

LSU Algebra Question Bank Solution

Ayanava Mandal

April 2025

Contents

1	Group Theory	1
2	Ring Theory	5
3	Module Theory	9
4	Linear Algebra	11

Chapter 1

Group Theory

G1: Let H be a normal subgroup of a group G , and let K be a subgroup of H .

- (a) Give an example of this situation where K is not a normal subgroup of G ,
- (b) Prove that if the normal subgroup H is cyclic, then K is normal in G .

Solution 1. (a) Let $G = S_4$, $H = A_4$, and $K = \{e, (123), (132)\}$.

- (b) Let $H = \langle h \rangle$ be cyclic. Let $K = \langle k \rangle$ where $k = h^a$ for some $a \in \mathbb{N}$.
 Since H is normal, $ghg^{-1} = h^b \in H$ for some b .
 $gkg^{-1} = gh^a g^{-1} = (ghg^{-1})^a = h^{ba} = k^b \in K$. So, K is normal in G .

□

G2: Prove that every finite group of order at least three has a nontrivial automorphism.

Solution 2. We will try this in two cases:

Case 1: The group is not abelian. Let $g \notin Z(G)$. Let ϕ_g be the nontrivial automorphism $h \mapsto ghg^{-1}$.

Case 2: The group is abelian. If there is an element of order not equal to 2, the inverse map is a nontrivial automorphism. If every element is of order 2: $G = (\mathbb{Z}/2\mathbb{Z})^n$, where $n > 1$. Swap 2 elements. □

G3:

- (a) State the structure theorem for finitely generated Abelian group.
- (b) If p and q are distinct primes, determine the number of nonisomorphic Abelian groups of order $p^3 q^4$.

Solution 3. (a) If G is finitely generated Abelian group, G is isomorphic to $\mathbb{Z}^n \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}$ where $a_i \mid a_{i+1}$, $\mathbb{Z}_a = \mathbb{Z}/a\mathbb{Z}$ cyclic group of order a .

- (b) Let $P(n)$ be the partition function. The number of nonisomorphic Abelian groups of order $p^3 q^4 = P(3)P(4) = 3 \times 5 = 15$.

□

G4: Let $G = \text{GL}(2, \mathbb{F}_p)$ be the group of invertible 2×2 matrices with entries in the finite field \mathbb{F}_p , where p is a prime.

- (a) Show that G has order $(p^2 - 1)(p^2 - p)$.
- (b) Show that for $p = 2$ the group G is isomorphic to the symmetric group S_3 .

Solution 4. Let $G = \text{GL}(2, \mathbb{F}_p)$.

- (a) Choosing a invertible 2×2 matrix is equivalent to choosing two linearly independent vectors (which will be the columns of the matrix) from the space \mathbb{F}_p^2 . We can choose a nonzero vector in $|\mathbb{F}_p^2| - 1 = p^2 - 1$ ways and the second vector can't be a multiple of the first vector (there are p of them). So, we can choose the second vector in $p^2 - p$ ways.
- (b) The group is of order 6. We just have to show that it is not abelian. Show for the elements $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. $ab = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $ba = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

□

G5: Let G be the group of units of the ring $\mathbb{Z}/247\mathbb{Z}$.

- (a) Determine the order of G (note that $247 = 13 \cdot 19$).

- (b) Determine the structure of G (as in the classification theorem for finitely generated abelian groups).
Hint: Use the Chinese Remainder Theorem.

Solution 5. We will discuss a bit about the group of units. Let $N = 2^k p_1^{k_1} \cdots p_n^{k_n}$ where p_i s are odd primes. By CRT, we have $(\mathbb{Z}_N)^\times = (\mathbb{Z}_{2^k})^\times \times (\mathbb{Z}_{p_1^{k_1}})^\times \times \cdots \times (\mathbb{Z}_{p_n^{k_n}})^\times$. We have the unit group

$$(\mathbb{Z}_N)^\times = (\mathbb{Z}_{2^k})^\times \times (\mathbb{Z}_{p_1^{k_1}})^\times \times \cdots \times (\mathbb{Z}_{p_n^{k_n}})^\times$$

. For odd prime powers, we have that the unit group is cyclic $(\mathbb{Z}_{p^k})^\times = \mathbb{Z}_{p^k - p^{k-1}}$.

For 2^k we have $(\mathbb{Z}_2)^\times = \mathbb{Z}_1$ the trivial group, $(\mathbb{Z}_4)^\times = \mathbb{Z}_2$ cyclic and $(\mathbb{Z}_{2^k})^\times = \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ noncyclic groups for $2^k \geq 8$. So the only time where the unit group is cyclic is $N = 1, 2, 4, p^k, 2p^k$ where p is an odd prime.

