Abstract

This is the Cal Poly Algebra Test Bank. Beginning with the September 2025 exam, all problems will be drawn from a public "problem bank." This bank contains two types of problems: template problems and pool problems. **Template problems** are generally computational with easily adjustable specifics. These types of problems are especially prevalent in linear algebra. **Pool problems** make up the rest of the problem bank, and include all problems that are not easily adjustable. These problems, when chosen, will usually be asked as is.

Group Theory

§ Pool Problems

Exercise 1. Let G be a group. Prove that G is non-cyclic if and only if G is the union of its proper subgroups.

Exercise 2. Let G be a group, and $G \times G$ the direct product. The set $D = \{(g, g) \mid g \in G\}$ is a subgroup of $G \times G$. Prove that if D is normal in $G \times G$ then G is abelian.

Exercise 3. The dihedral group, D_8, is the group of eight rigid symmetries of a square. Prove that D_8 is not the internal direct product of two of its proper subgroups.

Exercise 4. Let G be a finite group and $H, K \trianglelefteq G$ be normal subgroups of relatively prime order. Prove that G is isomorphic to a subgroup of $G/H \times G/K$.

Exercise 5. Suppose G is a group that contains normal subgroups $H, K \trianglelefteq G$ with $H \cap K = \{e\}$ and $HK = G$. Prove that $G \cong H \times K$.

Exercise 6. Let G be the group of upper-triangular real matrices

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

with $a, d \neq 0$, under matrix multiplication. Let S be the subset of G defined by $d = 1$. Show that S is normal and that $G/S \cong \mathbb{R}^\times$, the multiplicative group of nonzero real numbers.

Exercise 7. Let G be a group and suppose $\mathrm{Aut}(G)$ is trivial.

(a) Show that G is abelian.

(b) Show that for any abelian group H, the **inversion map** $\phi(h) = h^{-1}$ is an automorphism.

(c) Use parts (a) and (b) above to show that g^2 is the identity element for every $g \in G$.

Exercise 8.

(a) Suppose N is a normal subgroup of a group G and $\pi_N : G \to G/N$ is the usual projection homomorphism, defined by $\pi_N(g) = gN$. Prove that if $\phi : G \to H$ is any homomorphism with $N \leqslant \ker(\phi)$, then there exists a unique homomorphism $\psi : G/N \to H$ such that $\phi = \psi \circ \pi_N$. (You must explicitly define ψ, show it is well defined, show $\phi = \psi \circ \pi_N$, and show that ψ is uniquely determined.)

(b) Prove the **Third Isomorphism Theorem**: if $M, N \trianglelefteq G$ with $N \leq M$, then $(G/N)/(M/N) \cong G/M$.

Exercise 9. Let G be a group and $a \in G$ be an element. Let $n \in \mathbb{N}$ be the smallest positive number such that $a^n = e$, where e is the identity element. Show that the set

$$\{e, a, a^2, \dots, a^{n-1}\}$$

contains no repetitions.

Exercise 10. Let G be a finite abelian group of odd order. Let $\phi : G \to G$ be the function defined by $\phi(g) = g^2$ for all $g \in G$. Prove that ϕ is an automorphism.

Exercise 11. Let G be a group with exactly two conjugacy classes. Prove that G is abelian, and describe all such groups (with proof).

Exercise 12. Let $\mathbb{Z}_n$ denote the cyclic group of order n. Suppose $m \in \mathbb{N}$ is relatively prime to n. Define the function $\mu_m : \mathbb{Z}_n \to \mathbb{Z}_n$ by $m[a]_n = [ma]_n$.

(a) Prove that the map μ_m is a well-defined automorphism of $\mathbb{Z}_n$.

(b) Prove that any automorphism of $\mathbb{Z}_n$ has the form μ_m for some m.

Exercise 13. For a group G and an element $g \in G$, the **centralizer** of g in G is the subgroup

$$C_G(g) = \{h \in G : hgh^{-1} = g\}.$$

We say g and g' are **conjugate in** G if there exists an element $h \in G$ such that $g' = hgh^{-1}$.

Suppose S_n is a symmetric group with $n \geq 4$, and σ is one of the $(n-2)$-cycles in S_n.

(a) Prove that $[S_n : C_{S_n}(\sigma)] = [A_n : C_{A_n}(\sigma)]$.

(b) Determine whether all $(n-2)$-cycles are conjugate in A_n.

Exercise 14. Let G be a finite group and $n > 1$ an integer such that $(ab)^n = a^n b^n$ for all $a, b \in G$. Let

$$G_n = \{c \in G \mid c^n = e\}, \qquad G^n = \{c^n \mid c \in G\}.$$

You may take for granted that these are subgroups. Prove that both G_n and G^n are normal in G, and $|G^n| = [G : G_n]$.

Exercise 15. Suppose G is a group, $H \leq G$ a subgroup, and $a, b \in G$. Prove that the following are equivalent:

(a) $aH = bH$

(b) $b \in aH$

(c) $b^{-1}a \in H$

Exercise 16. Let G be a group, and let $\mathrm{Aut}(G)$ denote the group of automorphisms of G. There is a homomorphism $\gamma : G \to \mathrm{Aut}(G)$ that takes $s \in G$ to the automorphism γ_s defined by $\gamma_s(t) = sts^{-1}$.

(a) Prove rigorously, possibly with induction, that if $\gamma_s(t) = t^b$, then $\gamma_{s^n}(t) = t^{b^n}$.

(b) Suppose $s \in G$ has order 5, and $sts^{-1} = t^2$. Find the order of t. Justify your answer.

