Problems

As usual, we let **R**, **Q**, **C** denote the real, rational, and complex numbers respectively, and let **Z** denote the integers. Some of these problems are taken directly from the book, and in such cases a reference to the appropriate section is given.

You should assume:

- All rings R are commutative.
- All rings R have multiplicative identity.
- All ring homomorphisms $R \to S$ send 1_R to 1_S.

1. (7.1.11) Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.
2. Prove that for any commutative ring R, there is a canonical (unique) ring homomorphism from $\mathbf{Z}$ to R.
3. (7.3.26) Define the characteristic of a ring R to be the smallest positive integer n such that $1 + 1 + \ldots + 1$ (n times) is equal to 0 in R. If no such n exists say that R has characteristic zero.
   (a) If R is a domain, show that the characteristic is either 0 or prime.
   (b) If $\mathbf{Z} \to R$ is the canonical ring homomorphism, show that the kernel of this homomorphism is the ideal (n), where n is the characteristic of R.
   (c) Deduce that if p is prime, then R has characteristic p if and only if there is a ring homomorphism $\mathbf{Z}/p\mathbf{Z} \to R$.
4. (7.3.26) Let R be a commutative ring of characteristic p for some prime p. Prove that the map $\phi : R \to R$ given by $\phi(r) = r^p$ is a homomorphism.
5. (7.3.29) We call $r \in R$ **nilpotent** if $r^n = 0$ in R for some integer n. Let I denote the set of nilpotent elements in R. Prove that I is an ideal.
6. If $r \in R$ is nilpotent, prove that $1 + r$ is a unit in R.
7. (7.3.33) Let $p(x) \in R[x]$, and suppose that $p(x) = a_0 + a_1 x + \ldots + a_n x^n$. Prove that $p(x)$ is nilpotent in $R[x]$ if and only if $a_i \in R$ is nilpotent for every i.
8. (7.3.32) Let $\phi : R \to S$ be a homomorphism of rings. Prove that if $r \in R$ is nilpotent, then $\phi(r) \in S$ is nilpotent.
9. Let $\phi : R \to A$ be a ring homomorphism. Then show that A has the structure of an R-module via $r.a = \phi(r)a$.
10. Suppose that R is a commutative ring. Suppose that the ideals (a) and (b) are equal.
    (a) (7.4.8) If R is a domain, prove that there exists a unit $u \in R$ such that $a = bu$.
    (b) * Is the result still true if R is not assumed to be a domain?
11. **Idempotents:** We call $e \in R$ **idempotent** if $e^2 = e$, and $e \neq 0$.
    (a) Show that 1_R is an idempotent element.

(b) Show that $eR := \{er \mid r \in R\}$ can be given the structure of a ring (with multiplicative identity e) such that the map $\psi : R \to eR$ with $\psi(r) = er$ is a homomorphism.

(c) Suppose that there are rings A and B such that $R \simeq A \oplus B$ as rings. Prove that there exists idempotents e_A and e_B in R such that $e_A + e_B = 1$.

(d) Conversely, suppose that R admits two idempotents e_A and e_B with $e_A + e_B = 1$. Prove that there exist rings A and B with $R \simeq A \oplus B$.

12. **The Euclidean Algorithm:** We proved in class that if R is a Euclidean Domain (ED), then R is a Principal Ideal Domain (PID). It follows that, given $a, b \in R$, we have $(a, b) = (d)$. The Euclidean Algorithm gives an explicit way of finding x and y in R such that $ax + by = d$. Let R be an ED.

    (a) Define a sequence inductively as follows. Let $a_0 = a$ and $a_1 = b$. Given a_{m-1} and a_m, we may, since R is a ED, write

    $$a_{m-1} = q_m a_m + r_m,$$

    where $N(r_m) < N(a_m)$. If $r_m \neq 0$, let $a_{m+1} := r_m$. Prove that this sequence terminates; that is, for some integer n, we have $r_n = 0$.

    (b) Prove that the ideals (a_{m-1}, a_m) and (a_m, a_{m+1}) are equal. (Hint: write a_{m-1} as an element of (a_m, a_{m+1}), and a_{m+1} as an element of (a_{m-1}, a_m).