So, for $N = 247$ the order of the group is $12 \times 18 = 216$. And the structure of G is $\mathbb{Z}_{12} \times \mathbb{Z}_{18} = \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_2 = \mathbb{Z}_6 \times \mathbb{Z}_{36}$. □

G6: Let G be the group of invertible 2×2 upper triangular matrices with entries in \mathbb{R} . Let $D \subseteq G$ be the subgroup of invertible diagonal matrices and let $U \subseteq G$ be the subgroup of matrices of the form $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ where $x \in \mathbb{R}$ is arbitrary.

- (a) Show that U is a normal subgroup of G and that G/U is isomorphic to D .

- (b) True or False (with justification): $G \cong U \times D$

Solution 6. Let's look at the structure of U . We have $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$. So, U is Abelian.

- (a) Let $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ and $u = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U$. $gug^{-1} = \begin{pmatrix} 1 & \frac{ax}{d} \\ 0 & 1 \end{pmatrix} \in U$. So, $U \trianglelefteq G$.

Let $\phi: G \rightarrow D$ be a map $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \mapsto \begin{pmatrix} a_1 a_2 & 0 \\ 0 & d_1 d_2 \end{pmatrix}$ is a homomorphism with kernel U and image D .

- (b) G is nonabelian but the RHS is Abelian.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

G7: Let G be a group and let Z denote the center of G . □

- (a) Show that Z is a normal subgroup of G .
(b) Show that if G/Z is cyclic, then G must be abelian.
(c) Let D_6 be the dihedral group of order 6. Find the center of D_6 .

Solution 7. Let G be a group with center Z .

- (a) $gzg^{-1} = zgg^{-1} = z \in Z$.

- (b) Let $G/Z = C = \langle a \rangle$.

$$\text{Let } g_1, g_2 \in G. \quad g_i Z = a^{k_i} Z \implies g_i = a^{k_i} z'_i z_i^{-1}. \quad g_1 g_2 = g_2 g_1 = a^{k_1 + k_2} z_1 z_2 z'_1 z'_2.$$

- (c) $D_6 = \{e, r, r^2, s, sr, sr^2\}$, $rs = sr^2 \neq sr, r^2 \cdot rs = s, rs \cdot r^2 = ssr sr^2 = sr^4 = sr$. So, $Z = \{e\}$. □

G8: List all abelian groups of order 8 up to isomorphism. Identify which group on your list is isomorphic to each of the following groups of order 8. Justify your answer.

- (a) $(\mathbb{Z}/15\mathbb{Z})^*$ = the group of units of the ring $\mathbb{Z}/15\mathbb{Z}$.

- (b) The roots of the equation $z^8 - 1 = 0$ in \mathbb{C} .

- (c) \mathbb{F}_8^+ = the additive group of the field \mathbb{F}_8 with eight elements.

Solution 8. We use structure theorem for finitely generated Abelian group. G is isomorphic to one of these three groups. $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(a) $(\mathbb{Z}/15\mathbb{Z})^\times = (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times = \mathbb{Z}_2 \times \mathbb{Z}_4$.

(b) $\mu_8 = e^{\frac{2\pi i}{8}}$ has order 8. So, it's isomorphic to $\mathbb{Z}/8\mathbb{Z}$.

(c) The field is of char 2. So, each element has order 2. So, it's isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. □

G9: Let S_9 denote the symmetric group on 9 elements.

(a) Find an element of S_9 of order 20.

(b) Show that there is no element of S_9 of order 18.

Solution 9. Order of an element is the l.c.m. of the cycle lengths.

(a) (12345)(6789).

(b) We can't partition 9 into parts such that the lcm is 20. □

G10: $G = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} : a, b \in \mathbb{R}, a > 0 \right\}$ and $N = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} : c \in \mathbb{R} \right\}$ are groups under matrix multiplication.

(a) Show that N is a normal subgroup of G and that G/N is isomorphic to the multiplicative group of positive real numbers \mathbb{R}^+ .

(b) Find a group N' with $N \subseteq N' \subseteq G$, with both inclusions proper, or prove that no such N' exists.

G11. Let R be a commutative ring with identity, and let H be a subgroup of the group of units R^* of R . Let $N = \{A \in \text{GL}(n, R) : \det A \in H\}$. Prove that N is a normal subgroup of $\text{GL}(n, R)$ and $\text{GL}(n, R)/N \cong R^*/H$.

G11. Let G be a group of order $2p$ where p is an odd prime. If G has a normal subgroup of order 2, show that G is cyclic.

G12. Prove that every finitely generated subgroup of the additive group of rational numbers is cyclic.

G13. Prove that any finite group of order n is isomorphic to a subgroup of the orthogonal group $O(n, \mathbb{R})$.