Exercise 17. Let G be an abelian group and G_T be the set of elements of finite order in G.

(a) Prove that G_T is a subgroup of G.

(b) Prove that every non-identity element of G/G_T has infinite order.

(c) Characterize the elements of G_T when $G = \mathbb{R}/\mathbb{Z}$, where $\mathbb{R}$ is the additive group of real numbers.

Exercise 18. Suppose G is a finite group of even order.

(a) Prove that an element in G has order dividing 2 if and only if it is its own inverse.

(b) Prove that the number of elements in G of order 2 is odd.

(c) Use (b) to show G must contain a subgroup of order 2.

Exercise 19. Let N be a finite normal subgroup of G. Prove there is a normal subgroup M of G such that $[G : M]$ is finite and $nm = mn$ for all $n \in N$ and $m \in M$.

(Hint: You may use the fact that the centralizer $C(h) := \{g \in G \mid ghg^{-1} = h\}$ is a subgroup of G.)

Exercise 20. Show that every finite group with more than two elements has a nontrivial automorphism.

Exercise 21. Suppose G_1 and G_2 are groups, with identity elements e_1 and e_2, respectively. Prove that if $\phi : G_1 \to G_2$ is an isomorphism, then $\phi(e_1) = e_2$.

Exercise 22. Suppose A and B are subgroups of a group G, and suppose B is of finite index in G.

(a) Show that the index of $A \cap B \leq A$ is finite, and in fact $|A : A \cap B| \leq |G : B|$. Hint: Find a set map $A/A \cap B \to G/B$.

(b) Prove that equality holds in (a) if and only if $G = AB$.

Exercise 23. Let G be a group. For each $a \in G$, let γ_a denote the automorphism of G defined by $\gamma_a(b) = aba^{-1}$ for all $b \in G$. The set $\mathrm{Inn}(G) = \{\gamma_a : a \in G\}$ is a subgroup of the automorphism group of G, called the subgroup of **inner automorphisms**.

Prove that $\mathrm{Inn}(G)$ is isomorphic to $G/Z(G)$, where $Z(G)$ is the center of G.

Exercise 24. Let G be a group of order $2p$, where p is an odd prime. Prove G contains a nontrivial, proper normal subgroup.

Exercise 25. Prove from the definition along that there are no nonabelian groups of order less than 5.

Exercise 26. Let G be a group and $H, K \trianglelefteq G$ be normal subgroups with $H \cap K = \{e\}$. Show that each element in H commutes with every element in K.

Exercise 27. Let G be a group and N a normal subgroup of G. Let aN denote the left coset defined by $a \in G$, and consider the binary operation

$$G/N \times G/N \to G/N$$

given by $(aN, bN) \mapsto abN$.

(a) Show the operation is well defined.

(b) Show the operation is well defined only if the subgroup N is normal.

Exercise 28. Let G be a group, $H \leq G$ a subgroup that is not normal. Prove there exist cosets Ha and Hb such that $HaHb \neq Hab$.

Exercise 29. Let H be a subgroup of a group G. The **normalizer** of H in G is the set $\mathbb{N}_G(H) = \{g \in G \mid gH = Hg\}$.

(a) Prove $\mathbb{N}_G(H)$ is a subgroup of G containing H.

(b) Prove $\mathbb{N}_G(H)$ is the largest subgroup of G in which H is normal.

Exercise 30. Let G be a group and suppose $H \leq G$. The **normalizer** of H in G is defined to be $N(H) = \{g \in G \,|\, gH = Hg\}$ and the **centralizer** of H in G is defined to be $C(H) = \{g \in G \,|\, gh = hg \text{ for all } h \in H\}$.

(a) Prove that $N(H)$ is a subgroup of G.

(b) Prove that $C(H)$ is a normal subgroup of $N(H)$ and that $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Exercise 31. Suppose G is a cyclic group of order n, and $t \in G$ is a generator.

(a) Give a positive integer d such that $t^{-1} = t^d$.

(b) Let c be an integer and let $m = \gcd(n, c)$. Prove that the order of t^c is $\frac{n}{m}$.

Exercise 32. Let G be a finite group. Prove *from the definitions* that there exists a number N such that $a^N = e$ for all $a \in G$.

Exercise 33. Suppose G is a group and $N \trianglelefteq G$ is a finite normal subgroup. Prove that if G/N contains an element of order n, then G also contains an element of order n.

Exercise 34. Suppose $\phi : G \to G'$ is a surjective homomorphism, $H \leq G$ is a subgroup containing $\ker(\phi)$, and $H' = \phi(H)$. Prove $\phi^{-1}(H') = H$, where $\phi^{-1}(H') = \{g \in G \mid \phi(g) \in H'\}$. Make sure to state explicitly where each hypothesis is used.

Exercise 35. Let G be a group, and H, K be subgroups of G. Let $HK = \{hk \mid h \in H, k \in K\}$ denote the set product. Prove that HK is a group if and only if $HK = KH$.

Exercise 36. Suppose G is a nontrivial finite group and $H, K \trianglelefteq G$ are normal subgroups with $\gcd(|H|, |K|) = 1$.

(a) Define a nontrivial group homomorphism $\phi : G \to G/H \times G/K$

(b) Prove G is isomorphic to a subgroup of $G/H \times G/K$.

(c) Suppose $\gcd(m, n) = 1$. Prove $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Exercise 37. Suppose G is a group, H and K are normal subgroups of G, and $H \leq K$.

(a) Define a group homomorphism from K to G/H.

(b) Compute the kernel of the homomorphism in (a), and apply the First Isomorphism Theorem.