    (c) Deduce that $(a, b) = (a_0, a_1) = (a_{n-1}, a_n) = (a_n)$, where a_n is the last term in the sequence (where $r_n = 0$).

    (d) Show that a_n can be written as an R-linear combination of a_{n-1} and a_{n-2}.

    (e) Supppose that a_n can be written as an R-linear combination of a_m and a_{m+1}. Prove that a_n can be written as an R-linear combination of a_{m-1} and a_m. (Hint: write a_{m+1} in terms of a_m and a_{m-1}.

    (f) Show that this gives an algorithm for writing $a_n = xa_0 + ya_1 = ax + by$ with x, $y \in R$.

13. Let $p(x) = x^5 + x^3 + x$ and $q(x) = x^2 + 1$ be two elements of $\mathbf{Q}[x]$. Prove that the ideal $I = (p(x), q(x))$ is equal to all of $\mathbf{Q}[x]$, and explicitly construct polynomials $a(x)$ and $b(x)$ such that

    $$a(x)p(x) + b(x)q(x) = 1.$$

    (Hint: use the Euclidean algorithm)

14. For any commutative ring R, prove that there is a unique homomorphism $\phi : \mathbf{Z} \to R$. If R is a domain, prove that either $\ker(\phi) = (0)$ or $\ker(\phi) = (p)$ for some prime p.

15. Prove that the following polynomials are irreducible in $\mathbf{Q}[x]$

    (a) $x^3 - x - 1$

    (b) $(x^4 + 1)^2 + 1$.

16. If $f(x) \in \mathbf{Q}[x]$ is irreducible, then is $f(x^2)$ always irreducible?

17. Find (with proof) all prime ideals in the ring of dual numbers $\mathbf{R}[\epsilon]/\epsilon^2$.

18. (10.1.8)

19. (10.2.1) Show that the image of a module M under a module homomorphism $M \to N$ is a submodule.

20. (10.3.18) homework problem.

21. (10.3.15) (since R is commutative, all idempotents are central).

22. (12.1.13) If M is a finitely generated module over the P.I.D. R, describe the structure of $M/\mathrm{Tor}(M)$.

23. Prove that $I = (x^2 - 1)$, and find polynomials $a(x)$, $b(x)$ such that

$$x^2 - 1 = a(x)(x^{14} - 1) + b(x)(x^8 - 1).$$

Hint: use the Euclidean Algorithm.

24. (7.4.13) Let $\phi : R \to S$ be a homomorphism of commutative rings. Suppose that $P \subset S$ is a prime ideal.

(a) Prove that

$$\phi^{-1}(P) := \{r \in R \mid \phi(r) \in P\}$$

is a prime ideal of R.

(b) If P is a *maximal* ideal of S, show that $\phi^{-1}(P)$ is not always a maximal ideal or R.

(c) if ϕ is surjective, and P is a *maximal* ideal of S, show that $\phi^{-1}(P)$ is a maximal ideal or R.

(d) If Q is a prime ideal of R, is $\phi(Q)$ always a prime ideal of S?

25. (8.1.2) Compute (6003722857,77695236973) using the Euclidean Algorithm.

26. (8.1.8) Let $\omega = \frac{1+\sqrt{-7}}{2}$, and let $R = \mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\}$. Prove that R is a ring with the obvious operations of multiplication and addition. Define a norm on R by the formula:

$$N(a + b\omega) = a^2 + ab + 2b^2.$$

(a) Show that if $x, y \in R$ then $N(xy) = N(x)N(y)$, and that $N(x) = 0$ if and only if $x = 0$.

(b) Prove that R is a Euclidean Domain with respect to this norm.

(c) Write the $(\omega - 7, 11)$ as a principal ideal of R.

(d) Write $(\omega - 23, 127)$ as a principal ideal of R.

27. Let a and b be positive integers, and suppose that $(a, b) = (d)$, with $d > 0$ in $\mathbf{Z}$. Prove that $(x^a - 1, x^b - 1) = (x^d - 1)$ in $\mathbf{Q}[x]$.

28. Exercise 8.3.8

29. (9.2.3) Let $p(x)$ be a polynomial in $K[x]$, for a field K. Prove that $K[x]/p(x)$ is a field if and only if $p(x)$ is irreducible.