G14. Prove that the group $\text{GL}(2, \mathbb{R})$ has cyclic subgroups of all orders $n \in \mathbb{N}$. (Hint: The set of matrices

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ where a and b are arbitrary real numbers, is a subring of the ring of 2×2 matrices which is isomorphic to \mathbb{C} .)

G15. Let H_1 be the subgroup of \mathbb{Z}^2 generated by $\{(1, 3), (1, 7)\}$ and let H_2 be the subgroup of \mathbb{Z}^2 generated by $\{(2, 4), (2, 6)\}$. Are the quotient groups $G_1 = \mathbb{Z}^2/H_1$ and $G_2 = \mathbb{Z}^2/H_2$ isomorphic?

G16. Let H and N be subgroups of a group G with N normal. Prove that $HN = NH$ and that this set is a subgroup of G .

G17. Let $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$ and let $H = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$. Express the abelian group $\text{Hom}(G, H)$ of homomorphisms from G to H as a direct sum of cyclic groups.

G18. Let G be an abelian group generated by x, y, z subject to the relations

$$15x + 3y = 0$$

$$3x + 7y + 4z = 0$$

$$18x + 14y + 8z = 0$$

(a) Write G as a product of two cyclic groups.

(b) Write G as a direct product of cyclic groups of prime power order.

(c) How many elements of G have order 2?

G19. Let \mathbb{F} be a field and let

$$H(\mathbb{F}) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{F} \right\}$$

(a) Verify that $H(\mathbb{F})$ is a nonabelian subgroup of $\text{GL}(3, \mathbb{F})$.

(b) If $|\mathbb{F}| = q$, what is $|H(\mathbb{F})|$?

(c) Find the order of all elements of $H(\mathbb{Z}/2\mathbb{Z})$.

(d) Verify that $H(\mathbb{Z}/2\mathbb{Z}) \cong D_8$, the dihedral group of order 8.

G20. Let R be an integral domain and let G be a finite subgroup of R^* , the group of units of R . Prove that G is cyclic.

G21. Let α and β be conjugate elements of the symmetric group S_n . Suppose that α fixes at least two symbols. Prove that α and β are conjugate via an element γ of the alternating group A_n .

G22. Are $(13)(25)$ and $(12)(45)$ conjugate in S_5 ? If you say "yes", find an element giving the conjugation; if you say "no", prove your answer.

G23. (a) Suppose that G is a group and $a, b \in G$ are elements such that the order of a is m and the order of b is n . If $ab = ba$ and if m and n are relatively prime, show that the order of ab is mn .

(b) Prove that an abelian group of order pq , where p and q are distinct primes, must be cyclic.

(c) If m and n are relatively prime, must a group of order mn be cyclic? Justify your answer.

G24. Let $\varphi : G \rightarrow H$ be a surjective group homomorphism and let N be a normal subgroup of G . Show that $\varphi(N)$ is a normal subgroup of H . What happens if φ is not surjective? Explain your answer.

G25. Let $Q = \{1, -1, i, -i, j, -j, k, -k\}$ be the quaternion group and $N = \{1, -1, i, -i\}$. Show that N is a normal subgroup of Q . Describe the quotient group Q/N .

G26. Let G be a finite abelian group of odd order. If $\varphi : G \rightarrow G$ is defined by $\varphi(a) = a^2$ for all $a \in G$, show that φ is an isomorphism. Generalize this result.

G27. Prove that the direct product of two infinite cyclic groups is not cyclic.

G28. Prove that if a group has exactly one element of order two, then that element is in the center of the group.

G29. Prove that a group of order 30 can have at most 7 subgroups of order 5.

G30. Let $H = \{1, -1, i, -i\}$ be the subgroup of the multiplicative group $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ consisting of the fourth roots of unity. Describe the cosets of H in G , and show that the quotient G/H is isomorphic to G .

G31. (a) Show that the set of all elements of finite order in an abelian group form a subgroup.

(b) Let $G = \mathbb{R}/\mathbb{Z}$. Show that the set of elements of G of finite order is the subgroup \mathbb{Q}/\mathbb{Z} .

G32. Determine all the finite groups which have exactly 3 conjugacy classes.

G33. (a) Find a Sylow 2-subgroup of S_4 and identify its isomorphism type.

(b) How many Sylow 2-subgroups of S_4 are there? Please justify your answer.

G34. (a) Determine the number of Sylow p -subgroups of S_5 for each prime factor p of $|S_5|$. Please prove your assertion.

(b) Identify the isomorphism type of each Sylow p -subgroup of S_5 . Please prove your assertion.

G35. Let $p < q$ be prime numbers such that $p \mid (q - 1)$. Show there exists a unique nonabelian group of order pq up to isomorphism.

G36. (a) Define what it means for a group G to act on a set A .