Exercise 38. Let G be a finite group and $\mathrm{Z}(G)$ denote its center.

(a) Prove that if $G/\mathrm{Z}(G)$ is cyclic, then G is abelian.

(b) Prove that if G is nonabelian, then $|\mathrm{Z}(G)| \leq \frac{1}{4}|G|$.

Exercise 39. Let G be a group, $m \in \mathbb{N}$, and $g \in G$ be an element such that $g^m = e$. Prove that $\mathrm{o}(g) \mid m$, where $\mathrm{o}(g)$ is the order of g.

Exercise 40.

(a) Show that if G is any group (not necessarily finite) and H is a subgroup, then G is a disjoint union of left cosets of H.

(b) State and prove Lagrange's Theorem for finite groups.

Exercise 41. Let G be a group and $H \leq G$ a subgroup. For each coset aH of H in G, define the set

$$G_{aH} = \{b \in G \,|\, baH = aH\}.$$

(a) Prove that G_{aH} is a subgroup of G.

(b) Suppose that H is normal in G. Prove that $G_{aH} = H$.

Exercise 42. Let G be a group of order $2n$ for some positive integer $n > 1$.

(a) Prove there exists a subgroup K of G of order 2.

(b) Suppose K in (a) is a *normal* subgroup. Prove that K is contained in the center $\mathrm{Z}(G)$. (Recall $\mathrm{Z}(G) = \{a \in G \mid ab = ba \text{ for all } b \in G\}$.)

Exercise 43. The additive group $\mathbb{Z} = (\mathbb{Z}, +)$ of rational integers is a subgroup of the additive group $\mathbb{Q} = (\mathbb{Q}, +)$. Show that $\mathbb{Z}$ has infinite index in $\mathbb{Q}$.

§ Template Problems

Exercise 44. Let G and H be groups of order 10 and 15, respectively. Prove that if there is a nontrivial homomorphism $\phi : G \to H$, then G is abelian.

Exercise 45. Let n be a number between 0 and 10. Compute $n^{111} \pmod{11}$, expressing your answer as a number between 0 and 10. Give as detailed a proof as you can, justifying every step, no matter how trivial you think it is.

Exercise 46. Let S_n denote the symmetric group on n letters.

(a) Is the element $(1\,2\,3\,4)(2\,5\,3\,4\,6)(1\,5\,3\,2\,4\,7) \in S_7$ even or odd? Indicate your reasoning.

(b) Find the order of $(1\,3\,4)(2\,4\,3)(1\,3\,4) \in S_4$. Show all work.

(c) Write $(1\,5\,2\,3)(2\,1\,3\,4)(1\,5\,2\,3)^{-1} \in S_5$ in disjoint cycle form. Show all work.

Exercise 47. Determine with proof the automorphism group $\mathrm{Aut}(V)$ of the Klein 4-group $V = \{e, a, b, ab\}$. To what familiar group is it isomorphic?

Exercise 48. Determine the number of group homomorphisms ϕ between the given groups. Here K_4 denotes the Klein four-group (also known as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) and S_3 denotes the symmetric group on three elements.

(a) $\phi : K_4 \to \mathbb{Z}/2\mathbb{Z}$

(b) $\phi : \mathbb{Z}/2\mathbb{Z} \to K_4$

(c) $\phi : S_3 \to K_4$

(d) $\phi : K_4 \to S_3$

Exercise 49. Explicitly list all group homomorphisms $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$.

Exercise 50. Let C be a (possibly infinite) cyclic group, and let $\mathrm{Aut}(C)$ and $\mathrm{Inn}(C)$ be the groups of automorphisms and inner automorphisms, respectively. (Recall an automorphism γ is **inner** if it is given by conjugation: $\gamma(b) = aba^{-1}$ for some $a \in C$.)

(a) Describe $\mathrm{Aut}(C)$ and $\mathrm{Inn}(C)$ in familiar terms, as groups you would study in a first algebra course. Prove your result. (*Hint:* Where do generators go?)

(b) Write $\mathrm{Aut}(\mathbb{Z}_{12})$ down explicitly, giving its generic name and computing the order of every element. Show all work.

Exercise 51. Let A_5 denote the alternating group on a 5-element set $\{1, 2, 3, 4, 5\}$. The set of automorphisms of A_5 form a group, denoted $\mathrm{Aut}(A_5)$. The group of **conjugations** of A_5, denoted $\mathrm{Conj}(A_5)$, is the subgroup of $\mathrm{Aut}(A_5)$ consisting of automorphisms of the form $\gamma_s := s(-)s^{-1}$ where $s \in A_5$. Explicitly, $\gamma_s(x) = sxs^{-1}$ for any $x \in A_5$.

(a) Prove that the function $\gamma : A_5 \to \mathrm{Conj}(A_5)$, taking $s \in A_5$ to γ_s, is a surjective homomorphism.

(b) Prove that A_5 is isomorphic to $\mathrm{Conj}(A_5)$.

Exercise 52. Suppose H is a group of order 15. Prove there does not exist a nontrivial group homomorphism $\phi : D_5 \to H$, where D_5 is the dihedral group with ten elements.

Exercise 53. Let S_7 denote the symmetric group.

(a) Give an example of two non-conjugate elements of S_7 that have the same order.

(b) If $g \in S_7$ has maximal order, what is the order of g?

(c) Does the element g that you found in part (b) lie in A_7? Fully justify your answer.

(d) Determine whether the set $\{h \in S_7 \mid |h| = |g|\}$ is a single conjugacy class in S_7, where g is the element you found in part (b).