30. (9.1.8) Let F be a field, and let $R = F[x, x^2y, x^3y^2, x^4y^3, \ldots, x^ny^{n-1}, \ldots]$ be a subring of $F[x, y]$.

(a) Prove that the field of fractions of R and $F[x, y]$ are the same.

(b) Prove that R contains an ideal that is not finitely generated.

31. Let R be a commutative ring. We call $r \in R$ **nilpotent** if $x^n = 0$ in R for some integer n. Let I denote the set of nilpotent elements in R. Prove that if $P \subset R$ is a prime ideal of R, then $I \subset P$.

32. **The nilradical:** Let R be a commutative ring. If I is the set of nilpotent elements of R, let $R_{\mathrm{red}} = R/I$ (I is called the *nilradical* of R). Prove that:

(a) R_{red} has no nilpotent elements besides zero.

(b) If S is any ring with no nilpotent elements, and there exists a ring homomorphism $\phi : R \to S$, then $I \subset \ker(\phi)$, and thus the map ϕ factors into the map $R \to R_{\text{red}}$ composed with a map from R_{red} to S.

33. **The Jacobson Radical:** Let J be the intersection of all maximal ideals $\mathfrak{m}$ of R. (J is known as the *Jacobson radical* of R.)

(a) Prove that J is an ideal.

(b) Prove that J contains the nilradical I.

(c) Prove that if u is a unit of R, and $x \in J$, then $u + x$ is a unit in R (Hint: show otherwise that $u + x$ is contained in a maximal ideal $\mathfrak{m}$.)

(d) A ring is *Jacobson* if $J = I$.

i. For a field F, prove that $F[T]$ is a Jacobson ring.

ii. For a field F, prove that $F[\![T]\!]$ is not a Jacobson ring.

34. **Local Rings:** A ring A is *local* if it has a unique maximal ideal $\mathfrak{m}$.

(a) Prove that fields F are local rings.

(b) Prove that, if $(A, \mathfrak{m})$ is a local ring (that is, A is a local ring with maximal ideal $\mathfrak{m}$), then $x \in A$ is a unit if and only if $x \in \mathfrak{m}$.

(c) Find a ring A which is a local ring but is *not* a field.

(d) Find an integral domain A which is a local ring but is *not* a field.

35. (7.5.3) Let K be a field. Prove that either:

(a) K has characteristic $p > 0$, and K contains $\mathbf{Z}/p\mathbf{Z}$ as a subfield.

(b) K has characteristic 0, and K contains $\mathbf{Q}$ as a subfield.

36. Let K be a field, and let $K((T))$ denote formal sums:

$$\left\{ \sum_{-\infty}^{\infty} a_n T^n, \;\middle|\; a_n \in K,\ a_n = 0 \text{ for } n \ll 0 \right\}.$$

Prove that $K((T))$ is a field.

37. Express the following finitely abelian groups A in standard form:

(a) The abelian group A generated by x, y, and z subject to the relations:

$$\begin{aligned} 5x + 7y + 14z &= 0 \\ 9x - 3y + 4z &= 0 \end{aligned}$$

(b) The quotient A of $\mathbf{Z}^3$ by the submodule generated by the following vectors:

$$\begin{pmatrix} 3 & 4 & 5 \\ 6 & 7 & 8 \\ -1 & -2 & -4 \\ 4 & 11 & 13 \end{pmatrix}$$

(c) The submodule A of $\mathbf{Z}^3$ generated by the same vectors as the previous question.

(d) Let G be the non-commutative group with presentation

$$G = \langle x, y, z \mid x^3 y x^{-2} = zx, y^{-1} z y = x^3 \rangle$$

Let $[G, G]$ be the commutator subgroup of G, then let A be the abelian group $A = G/[G, G]$.

38. Let $R \subset \mathbf{Q}[x]$ be the subring consisting of all polynomials with vanishing x coefficient. Prove that R is not a P.I.D.

39. Let $R \subset \mathbf{Q}[x]$ be the subring consisting of all polynomials with vanishing x coefficient. Let $S = \mathbf{Q}[y, z]/(y^2 - z^3)$. Prove that the map $S \to R$ given by sending y to x^3 and z to x^2 is an isomorphism.