(b) The group $\text{GL}_2(\mathbb{C})$ acts by left-multiplication on the set of matrices $M_{2,5}(\mathbb{C})$. Describe the orbits. How many are there?

Chapter 2

Ring Theory

R1: Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$.

- (a) Why is R an integral domain?
- (b) What are the units in R ?
- (c) Is the element 2 irreducible in R ?
- (d) If $x, y \in R$, and 2 divides xy , does it follow that 2 divides either x or y ? Justify your answer.

R2. (a) Give an example of an integral domain with exactly 9 elements.

- (b) Is there an integral domain with exactly 10 elements? Justify your answer.

R3. Let

$$F = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

- (a) Prove that F is a field under the usual matrix operations of addition and multiplication.
- (b) Prove that F is isomorphic to the field $\mathbb{Q}(\sqrt{2})$.

R3. Let \mathbb{F} be a field and let $R = \mathbb{F}[X, Y]$ be the ring of polynomials in X and Y with coefficients from \mathbb{F} .

- (a) Show that $M = \langle X + 1, Y - 2 \rangle$ is a maximal ideal of R .
- (b) Show that $P = \langle X + Y + 1 \rangle$ is a prime ideal of R .
- (c) Is P a maximal ideal of R ? Justify your answer.

R4. Let R be an integral domain containing a field k as a subring. Suppose that R is a finite-dimensional vector space over k , with scalar multiplication being the multiplication in R . Prove that R is a field.

R5. Let R be a commutative ring with identity and let I and J be ideals of R .

- (a) Define

$$(I : J) = \{r \in R : rx \in I \text{ for all } x \in J\}$$

Show that $(I : J)$ is an ideal of R containing I .

- (b) Show that if P is a prime ideal of R and $x \notin P$, then $(P : \langle x \rangle) = P$, where $\langle x \rangle$ denotes the principal ideal generated by x .

- (a) Define what is meant by the sum $I + J$ and the product IJ of the ideals I and J .
- (b) If I and J are distinct maximal ideals, show that $I + J = R$ and $I \cap J = IJ$.

R6. Let \mathbb{F}_2 be the field with 2 elements.

- (a) Show that $f(X) = X^3 + X^2 + 1$ and $g(X) = X^3 + X + 1$ are the only irreducible polynomials of degree 3 in $\mathbb{F}_2[X]$.

- (b) Give an explicit field isomorphism

$$\mathbb{F}_2[X]/\langle f(X) \rangle \cong \mathbb{F}_2[X]/\langle g(X) \rangle$$

R7. Show that $\mathbb{Z}[i]/\langle 1 + i \rangle$ is isomorphic to the field \mathbb{F}_2 with 2 elements. As usual, i denotes the complex number $\sqrt{-1}$ and $\langle 1 + i \rangle$ denotes the principal ideal of $\mathbb{Z}[i]$ generated by $1 + i$.

R8. Consider the ring $\mathbb{Z}[X]$ of polynomials in one variable X with coefficients in \mathbb{Z} .

- (a) Find all the units of $\mathbb{Z}[X]$.
- (b) Describe an easy way to recognize the elements of the ideal I of $\mathbb{Z}[X]$ generated by 2 and X .
- (c) Find a prime ideal of $\mathbb{Z}[X]$ that is not maximal.

R9. Determine, with justification, all of the irreducible polynomials of degree 4 over the field \mathbb{F}_2 of two elements.

R10. Let $R = \mathbb{Z}[\sqrt{-10}]$.

- (a) Show that R is not a PID. (Hint: Show that 10 admits two essentially different factorizations into irreducible elements of R .)

- (b) Let $P = \langle 7, 5 + \sqrt{-10} \rangle$. Show that R/P is isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

R11. Suppose that R is an integral domain and X is an indeterminate.

(a) Prove that if R is a field, then the polynomial ring $R[X]$ is a PID (principal ideal domain).

(b) Show, conversely, that if $R[X]$ is a PID, then R is a field.

R12. (a) Prove that every Euclidean domain is a principal ideal domain (PID).

(b) Give an example of a unique factorization domain that is not a PID and justify your answer.

R13. (a) Show that for each natural number $n \in \mathbb{N}$, there is an irreducible polynomial $P_n(X) \in \mathbb{Q}[X]$ of degree n .

(b) Is this true when \mathbb{Q} is replaced by \mathbb{R} ? Explain.

R14. Let R be a commutative ring with identity. If $I \subseteq R$ is an ideal, then the radical of I , denoted \sqrt{I} , is defined by

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some positive integer } n\}$$

(a) Prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(b) If P is a prime ideal of R and $r \in \mathbb{N}$, find $\sqrt{P^r}$ and justify your answer.