Exercise 54. Let G be the additive group $\mathbb{Z}_{2020}$ and let $H \subseteq G$ be the subset consisting of those elements with order dividing 20.

(a) Prove H is a subgroup of G.

(b) Find an explicit generator for H and determine its order.

Exercise 55. Let G denote the set of invertible 2×2 matrices with values in a field. Prove G is a group by defining a group law, identity element, and verifying the axioms. Credit is based on completeness.

Ring Theory

§ Pool Problems

Exercise 56. Consider the additive group of integers $\mathbf{Z}$.

(a) Prove that every subgroup of $\mathbf{Z}$ is cyclic.

(b) Prove that every homomorphic image of $\mathbf{Z}$ is cyclic.

(c) Consider the *ring* $\mathbf{Z}$. Exhibit a prime ideal of $\mathbf{Z}$ that is not maximal.

Exercise 57. Let R be an integral domain. Suppose a and b are non-associate irreducible elements in R, and the ideal (a, b) generated by a and b is a proper ideal. Show that R is not a principal ideal domain (PID).

Exercise 58. Let R be a commutative ring with 1. Suppose that for every $a \in R$ there exists $n \geq 2$ such that $a^n = a$. Show that every prime ideal of R is maximal.

Exercise 59. Let R be a commutative ring with 1, and $\sigma : R \to R$ be a ring automorphism.

(a) Show that $F = \{r \in R \mid \sigma(r) = r\}$ is a subring of R with 1.

(b) Show that if σ^2 is the identity map on R, then each element of R is the root of a monic polynomial of degree 2 in $F[x]$, where F is as in (a).

Exercise 60. Suppose R is a ring such that $r^2 = r$ for every $r \in R$.

(a) Prove that $r = -r$ for every $r \in R$.

(b) Show that R must be commutative. *Hint: Consider* $(a + b)^2$.

Exercise 61. Let R be a commutative ring with 1. The **characteristic** $\mathrm{char}(R)$ of R is the unique integer $n \geq 0$ such that $\langle n \rangle \subset \mathbf{Z}$ is the kernel of the homomorphism $\theta : \mathbf{Z} \to R$ defined by

$$\theta(m) = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{m}, & m \geq 0 \\ \underbrace{-1_R + \cdots + -1_R}_{|m|}, & m < 0 \end{cases}.$$

(a) Prove that if $f : R \to S$ is a monomorphism of commutative rings with 1, then $\mathrm{char}(R) = \mathrm{char}(S)$.

(b) Give an example showing that $\mathrm{char}(R)$ is not always preserved by ring homomorphisms.

Exercise 62. (a) Prove that for every commutative ring with unity R, there is a unique ring homomorphism $\phi_R : \mathbf{Z} \to R$, and that $\ker(\phi_R) = \langle d_R \rangle$ for a unique nonnegative integer d_R. The number d_R is called the **characteristic** of R, denoted $\mathrm{char}(R)$.

(b) Suppose F_1 and F_2 are fields for which there exists a ring homomorphism $f : F_1 \to F_2$. Prove that $\mathrm{char}(F_1) = \mathrm{char}(F_2)$.

Exercise 63. Let A be a commutative ring with 1. The **dimension** of A is the maximal length d of a chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$. Prove that if A is a PID, then $\dim(A) \leq 1$.

Exercise 64. Prove that every Euclidean domain is a principal ideal domain.

Exercise 65. Let F be a field and let α generate a field extension of F of degree 5. Prove that α^2 generates the same extension.

Exercise 66. Let R be a commutative ring with 1. Use theorems in ring theory to prove:

(a) $\langle x \rangle$ is a prime ideal in $R[x]$ if and only if R is an integral domain.

(b) $\langle x \rangle$ is a maximal ideal in $R[x]$ if and only if R is a field.

Exercise 67. Let F be a field and $F[x]$ the polynomial ring, which is a PID. Let

$$R = \{f \in F[x] : f' \in (x)\},$$

where $(x) \subset F[x]$ and f' is the formal derivative.

(a) Prove that x^2 and x^3 are irreducible elements of R.

(b) Let (x^2, x^3) be the ideal generated by x^2 and x^3. Prove it is a proper ideal of R.

(c) Prove that (x^2, x^3) is not a principal ideal of R.

Exercise 68. Let R be a commutative ring with 1 and $e \in R$ an idempotent element ($e^2 = e$).

(a) Prove that $1 - e$ is idempotent.

(b) If $e \neq 0, 1$, show that Re and $R(1-e)$ are proper ideals of R.

(c) Prove that $R \cong Re \times R(1-e)$.

Exercise 69. An element r of a ring R is idempotent if $r^2 = r$. Suppose R is commutative with 1 and contains an idempotent e.

(a) Prove $1 - e$ is idempotent.

(b) Prove eR and $(1-e)R$ are ideals and $R \cong eR \times (1-e)R$.

(c) Prove that if R has a unique maximal ideal, the only idempotents are 0 and 1.

Exercise 70. Prove that if $\phi : R \to S$ is a surjective ring homomorphism between commutative rings with 1, then $\phi(1_R) = 1_S$.

Exercise 71. Suppose R is a PID. Prove that an ideal $I \subset R$ is maximal if and only if $I = \langle p \rangle$ for a prime $p \in R$.

Exercise 72. Let R be a commutative ring.

(a) Prove that the set N of all nilpotent elements of R is an ideal.

(b) Prove that R/N has no nonzero nilpotent elements.

(c) Show that N is contained in every prime ideal of R.

