2$ and $((1-a)(1-b))^2$ in two ways each. Observe that

$$((1 + a)b)^2 = (1 + a)^2b^2 \iff bab = ab^2,$$
$$((a(1 + b))^2 = a^2(1 + b)^2 \iff aba = a^2b,$$

and

$$((1 - a)(1 - b))^2 = (1 - a)^2(1 - b)^2 \iff ab - ab^2 - a^2b = ba = bab - aba$$
$$\iff ab = ba.$$

Therefore, R is commutative. $\square$

23. Give an example of a noncommutative ring (of course, without 1) in which $(ab)^2 = a^2b^2$ for all elements a and b.

Proof. Consider the ring R defined as:

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_2 \right\}$$

Then for any $a = \begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}$,

$$(ab)^2 = \begin{pmatrix} pr & ps \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} (pr)^2 & p^2rs \\ 0 & 0 \end{pmatrix}$$

where

$$a^2b^2 = \begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix}^2 \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} p^2 & pq \\ 0 & 0 \end{pmatrix} \begin{pmatrix} r^2 & rs \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} (pr)^2 & p^2rs \\ 0 & 0 \end{pmatrix}$$

so that $(ab)^2 = a^2b^2$. But R is not commutative as

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

□

24. a) Let R be a ring with unit element 1 such that $(ab)^2 = (ba)^2$ for all $a, b \in R$. If in R, $2x = 0$ implies $x = 0$, prove that R must be commutative.

Proof. Similarly with Problem 22, we compute $((1+a)b)^2$, $(a(1+b))^2$ and $((1-a)(1-b))^2$ in two ways each. Observe that

$$((1+a)b)^2 = (b(1+a))^2 \iff ab^2 = b^2a,$$
$$((a(1+b))^2 = ((1+b)a)^2 \iff a^2b = ba^2,$$

and

$$((1-a)(1-b))^2 = ((1-b)(1-a))^2 \iff 2ab - a^2b - ab^2 = 2ba - b^2a - ba^2$$
$$\iff 2(ab - ba) = 0 \implies ab = ba.$$

Therefore, R is commutative. □

b) Show that the result of a) may be false if $2x = 0$ for some $x \neq 0$.

Proof. Consider the ring R defined as:

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \,\middle|\, a, b, c, d \in \mathbb{Z}_2 \right\}$$

It consists of the unit element I_3. Further, suppose $a = \begin{pmatrix} p & q & r \\ 0 & p & s \\ 0 & 0 & p \end{pmatrix}$ and $b = \begin{pmatrix} x & y & z \\ 0 & x & w \\ 0 & 0 & x \end{pmatrix}$.

Then

$$(ab)^2 = \begin{pmatrix} px & py + qx & pz + qw + rx \\ 0 & px & pw + sx \\ 0 & 0 & px \end{pmatrix}^2 = \begin{pmatrix} (px)^2 & 0 & (py + qx)(pw + sx) \\ 0 & (px)^2 & 0 \\ 0 & 0 & (px)^2 \end{pmatrix},$$

$$(ba)^2 = \begin{pmatrix} px & py + qx & pz + sy + rx \\ 0 & px & pw + sx \\ 0 & 0 & px \end{pmatrix}^2 = \begin{pmatrix} (px)^2 & 0 & (py + qx)(pw + sx) \\ 0 & (px)^2 & 0 \\ 0 & 0 & (px)^2 \end{pmatrix},$$

so that $(ab)^2 = (ba)^2$. We also see that $2I_3 = 0$ but $I_3 \neq 0$. Moreover, R is not commutative since

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0 \neq \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

□

c) Even if $2x = 0$ implies $x = 0$ in R, show that the result of a) may be false if R does not have a unit element.

Proof. Consider the ring R defined as:

$$R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Z}_3 \right\}$$

This ring has no unit element, and $2x = 0$ holds only for $x = 0$. Moreover, power of every product a and b is zero. That is, $(ab)^2 = 0 = (ba)^2$ for all $a, b \in R$. But R is not commutative since

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

□

25. Let R be a ring in which $x^n = 0$ implies $x = 0$. If $(ab)^2 = a^2b^2$ for all $a, b \in R$, prove that R is commutative.

Proof. We shall compute $(a(a+b))^2$ and $((a+b)b)^2$ in two different ways each. Observe that

$$(a(a+b))^2 = a^2(a+b)^2 \iff aba^2 = a^2ba,$$
$$((a+b)b)^2 = (a+b)^2b^2 \iff b^2ab = bab^2,$$

so that

$$(ab - ba)^3 = 0 \implies ab = ba.$$

Therefore, R is commutative. □

26. Let R be a ring in which $x^n = 0$ implies $x = 0$. If $(ab)^2 = (ba)^2$ for all $a, b \in R$, prove that R must be commutative.

Proof. We can get $(ab-ba)^5 = 0$ which leads to $ab = ba$. Refer "Commutativity Theorems Examples in Search of Algorithms", John J Wavrik, Dept of Math Univ of Calif - San Diego. □

27. Let $p_1, p_2, \cdots, p_k$ be distinct primes, and let $n = p_1p_2\cdots p_k$. If R is the ring of integers modulo n, show that there are exactly 2^k elements a in R such that $a^2 = a$.

Proof. By the Chinese Remainder Theorem,

$$R = Z_n \simeq Z_{p_1} \times Z_{p_2} \times \cdots \times Z_{p_k}.$$

Note that for each Z_{p_i}, there are exactly 2 elements in Z_{p_i} satisfying $a^2 = a$. Therefore, there are total of k times of 2, 2^k elements in R satisfying $a^2 = a$. □

28. Construct a polynomial $q(x) \neq 0$ with integer coefficients which has no rational roots but is such that for any prime p we can solve the congruence $q(x) \equiv 0 \bmod p$ in the integers.

Proof. From the theory of Quadratic residues, $x^2 \equiv -1 \bmod p$ has solution iff $p \equiv 1 \bmod 4$. Also, $x^2 \equiv 2 \bmod p$ has solution iff $p \equiv 1, 7 \bmod 8$ and $x^2 \equiv -2 \bmod p$ has solution iff $p \equiv 1, 3 \bmod 8$. Therefore, for every prime p, it must have either $-1, 2$ or,-2 as its quadratic residue. Thus, $q(x) = (x^2+1)(x^2+2)(x^2-2)$ is a polynomial with integer coefficients which has no rational roots, but has a root in Z_p. □