(c) Find \sqrt{I} , where I is the ideal $\langle 108 \rangle$ in the ring \mathbb{Z} of integers.

R15. (a) Show that $\mathbb{Z}[i]/\langle 3+i \rangle \cong \mathbb{Z}/10\mathbb{Z}$, where i is the usual complex number $\sqrt{-1}$.

(b) Is $\langle 3+i \rangle$ a maximal ideal of $\mathbb{Z}[i]$? Give a reason for your answer.

R16. Let $R = \mathbb{Z}[X]$. Answer the following questions about the ring R . You may quote an appropriate theorem, provide a counterexample, or give a short proof to justify your answer.

(a) Is R a unique factorization domain?

(b) Is R a principal ideal domain?

(c) Find the group of units of R .

(d) Find a prime ideal of R which is not maximal.

(e) Find a maximal ideal of R .

R17. An element a in a ring R is nilpotent if $a^n = 0$ for some natural number n .

(a) If R is a commutative ring with identity, show that the set of nilpotent elements forms an ideal.

(b) Describe all of the nilpotent elements in the ring $\mathbb{C}[X]/\langle f(X) \rangle$, where

$$f(X) = (X-1)(X^2-1)(X^3-1)$$

(c) Show that part (a) need not be true if R is not commutative. (Hint: Try a matrix ring.)

R18. Let R be a ring, let R^* be the set of units of R , and let $M = R \setminus R^*$. If M is an ideal, prove that M is a maximal ideal and that moreover it is the only maximal ideal of R .

R19. (a) Let R be a PID and let I, J be nonzero ideals of R . Show that $IJ = I \cap J$ if and only if $I + J = R$.

(b) Show that $\mathbb{Z}/900\mathbb{Z}$ is isomorphic to $\mathbb{Z}/100\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ as rings.

(a) Let $I = \langle X^2 + 2, 5 \rangle \subseteq \mathbb{Z}[X]$ and let $J = \langle X^2 + 2, 3 \rangle$. Show that I is a maximal ideal, but J is not a maximal ideal.

R20. Let F be a subfield of a field K and let $f(X), g(X) \in F[X] \setminus \{0\}$. Prove that the greatest common divisor of $f(X)$ and $g(X)$ in $F[X]$ is the same as the greatest common divisor taken in $K[X]$.

R21. Find the greatest common divisor of $X^3 - 6X^2 + X + 4$ and $X^5 - 6X + 1$ in $\mathbb{Q}[X]$.

R22. Define $\varphi : \mathbb{C}[X, Y] \rightarrow \mathbb{C}[T]$ by $\varphi(X) = T^2, \varphi(Y) = T^3$.

(a) Show that $\text{Ker}(\varphi) = \langle Y^2 - X^3 \rangle$.

(b) Find the image of φ .

R23. Prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

R24. Let m, n be two non-zero integers. Prove that the greatest common divisor of m and n in \mathbb{Z} is the same as the greatest common divisor taken in $\mathbb{Z}[i]$. Generalize this to a statement about the greatest common divisor of elements a and b in a Euclidean domain R which is a subring of a Euclidean domain S .

R25. Prove that the center of the matrix ring $M_n(\mathbb{R})$ is the set of scalar matrices, i.e., $C(M_n(\mathbb{R})) = \{aI_n : a \in \mathbb{R}\}$.

R26. Let $R_1 = \mathbb{F}_p[X]/\langle X^2 - 2 \rangle$ and $R_2 = \mathbb{F}_p[X]/\langle X^2 - 3 \rangle$ where \mathbb{F}_p is the field of p elements, p a prime. Determine if R_1 is isomorphic to R_2 in each of the cases $p = 2, p = 5$, and $p = 11$.

R27. (a) Show that the only automorphism of the field \mathbb{R} of real numbers is the identity.

(b) Show that any automorphism of the field \mathbb{C} of complex numbers which fixes \mathbb{R} is either the identity or complex conjugation.

R28. (a) Find all ideals of the ring $\mathbb{Z}/24\mathbb{Z}$.

(b) Find all ideals of the ring $\mathbb{Q}[X]/\langle X^2 + 2X - 2 \rangle$.

R29. Let R be an integral domain. Show that the group of units of the polynomial ring $R[X]$ is equal to the group of units of the ground ring R .

R30. Express the polynomial $X^4 - 2X^2 - 3$ as a product of irreducible polynomials over each of the following fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_5$.

R31. Let $\omega = (1 + \sqrt{-3})/2 \in \mathbb{C}$ and let $R = \{a + b\omega : a, b \in \mathbb{Z}\}$.

(a) Show that R is a subring of \mathbb{C} .

(b) Show that R is a Euclidean domain with respect to the norm function $N(z) = z\bar{z}$, where, as usual, \bar{z}

denotes the complex conjugate of z .