Exercise 73. Let R be a commutative ring with 1. An element $n \in R$ is nilpotent if $n^k = 0$ for some $k \in \mathbf{N}$.

(a) Show that if n is nilpotent, then $1 - n$ is a unit.

(b) Give an example of a commutative ring with 1 with no nonzero nilpotent elements, but not an integral domain.

Exercise 74. Let D be a PID. Prove that every proper nonzero prime ideal is maximal.

Exercise 75. Let $I \subseteq \mathbf{Z}[x]$ be the set of polynomials with even constant term.

(a) Prove that I is an ideal.

(b) Prove that I is not a principal ideal.

Exercise 76. Let R be a commutative ring with 1.

(a) Define what it means for an element to be **prime** and **irreducible**.

(b) Prove that if R is an integral domain, every prime element is irreducible.

Exercise 77. Let R be a commutative ring with 1, $I \subseteq R$ an ideal, and $\pi : R \to R/I$ the natural projection.

(a) Show that if $\wp$ is a prime ideal of R/I, then $\pi^{-1}(\wp)$ is a prime ideal of R.

(b) Show that the map $\wp \mapsto \pi^{-1}(\wp)$ is injective on prime ideals of R/I.

Exercise 78. Let A be a commutative ring with 1. We say A is **Boolean** if $a^2 = a$ for every $a \in A$. Prove that in a Boolean ring:

(a) $2a = 0$ for all $a \in A$.

(b) If I is a prime ideal, then A/I has two elements, so I is maximal.

(c) If $I = (a, b)$, then I can be generated by $a + b + ab$. Conclude every finitely generated ideal is principal.

Exercise 79. Let R be a commutative ring. For $X \subseteq R$ nonempty, define the **annihilator** $\text{ann}(X) = \{a \in R \mid ax = 0 \text{ for all } x \in X\}$.

(a) Prove that $\text{ann}(X)$ is an ideal.

(b) Prove that $X \subseteq \text{ann}(\text{ann}(X))$.

Exercise 80. Suppose $\phi : R \to S$ is a ring homomorphism, and S has no nonzero zero-divisors. Prove that $\ker(\phi)$ is a prime ideal.

Exercise 81. Let R be a commutative ring with 1, and $N = \{a \in R \mid a^n = 0 \text{ for some } n\}$. Let $[b]$ be the image of $b \in R$ in R/N. Prove that if $[a]^m = 0$ in R/N, then $[a] = [0]$.

Exercise 82. Let R be a commutative ring. The **nilradical** of R is $N = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbf{N}\}$.

(a) Prove that N is an ideal of R.

(b) Prove that N is contained in the intersection of all prime ideals of R.

§ Template Problems

Exercise 83. Suppose I and J are ideals in a commutative ring R such that $R = I + J$.

(a) Prove that the map $f : R \to R/I \times R/J$ given by $f(x) = (x+I, x+J)$ induces the isomorphism

$$R/IJ \cong R/I \times R/J.$$

(b) Prove that $(\mathbb{Z}/3\mathbb{Z})[x]/(x^3 - x^2 - 1) \cong (\mathbb{Z}/3\mathbb{Z})[x]/(x^3 + x + 1)$. (*Hint: Use part (a).*)

Exercise 84. Let $\mathcal{C}([0,1])$ be the commutative ring of continuous real-valued functions on $[0,1]$, and let

$$M = \{f \in \mathcal{C}([0,1]) \mid f(1/2) = 0\}.$$

Prove that M is a maximal ideal.

Exercise 85. Let $z \in \mathbb{C}$ and $\epsilon_z : \mathbb{R}[x] \to \mathbb{C}$ be the evaluation homomorphism $\epsilon_z(p) = p(z)$.

(a) Show that $\ker(\epsilon_z)$ is a prime ideal.

(b) Compute $\ker(\epsilon_{1+i})$, $\text{im}(\epsilon_{1+i})$ and state the conclusion of the First Isomorphism Theorem applied to ϵ_{1+i}.

Exercise 86. Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, and let $R \subset \text{M}_2(\mathbb{Z})$ be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$. Prove that $\mathbb{Z}[\sqrt{2}]$ is isomorphic to R.

Exercise 87. Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$.

(a) Prove that $f(x)$ is irreducible.

(b) Prove that $\langle f(x) \rangle$ is a maximal ideal.

(c) Determine the cardinality of $\mathbb{Z}_5[x]/\langle f(x) \rangle$ and justify.

Exercise 88. (a) Write down an irreducible cubic polynomial over $\mathbb{F}_2$.

(b) Construct a field with exactly 8 elements and write its multiplication table.

Exercise 89. Let $\varepsilon : \mathbb{R}[x] \to \mathbb{C}$ be evaluation at i.

(a) Prove that $\ker(\varepsilon) = (x^2 + 1) \subseteq \mathbb{R}[x]$.

(b) Prove that $(x^2 + 1)$ is a maximal ideal in $\mathbb{R}[x]$.

Exercise 90. Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z},\ i^2 = -1\}$.

(a) Prove there is no ring homomorphism $\mathbb{Z}[i] \to \mathbb{Z}_{19}$, but there is one to $\mathbb{Z}_{13}$.

Exercise 91. Let $\mathbb{Z}_n$ be integers modulo n, and consider the ring homomorphism

$$\mathbb{Z}_{28} \to \mathbb{Z}_4 \times \mathbb{Z}_7, \quad [m]_{28} \mapsto ([m]_4, [m]_7),$$

which is an isomorphism by the Chinese Remainder Theorem. Let $\mathbb{Z}_n^\times$ denote the group of units. Prove that $\mathbb{Z}_{28}^\times \cong \mathbb{Z}_4^\times \times \mathbb{Z}_7^\times$.