40. If I and J are two ideals of R, recall that $I + J$ is the ideal generated by $i + j$ for all $i \in I$ and $j \in J$, and $I \cap J$ is the ideal of elements that ie in I and in J. Suppose that $I + J = R$. Prove that

$$R/(I \cap J) \simeq R/I \oplus R/J.$$

Hint: first show that the map $R \to R/I \oplus R/J$ sending r to $(r \mod I, r \mod J)$ has kernel $I \cap J$. Then show that this map is surjective.

41. Let R be a commutative ring, and let R^* denote the set of units in R. Prove that R^* is an abelian group with respect to the multiplcation on R.

42. Let $R = \mathbf{Z}[2i] = \{a + 2bi \mid a, b \in \mathbf{Z}\}$, where $i^2 = -1$. Show that R is a domain, but *not* a P.I.D.

43. (Compare – 12.1.15) Recall that an R-module N is noetherian if every submodule of N is finitely generated.

(a) If $M \subset N$ is an R-submodule, and N is finitely generated, prove that N/M is finitely generated.

(b) If $M \subset N$ is an R-submodule, and M and N/M are finitely generated, prove that N is finitely generated.

(c) If N is noetherian, prove that N/M is noetherian.

(d) If M and N/M are noetherian, prove that N is noetherian.

(e) If R is a noetherian ring (that is R is noetherian as an R-module). prove using (d) that R^n is noetherian for any $n \geq 1$. Deduce from (c) that any finitely generated R-module is noetherian. Thus, if R is a noetherian ring, and M is a finitely generated module, then any submodule of M is also finitely generated.

44. **Hom:** Let R be a commutative ring, and let M and N be R-modules. Let $\mathrm{Hom}_R(M, N)$ denote the collection of R-module homomorphisms:

$$\phi : M \to N.$$

(a) Prove that $\mathrm{Hom}_R(M, N)$ has the structure of an abelian group, where

$$(\phi + \psi)(m) := \phi(m) + \psi(n).$$

(b) Prove that $\mathrm{Hom}_R(M, N)$ has the structure of an R-module, where $(r \cdot \phi)(m) = r \cdot \phi(m)$.

(c) Prove that if $M = R$, i.e., M is a free R-module of rank one, then $\mathrm{Hom}_R(R, N) \simeq N$.

(d) Show that if $M = A \oplus B$ for R-modules A and B then $\mathrm{Hom}_R(M, N) = \mathrm{Hom}_R(A, N) \oplus \mathrm{Hom}_R(B, N)$.

(e) Consider the R-module $\mathrm{Hom}_R(\mathrm{Hom}_R(M, N), N)$, consisting of R-module homomorphisms from $\mathrm{Hom}_R(M, N)$ to N. Show there is a map of R-modules

$$M \to \mathrm{Hom}_R(\mathrm{Hom}_R(M, N), N)$$

defined by sending an element m to the map that sends a homomorphism $\phi \in \mathrm{Hom}_R(M, N)$ to $\phi(m)$.

45. **End:** Let R be a commutative ring, and M and R-module. The R-module $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ has the structure of an R-module by the previous question. In particular, $\mathrm{End}_R(M)$ has an addition.

(a) Prove that $\mathrm{End}_R(M)$ actually has the structure of a (possibly non-commutative) ring, where the multiplication of two maps is their composition, and the identity map $M \to M$ is the multiplicative identity.

(b) If $R = F$ is a field, and $M \simeq F^n$, show that $\mathrm{End}_F(F^n)$ is isomorphic to the non-commutative ring $M_n(F)$ of $n \times n$ matrices.

(c) Prove that there is a natural map of rings $R \to \mathrm{End}_R(M)$ sending the identity to the identity.

(d) Let $Z := Z(\mathrm{End}_R(M))$ be the center of $\mathrm{End}_R(M)$, that is, the R-module homomorphisms which commute (under composition) with all other R-module homomorphisms.

i. Prove that Z is closed under addition.

ii. Prove that Z is a commutative ring with unit (i.e. a ring!)

iii. Prove that the image of the map $R \to \mathrm{End}_R(M))$ lands in Z.

iv. Prove that if R is a field F and $M = F^n$, then the map

$$F \to Z(\mathrm{End}_F(F^n))$$

is an isomorphism. (Hint: show this is equivalent to the following statement: the only matrices in $M_n(F)$ which commute with all other matrices are scalar matrices, i.e. scalar multiples of the identity matrix.)