R32. Let I be an ideal of $\mathbb{R}[X]$ generated by an irreducible polynomial of degree 2. Show that $\mathbb{R}[X]/I$ is isomorphic to the field \mathbb{C} .

R33. Show that in the ring M of 2×2 real matrices (with the usual sum and multiplication of matrices), the only 2-sided ideals are $\langle 0 \rangle$ and the whole ring M .

R34. Let R be a commutative ring with identity. Suppose $a \in R$ is a unit and $b \in R$ is nilpotent. Show that $a + b$ is a unit.

R35. (b) Let R and S be commutative rings with identities 1_R and 1_S , respectively, let $f : R \rightarrow S$ be a ring homomorphism such that $f(1_R) = 1_S$. If P is a prime ideal of S show that $f^{-1}(P)$ is a prime ideal of R .

(c) Let f be as in part (b). If M is a maximal ideal of S , is $f^{-1}(M)$ a maximal ideal of R ? Prove that it is or give a counterexample.

R36. (a) Let \mathbb{H} be the ring of quaternions, $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, where $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$, $a, b, c, d \in \mathbb{R}$. Let $q^* = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$ and $\|q\|^2 = qq^* = a^2 + b^2 + c^2 + d^2$. Show that the set \mathbb{H}_1 of quaternions with $\|q\| = 1$ is a group under quaternion multiplication. Hint: show $(q_1 q_2)^* = q_2^* q_1^*$ and use $q^{**} = q, a^* = a$ for $a \in \mathbb{R}$.

(b) Show that the map

$$\mathbb{H} \rightarrow M_2(\mathbb{C}), \quad q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mapsto M(q) := \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix} \quad i = \sqrt{-1},$$

is an \mathbb{R} -algebra homomorphism, and that $\|q\|^2 = \det M(q)$.

R37. Let $\mathbb{H} \rightarrow M_2(\mathbb{C})$ be the ring homomorphism of part (b) of problem R40. Show that this induces an isomorphism

$$\mathbb{H}_1 \cong SU_2 = \{T \in M_2(\mathbb{C}) \mid T^t \bar{T} = I_2, \det T = 1\}$$

R38. Let $\mathbb{H}_1 \rightarrow SU_2$ be the isomorphism of R 41. For each $q \in \mathbb{H}_1$, define a map $\mathbb{R}^3 \rightarrow \mathbb{R}^3$:

$$\mathbf{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto R_q(\mathbf{v}) = \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}$$

by the rule $q(a\mathbf{i} + b\mathbf{j} + c\mathbf{k})q^* = a'\mathbf{i} + b'\mathbf{j} + c'\mathbf{k}$. Show that this makes sense: the quaternion $q(a\mathbf{i} + b\mathbf{j} + c\mathbf{k})q^*$ has only $\mathbf{i}, \mathbf{j}, \mathbf{k}$ components. The map $\mathbf{v} \mapsto R_q(\mathbf{v})$ is clearly an invertible \mathbb{R} -linear map, hence an element of $GL(3, \mathbb{R})$. Now show that it preserves the dot-product of vectors in \mathbb{R}^3 , $(a_1, b_1, c_1) \cdot (a_2, b_2, c_2) = a_1 a_2 + b_1 b_2 + c_1 c_2$, that is

$$R_q(\mathbf{v}_1) \cdot R_q(\mathbf{v}_2) = \mathbf{v}_1 \cdot \mathbf{v}_2.$$

Hint: Let $\text{quat}(a, b, c) = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$, then

$$\mathbf{v}_1 \cdot \mathbf{v}_2 = [\text{quat}(\mathbf{v}_1) \text{quat}(\mathbf{v}_2)^* + \text{quat}(\mathbf{v}_2) \text{quat}(\mathbf{v}_1)^*] / 2.$$

Therefore $R_q \in SO_3(\mathbb{R}) = \{T \in M_3(\mathbb{R}) \mid T^t T = I_3, \det T = 1\}$.

R39. Show that the map $q \mapsto R_q$ is a homomorphism $\mathbb{H}_1 \rightarrow SO(3, \mathbb{R})$, i.e., $R_{q_1 q_2} = R_{q_1} R_{q_2}$. Show that it induces an isomorphism $SU_2 / \pm 1 \cong SO(3, \mathbb{R})$.

Chapter 3

Module Theory

M1: Let $\mathbb{Z}[\frac{1}{2}]$ denote the subring of \mathbb{Q} generated by \mathbb{Z} and $\frac{1}{2}$. Is $\mathbb{Z}[\frac{1}{2}]$ finitely generated as a \mathbb{Z} -module? Justify your answer.