Exercise 92. Let $k \subset K$ be fields, and $k[X]$ the polynomial ring. The **evaluation** at $z \in K$ is $\varepsilon : k[X] \to K$, $\varepsilon(f(X)) = f(z)$. Prove that if ε is not injective, then $\varepsilon(k[X])$ is a field.

Exercise 93. Let i be the imaginary unit, $\mathbb{Z}[i]$ the Gaussian integers, and $\mathbb{Z}_2$ the finite field with two elements.

(a) Define a ring homomorphism $\mathbb{Z}[i] \to \mathbb{Z}_2$ and prove it is a homomorphism.

(b) Find a generator for the kernel of your homomorphism with proof.

Exercise 94. Let $\mathbb{Z}[i]$ be the Gaussian integers.

(a) Prove there exists a nonzero ring homomorphism $\mathbb{Z}[i] \to \mathbb{Z}_5$.

(b) Compute the kernel explicitly and state the conclusion given by the First Isomorphism Theorem. (*Hint: The kernel requires two generators.*)

Exercise 95. Let $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ be a field of 8 elements with natural projection $\pi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$.

(a) Write down eight distinct coset representatives.

(b) Determine the multiplicative inverse of $\pi(x)$ in terms of your coset representatives.

Exercise 96. Let $\mathbb{F}_9$ be the field of nine elements.

(a) Show that each nonzero $a \in \mathbb{F}_9$ is a root of $X^3 - 1 = (X-1)(X^2+1)(X^4+1) \in \mathbb{F}_3[X]$.

(b) Use the Pigeonhole Principle to prove that $\mathbb{F}_9$ has an element of multiplicative order 8, including a justification for applying the principle.

Exercise 97. Let $\mathbb{Z}[X]$ be the ring of polynomials with integer coefficients, and let $K \subset \mathbb{Z}[X]$ be the kernel of the "evaluation at 1" map.

Linear Algebra

§ Pool Problems

Exercise 98.

(a) Give an explicit example (with proof) showing that the union of two subspaces (of a given vector space) is not necessarily a subspace.

(b) Suppose U_1 and U_2 are subspaces of a vector space V. Recall that their **sum** is defined to be the set $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$. Prove $U_1 + U_2$ is a subspace of V containing U_1 and U_2.

Exercise 99. Suppose F is a field and A is an $n \times n$ matrix over F. Suppose further that A possesses distinct eigenvalues λ_1 and λ_2 with $\dim \operatorname{Null}(A - \lambda_1 I_n) = n - 1$. Prove A is diagonalizable.

Exercise 100. Let $\phi : V \to W$ be a surjective linear transformation of finite-dimensional linear spaces. Show that there is a $U \subseteq V$ such that $V = \ker(\phi) \oplus U$ and $\phi\,|_U : U \to W$ is an isomorphism. (Note that V is not assumed to be an inner-product space; also note that $\ker(\phi)$ is sometimes referred to as the **null space** of ϕ; finally, $\phi\,|_U$ denotes the restriction of ϕ to U.)

Exercise 101. Suppose V is a finite-dimensional real vector space and $T : V \to V$ is a linear transformation. Prove that T has at most $\dim(\text{range } T)$ distinct nonzero eigenvalues.

Exercise 102. Let $T : V \to V$ be a linear transformation on a finite-dimensional vector space. Prove that if $T^2 = T$, then

$$V = \ker(T) \oplus \operatorname{im}(T).$$

Exercise 103. Let $\mathbb{R}^3$ denote the 3-dimensional vector space, and let $\mathbf{v} = (a, b, c)$ be a fixed nonzero vector. The maps $C : \mathbb{R}^3 \to \mathbb{R}^3$ and $D : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $C(\mathbf{w}) = \mathbf{v} \times \mathbf{w}$ and $D(\mathbf{w}) = (\mathbf{v} \cdot \mathbf{w})\mathbf{v}$ are linear transformations.

(a) Determine the eigenvalues of C and D.

(b) Determine the eigenspaces of C and D as subspaces of $\mathbb{R}^3$, in terms of a, b, c.

(c) Find a matrix for C with respect to the standard basis.

Show all work and explain reasoning.

Exercise 104. Suppose A is a real $n \times n$ matrix that satisfies $A^2\mathbf{v} = 2A\mathbf{v}$ for every $\mathbf{v} \in \mathbb{R}^n$.

(a) Show that the only possible eigenvalues of A are 0 and 2.

(b) For each $\lambda \in \mathbb{R}$, let E_λ denote the λ-eigenspace of A, i.e., $E_\lambda = \{\mathbf{v} \in \mathbb{R}^n \mid A\mathbf{v} = \lambda\mathbf{v}\}$. Prove that $\mathbb{R}^n = E_0 \oplus E_2$. (*Hint:* For every vector $\mathbf{v}$ one can write $\mathbf{v} = (\mathbf{v} - \frac{1}{2}A\mathbf{v}) + \frac{1}{2}A\mathbf{v}$.)

Exercise 105. Suppose $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation with distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$, and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ be corresponding eigenvectors. Prove $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ are linearly independent.

Exercise 106. Let $S : V \to V$ and $T : V \to V$ be linear transformations that commute, i.e., $S \circ T = T \circ S$. Let $\mathbf{v} \in V$ be an eigenvector of S such that $T(\mathbf{v}) \neq 0$. Prove that $T(\mathbf{v})$ is also an eigenvector of S.