46. If $R = K$ is a field, then an R-module M is a vector space V. If N is the vector space of dimension one (so $N = K$), we define the *dual* space V^* to be $\mathrm{Hom}_K(M, K)$ (see the question on **Hom**). By the results of that question, V^* is also a K-module so it is also a vector space.

(a) Show that if $\dim(V) = n$, where n is finite, then $\dim(V^*) = n$.

(b) Show that if $\dim(V) = n$, where n is finite, the map

$$V \to V^{**} = \mathrm{Hom}_K(\mathrm{Hom}_K(V, K), K)$$

defined in **Hom** is an isomorphism. Is it still an isomorphism if $\dim(V) = \infty$?

47. (7.4.33) Let R be the ring of all continuous functions from the closed interval $[0, 1]$ to $\mathbf{R}$. Let $I_c := \{f \in R \mid f(c) = 0\}$.

(a) Prove that I_c is an ideal.

(b) Prove that the map: $R \to c$ defined by sending f to $f(c)$ has kernel I_c, and deduce that I_c is a prime ideal and also a maximal ideal.

(c) Prove that if $f \in R$ does not vanish on $[0,1]$ then f is a unit.

(d) Prove that if $f, g \in R$ are two functions such that there does *not* exist a point $c \in \mathbf{R}$ such that $f(c) = g(c) = 0$, then the ideal (f, g) contains a unit. (Hint: squares are always non-negative).

(e) Deduce that any maximal ideal of R is of the form I_c for some $c \in R$,

(f) Prove that if b and c are two distinct points of $[0,1]$ then $I_b \neq I_c$.

(g) Prove that $I_c \neq (x-c)R$.

(h) Prove that I_c is not finitely generated.

48. If A is a matrix with generalized eigenvalues $\lambda_1, \ldots, \lambda_n$, prove that the generalized eigenvalues of A^k are $\lambda_1^k, \ldots, \lambda_n^k$.

49. Let $e \in M_2(\mathbf{C})$ be a matrix such that $e^2 = e$. Prove that e is diagonalizable.

50. Consider pairs (V, ϕ) consisting of a vector space V over $\mathbf{C}$ of dimension n, and a linear operator ϕ from V to itself satisfying $\phi^2 = 0$. Fix a positive integer n. Up to isomorphism, how many such pairs are there of dimension n?

51. If A and B are invertible matrices in $M_n(\mathbf{C})$, prove that AB and BA have the same generalized eigenvalues (counted with multiplicity)

52. * If A, B are matrices in $M_n(\mathbf{C})$, prove that AB and BA have the same generalized eigenvalues (counted with multiplicity).

53. Let $M \in M_2(\mathbf{C})$. Prove that if M is invertible, there exists a matrix $A \in M_2(\mathbf{C})$ such that $A^2 = M$.

54. * Let $M \in M_n(\mathbf{C})$. Prove that if M is invertible, there exists a matrix $A \in M_n(\mathbf{C})$ such that $A^2 = M$.

55. Suppose M is a 4×4 matrix with coefficients in $\mathbf{C}$ and characteristic polynomial $x^2(x^2-1)$. List the possible Jordan canonical forms for M up to conjugation.

56. Suppose M is a 4×4 matrix with coefficients in $\mathbf{C}$ and characteristic polynomial $(x^2+1)^2$. List the possible Jordan canonical forms for M up to conjugation.

57. Let $p(n)$ denote the number of $n \times n$ matrices over $\mathbf{C}$ up to conjugation with characteristic polynomial x^n. Compute $p(n)$ for $n = 1, \ldots, 10$.

58. Prove that $p(n) \geq n$ for all integers n.

59. * For any integer k, prove that $p(n) \geq n^k$ for all sufficiently large (depending on k) integers n.

60. * Let $f(x) \in \mathbf{Q}[x]$. Prove that if $f(x)$ is irreducible, then $f(x)$ has distinct roots (thought of as complex numbers).

61. * Let $p \geq 3$ be prime. Prove that $x^n - x - p$ is irreducible for all n. (Hint: show all the roots α satisfy $|\alpha| > 1$.)