M2: Let $\mathbb{Z}[\frac{1}{2}]$ denote the subring of \mathbb{Q} generated by \mathbb{Z} and $\frac{1}{2}$. Prove or disprove: $\mathbb{Z}[\frac{1}{2}]$ is a free \mathbb{Z} -module.

M3: (a) Show that \mathbb{Q} is a torsion-free \mathbb{Z} -module.

(b) Is \mathbb{Q} a free \mathbb{Z} -module? Justify your answer.

M4: Show that $\mathbb{Z}/3\mathbb{Z}$ is a $\mathbb{Z}/6\mathbb{Z}$ -module and conclude that it is not a free $\mathbb{Z}/6\mathbb{Z}$ -module.

M5: Let N be a submodule of an R -module M . Show that if N and M/N are finitely generated, then M is finitely generated.

M6: Let G be the abelian group with generators x, y , and z subject to the relations

$$5x + 9y + 5z = 0$$

$$2x + 4y + 2z = 0$$

$$x + y - 3z = 0.$$

Determine the elementary divisors of G and write G as a direct sum of cyclic groups.

M7: Let R be a ring and let $f : M \rightarrow N$ be a surjective homomorphism of R -modules, where N is a free R -module. Show that there exists an R -module homomorphism $g : N \rightarrow M$ such that $f \circ g = 1_N$. Show that $M = \text{Ker}(f) \oplus \text{Im}(g)$.

M8: Let R be an integral domain and let M be an R -module. A property P of M is said to be hereditary if, whenever M has property P , then so does every submodule N of M . Which of the following properties of M are hereditary? If a property is hereditary, give a brief reason. If it is not hereditary, give a counterexample.

(a) Free

(b) Torsion

(c) Finitely generated

M9: Let R be an integral domain. Determine if each of the following statements about R -modules is true or false. Give a proof or counterexample, as appropriate.

(a) A submodule of a free module is free.

(b) A submodule of a free module is torsion-free.

(c) A submodule of a cyclic module is cyclic.

(d) A quotient module of a cyclic module is cyclic.

M10: Let M be an R -module and let $f : M \rightarrow M$ be an R -module endomorphism which is idempotent, that is, $f \circ f = f$. Prove that $M \cong \text{Ker}(f) \oplus \text{Im}(f)$.

M11: Prove that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$, where d is the greatest common divisor of n and m .

M12: Compute $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q})$ and $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$.

M13: Let R be a commutative ring with 1 and let I and J be ideals of R . Prove that $R/I \cong R/J$ as R -modules if and only if $I = J$. Suppose we only ask that R/I and R/J be isomorphic as rings. Is the same conclusion valid? (Hint: Consider $F[X]/\langle X - a \rangle$ for $a \in F$.)

M14: Let $M \subseteq \mathbb{Z}^n$ be a \mathbb{Z} -submodule of rank n . Prove that \mathbb{Z}^n/M is a finite group.

M15: Let G, H , and K be finite abelian groups. If $G \times K \cong H \times K$, then prove that $G \cong H$.

M16: Let G be an abelian group and K a subgroup. For each of the following statements, decide if it is true or false. Give a proof or provide a counterexample, as appropriate.

(a) If $G/K \cong \mathbb{Z}^2$, then $G \cong K \oplus \mathbb{Z}^2$.

(b) If $G/K \cong \mathbb{Z}/2\mathbb{Z}$, then $G \cong K \oplus \mathbb{Z}/2\mathbb{Z}$.

M17: Let F be a field and let V and W be vector spaces over F . Make V and W into $F[X]$ -modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all $w \in W$. Denote the resulting $F[X]$ -modules by V_T and W_S respectively.

(a) Show that an $F[X]$ -module homomorphism from V_T to W_S consists of an F -linear transformation $R : V \rightarrow W$ such that $RT = SR$.

(b) Show that $V_T \cong W_S$ as $F[X]$ -modules if and only if there is an F -linear isomorphism $P : V \rightarrow W$ such that $T = P^{-1}SP$.

M18. Let $G = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. Determine the elementary divisors and invariant factors of G .

M19. (a) Find a basis and the invariant factors of the submodule N of \mathbb{Z}^2 generated by $x = (-6, 2)$, $y = (2, -2)$ and $z = (10, 6)$.

(b) From your answer to part (a), what is the structure of \mathbb{Z}^2/N ?

M20. Let R be a ring and let M be a free R module of finite rank. Prove or disprove each of the following statements.

(a) Every set of generators contains a basis.

(b) Every linearly independent set can be extended to a basis.

M21. Let R be a ring. An R -module N is called simple if it is not the zero module and if it has no submodules except N and the zero submodule.

(a) Prove that any simple module N is isomorphic to R/M , where M is a maximal ideal.