Exercise 107. Suppose A is a 5×5 matrix and $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are eigenvectors of A with distinct eigenvalues. Prove $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a linearly independent set. *Hint:* Consider a minimal linear dependence relation.

Exercise 108. Suppose V is a vector space, and $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ are in V. Prove that either $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent, or there exists a number $k \leq n$ such that $\mathbf{v}_k$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$.

Exercise 109. Let $M_4(\mathbb{R})$ denote the 16-dimensional real vector space of 4×4 matrices with real entries, in which the vectors are represented as matrices. Let $T : M_4(\mathbb{R}) \to M_4(\mathbb{R})$ be the linear transformation defined by $T(A) = A - A^\top$.

(a) Determine the dimension of $\ker(T)$.

(b) Determine the dimension of $\operatorname{im}(T)$.

Exercise 110. Let A be a real $n \times n$ matrix and let $A^\top$ denote its transpose.

(a) Prove that $(A\mathbf{v}) \cdot \mathbf{w} = \mathbf{v} \cdot (A^\top \mathbf{w})$ for all vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. *Hint:* Recall that the dot product $\mathbf{u} \cdot \mathbf{v}$ equals the matrix product $\mathbf{u}^\top \mathbf{v}$.

(b) Suppose now A is also symmetric, i.e., that $A^\top = A$. Also suppose $\mathbf{v}$ and $\mathbf{w}$ are eigenvectors of A with different eigenvalues. Prove that $\mathbf{v}$ and $\mathbf{w}$ are orthogonal.

Exercise 111. A real $n \times n$ matrix A is called **skew-symmetric** if $A^\top = -A$. Let V_n be the set of all skew-symmetric matrices in $\mathrm{M}_n(\mathbb{R})$. Recall that $\mathrm{M}_n(\mathbb{R})$ is an n^2-dimensional $\mathbb{R}$-vector space with standard basis $\{e_{ij} \mid 1 \leq i, j \leq n\}$, where e_{ij} is the $n \times n$ matrix with a 1 in the (i, j)-position and zeros everywhere else.

(a) Show V_n is a subspace of $\mathrm{M}_n(\mathbb{R})$.

(b) Find an ordered basis $\mathcal{B}$ for the space V_3 of all skew-symmetric 3×3 matrices.

§ Template Problems

Exercise 112. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation that rotates counterclockwise around the z-axis by $\frac{2\pi}{3}$.

(a) Write the matrix for T with respect to the standard basis $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$.

(b) Write the matrix for T with respect to the basis $\left\{ \begin{bmatrix} \frac{\sqrt{3}}{2} \\ -\frac{1}{2} \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$.

(c) Determine all (complex) eigenvalues of T.

(d) Is T diagonalizable over $\mathbf{C}$? Justify your answer.

Exercise 113. Let V denote the real vector space of polynomials in x of degree at most 3. Let $\mathcal{B} = \{1, x, x^2, x^3\}$ be a basis for V and $T : V \to V$ be the function defined by $T(f(x)) = f(x) + f'(x)$.

(a) Prove that T is a linear transformation.

(b) Find $[T]_{\mathcal{B}}$, the matrix representation for T in terms of the basis $\mathcal{B}$.

(c) Is T diagonalizable? If yes, find a matrix A so that $A[T]_{\mathcal{B}}A^{-1}$ is diagonal; otherwise explain why T is not diagonalizable.

Exercise 114. Let $\mathrm{M}_n(\mathbf{R})$ be the vector space of all $n \times n$ matrices with real entries. We say that $A, B \in \mathrm{M}_n(\mathbf{R})$ commute if $AB = BA$.

(a) Fix $A \in \mathrm{M}_n(\mathbf{R})$. Prove that the set of all matrices in $\mathrm{M}_n(\mathbf{R})$ that commute with A is a subspace of $\mathrm{M}_n(\mathbf{R})$.

(b) Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{M}_2(\mathbf{R})$ and let $W \subseteq \mathrm{M}_2(\mathbf{R})$ be the subspace of all matrices that commute with A. Find a basis of W.

Exercise 115. Let $V \subset \mathbf{R}^5$ be the subspace defined by the equation

$$x_1 - 2x_2 + 3x_3 - 4x_4 + 5x_5 = 0.$$

(a) Find (with justification) a basis for V.

(b) Find (with justification) a basis for $V^\perp$, the subspace of $\mathbf{R}^5$ orthogonal to V under the usual dot product.

Exercise 116. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation defined by

$$T\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} x+y \\ 2z-x \\ y+2z \end{bmatrix}.$$

(a) Find the matrix that represents T with respect to the standard basis for $\mathbf{R}^3$.

(b) Find a basis for the kernel of T.

(c) Determine the rank of T.

Exercise 117. Let $A = \begin{bmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix}$.

(a) Determine whether A is diagonalizable, and if so, give its diagonal form along with a diagonalizing matrix.

(b) Compute A^{42}. Remember to show all work.

Exercise 118. Let $A = \begin{bmatrix} 2 & -1 & -1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix}$.

(a) Compute the characteristic polynomial $p_A(x)$ of A.

(b) For each eigenvalue λ of A, find a basis for the eigenspace E_λ.

(c) Determine if A is diagonalizable. If so, give matrices P and B such that $P^{-1}AP = B$ and B is diagonal. If no, explain carefully why A is not diagonalizable.

Exercise 119. Let $A = \begin{bmatrix} 6 & -2 & -1 \\ 10 & -3 & -2 \\ 0 & 0 & 1 \end{bmatrix}$.

(a) Find bases for the eigenspaces of A.

(b) Determine if A is diagonalizable. If so, give an invertible matrix P and diagonal matrix D such that $P^{-1}AP = D$. If not, explain why not.

Exercise 120. Let $W \subset \mathbf{R}^5$ be the subspace spanned by the set of vectors

$$\{\langle 1,-2,0,2,-1\rangle, \langle -2,4,-1,1,2\rangle, \langle 0,1,2,-2,1\rangle\}.$$

(a) Compute the dimension of W.

(b) Determine the dimension of $W^\perp$, the perpendicular subspace in $\mathbf{R}^5$.

(c) Find a basis for $W^\perp$.

Exercise 121. Let P_3 be the real vector space of all real polynomials of degree three or less. Define $L : P_3 \to P_3$ by $L(p(x)) = p(x) + p(-x)$.

(a) Prove L is a linear transformation.

(b) Find a basis for the null space of L.

(c) Compute the dimension of the image of L.

Exercise 122. Let $V = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mid a_0, a_1, a_2 \in \mathbf{Q}\} \subseteq \mathbf{R}$. This set is a vector space over $\mathbf{Q}$.

(a) Verify V is closed under product (using the usual product operation in $\mathbf{R}$).

(b) Let $T : V \to V$ be the linear transformation defined by $T(v) = (\sqrt[3]{2} + \sqrt[3]{4})v$. Find the matrix that represents T with respect to the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for V.

(c) Determine the characteristic polynomial for T.

Exercise 123. Suppose $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a basis for $\mathbf{R}^3$ and $T : \mathbf{R}^3 \to \mathbf{R}^3$ is a linear transformation satisfying

$$T(\mathbf{v}_1) = 4\mathbf{v}_1 + 2\mathbf{v}_2, \quad T(\mathbf{v}_2) = 5\mathbf{v}_2, \quad T(\mathbf{v}_3) = -2\mathbf{v}_1 + 4\mathbf{v}_2 + 5\mathbf{v}_3.$$

Determine the eigenvalues of T and find a basis for each eigenspace.

Exercise 124. Let $W \subset \mathbf{R}^5$ be the space spanned by the vectors

$$\left\{ \begin{bmatrix} 1 \\ -2 \\ 0 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ 4 \\ -1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \\ -2 \\ 1 \end{bmatrix} \right\}.$$

(a) Compute the dimension of W.

(b) Let $W^\perp = \{\mathbf{v} \in \mathbf{R}^5 \mid \mathbf{v} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in W\}$. Determine the dimension of $W^\perp$, and explain why this follows immediately from (a) using a theorem.

(c) Find a basis for $W^\perp$.

Exercise 125. Let L be the line in $\mathbf{R}^2$ defined by $y = -3x$, and let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear transformation that orthogonally projects onto L and then stretches along L by a factor of two.

(a) Find the eigenvalues and an eigenbasis $\mathcal{B}$ for T.

(b) Determine the matrix for T with respect to the basis $\mathcal{B}$.

(c) Determine the matrix for T with respect to the standard basis.

Exercise 126. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the orthogonal projection to a 1-dimensional linear subspace $L \subset \mathbf{R}^3$.

(a) List the eigenvalues of T.

(b) Write the characteristic polynomial $p_T(x)$ for T.

(c) Is T diagonalizable? Justify your answer.

Exercise 127. Let L be the line parameterized by $L(t) = (2t, -3t, t)$ for $t \in \mathbf{R}$, and let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation that is orthogonal projection onto L.

(a) Describe $\ker(T)$ and $\mathrm{im}(T)$, either implicitly (using equations in x, y, z) or parametrically.

(b) List the eigenvalues of T and their geometric multiplicities.

(c) Find a basis for each eigenspace of T.

(d) Let A be the matrix for T with respect to the standard basis. Find a diagonal matrix B and an invertible matrix S such that $B = S^{-1}AS$. (You do not have to compute A.)

Exercise 128. Let $T : \mathbf{R}^4 \to \mathbf{R}^4$ be orthogonal projection to the 2-dimensional plane P spanned by the vectors $\mathbf{v} = (2, 0, 1, 0)$ and $\mathbf{w} = (-1, 0, 2, 0)$.

(a) Find (with proof) all eigenvalues and eigenvectors, along with their geometric and algebraic multiplicities.

(b) Find the matrix representing T with respect to the standard basis. Is this matrix diagonalizable? Why or why not?

Exercise 129. Let $a, b \in \mathbf{R}$ and $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation that is orthogonal projection onto the plane $z = ax + by$ (with respect to the usual Euclidean inner-product on $\mathbf{R}^3$).

(a) Find the eigenvalues of T and bases for the corresponding eigenspaces.

(b) Is T diagonalizable? Justify.

(c) What is the characteristic polynomial of T?

Exercise 130. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the orthogonal projection onto the plane $z = x + y$, with respect to the standard Euclidean inner product.

(a) Write the matrix representation of T with respect to the standard basis.

(b) Is T diagonalizable? Justify your answer.

Exercise 131. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation that expands radially by a factor of three around the line parameterized by $L(t) = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix} t$, leaving the line itself fixed.

(a) Find an eigenbasis for T and provide the matrix representation of T with respect to that basis.

(b) Provide the matrix representation of T with respect to the standard basis.

Exercise 132. Let $a, b \in \mathbf{R}$ and $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation which is reflection across the plane $z = ax + by$.

(a) Find the eigenvalues of T and for each find a basis for the corresponding eigenspace.

(b) Is T diagonalizable? Justify.

(c) What is the characteristic polynomial of T?

(d) What is the minimal polynomial of T?