(b) Prove Schur's Lemma: Let $\varphi : S \rightarrow S'$ be a homomorphism of simple modules. Then either φ is zero, or it is an isomorphism.

M22. (a) Give an example of a prime ideal in a ring that is not maximal.

(b) Describe $\text{Spec}(\mathbb{C}[x])$ (polynomial ring in one variable over the complex numbers).

(c) Describe $\text{Spec}(\mathbb{R}[x])$.

Chapter 4

Linear Algebra

L1: Let V be a vector space of dimension 3 over \mathbb{C} . Let $\{v_1, v_2, v_3\}$ be a basis for V and let $T : V \rightarrow V$ be the linear transformation defined by $T(v_1) = 0$, $T(v_2) = -v_1$, and $T(v_3) = 5v_1 + v_2$.

(a) Show that T is nilpotent.

(b) Find the Jordan canonical form of T .

(c) Find a basis of V such that the matrix of T with respect to this basis is the Jordan canonical form of T .

L2. Let p be a prime number and let V be a 2-dimensional vector space over the field \mathbb{F}_p with p elements.

(a) Find the number of linear transformations $T : V \rightarrow V$.

(b) Find the number of invertible linear transformations $T : V \rightarrow V$.

L3. Let $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ be a linear transformation, with minimal polynomial $m_T(X)$ in $\mathbb{R}[X]$. Assume that $m_T(X)$ factors in $\mathbb{R}[X]$ as $f(X)g(X)$ with $f(X)$ and $g(X)$ relatively prime. Show that \mathbb{R}^n can be written as a direct sum $\mathbb{R}^n = U \oplus V$, where U and V are T -invariant subspaces with $T|_U$ having minimal polynomial $f(X)$ and $T|_V$ having minimal polynomial $g(X)$.

L4. Let $T : \mathbb{C}^n \rightarrow \mathbb{C}^n$ be a nilpotent linear transformation.

(a) How is $\dim \text{Ker } T$ related to the Jordan normal form of T ? How is the minimal polynomial related to the Jordan normal form?

(b) Let $T, S : \mathbb{C}^6 \rightarrow \mathbb{C}^6$ be nilpotent linear transformations such that S and T have the same minimal polynomial and $\dim \text{Ker } T = \dim \text{Ker } S$. Show that S and T have the same Jordan form.

(c) Show that there are nilpotent linear transformations $T, S : \mathbb{C}^8 \rightarrow \mathbb{C}^8$ such that S and T have the same minimal polynomial and $\dim \text{Ker } T = \dim \text{Ker } S$, but S and T have different Jordan forms. That is, part (b) is false if 6 is replaced by 8.

L5. Let \mathbb{F} be a field and let

$$0 \longrightarrow V_1 \xrightarrow{T_1} V_2 \xrightarrow{T_2} \cdots \xrightarrow{T_n} V_{n+1} \longrightarrow 0$$

be an exact sequence of finite-dimensional vector spaces and linear transformations over \mathbb{F} . This means that T_1 is injective, T_n is surjective, and $\text{Im}(T_i) = \text{Ker}(T_{i+1})$ for $1 \leq i \leq n-1$. Show that

$$\sum_{i=1}^{n-1} (-1)^{i+1} \dim V_i = 0$$

L6. Let S and T be linear transformations between finite-dimensional vector spaces V and W over the field \mathbb{F} . Show that $\text{Ker } S = \text{Ker } T$ if and only if there is an invertible operator U on W such that $S = UT$.

L7. Let V be a finite-dimensional real vector space and let $T : V \rightarrow V$ be a nilpotent transformation (i.e. $T^j = 0$ for some positive integer j).

(a) Find the eigenvalues of T .

(b) Is $I - T$ invertible, where $I : V \rightarrow V$ is the identity transformation? Explain fully.

(c) Give an example of two non-similar linear transformations A and B on the same finite dimensional vector space V , having identical characteristic polynomials and identical minimal polynomials.

L8. Let V be the vector space of polynomials $p(X) \in \mathbb{C}[X]$ of degree ≤ 4 . Define a linear transformation $T : V \rightarrow V$ by $T(p(X)) = p''(X)$ (the second derivative of the polynomial $p(X)$). Compute the characteristic polynomial, minimal polynomial, and Jordan canonical form of the linear transformation T .

L9. Let p be a prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field with p elements, $V = \mathbb{F}_p^4$ (a 4-dimensional vector space over \mathbb{F}_p), and W the subspace of V spanned by the three vectors $\mathbf{a}_1 = (1, 2, 2, 1)$, $\mathbf{a}_2 = (0, 2, 0, 1)$, and $\mathbf{a}_3 = (-2, 0, -4, 3)$. Find $\dim_{\mathbb{F}_p} W$. (Note that this dimension depends on p .)

