LSU Algebra Question Bank Solution

Ayanava Mandal

April 2025

Contents

Chapter 1

Group Theory

1.1 Brief Discussion on Group of Units modulo N

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_is are odd primes. By CRT, we have $(\mathbb{Z}_N) = (\mathbb{Z}_{2^k}) \times (\mathbb{Z}_{p_1^{k_1}}) \times \cdots \times (\mathbb{Z}_{p_n^{k_n}})$. 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.

1.2 Solution

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

(b) Let $H =< h >$ be cyclic. Let $K =< k >$ 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.

$\square$

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

Solution 1.2. *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. $\square$

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 1.3. *(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 $p^3 q^4 = P(3)P(4) = 3 \times 5 = 15$.

$\square$

G4: *Let $G = \mathrm{GL}(2, \mathbb{F}_p)$ 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 $\left(p^2 - 1\right)\left(p^2 - p\right)$.

(b) *Show that for $p = 2$ the group G is isomorphic to the symmetric group S_3.*

Solution 1.4. *Let $G = \mathrm{GL}(2, \mathbb{F}_p)$.*

(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 $\mid \mathbb{F}_p^2 \mid -1 = p^2 - 1$ 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 $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. $ab = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, ba = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.*

$\square$

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 1.5. *See Section 1.1.*

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

$\square$

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

$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix} \mapsto \begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{pmatrix}$ *is a homomorphism with kernel U and image D.*

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

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

$\square$

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 abellan.*

(c) *Let D_6 be the dihedral group of order 6 . Find the center of D_6.*

Solution 1.7. *Let G be a group with center Z.*

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

(b) *Let $G/Z = C =< a >$.*
Let $g_1, g_2 \in G$. $g_iZ = a^{k_i}Z \implies g_i = a^{k_i} z_i' z_i^{-1}$. $g_1g_2 = g_2g_1 = a^{k_1+k_2} z_1z_2z_1'z_2'$.

(c) $D_6 = \{e, r, r^2, s, sr, sr^2\}$, $rs = sr^2 \neq sr$,$r^2 \cdot rs = s$, $rs \cdot r^2 = ssrsr^2 = sr^4 = sr$. *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) $(Z/15Z)^* =$ *the group of units of the ring* $Z/15Z$.

(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 1.8. *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 1.9. *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.*

Solution 1.10. (a) *Let* $\phi : G \to \mathbb{R}^+$ *be the homomorphism* $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto a$*(like solution 1.6) with kernel* N *and image* $\mathbb{R}^+$*. So,* $G/N \cong \mathbb{R}^+$.

(b) *Let* $< \frac{1}{2} >= \{\frac{1}{2^k} : k \in \mathbb{Z}\}$ *be a subgroup of* $\mathbb{R}^+$*. The corresponding subgroup of* G *containing* N *is* $N' = \{ \begin{pmatrix} \frac{1}{2^k} & c \\ 0 & 2^k \end{pmatrix} : k \in \mathbb{Z}, c \in \mathbb{R}\}$

□

G11.1: *Let* R *be a commutative ring with identity, and let* H *be a subgroup of the group of units* R^* *of* R*. Let* $N = \{A \in \mathrm{GL}(n, R) : \det A \in H\}$*. Prove that* N *is a normal subgroup of* $\mathrm{GL}(n, R)$ *and* $\mathrm{GL}(n, R)/N \cong R^*/H$.
G11.2: *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.*

Solution 1.11. 1. *Consider the homomorphism* $\phi : GL(n, R) \to R^*/H$ *by the map* $A \mapsto det(A) \pmod H$ *(Since* R *is commutative* H *is normal in* R^**).* $Ker(\phi) = N$ *normal with full image(diagonal with a entry* r *and rest* 1*). So, we have the isomorphism.*

2. *If* G *is abelian.* G *has element of order* p *and* 2*(Cauchy). Product of them has order* $lcm(2, p) = 2p$*. So, it generates* G.
Let $N = \{e, n\}$ *where* $n^2 = e$. $gng^{-1} = n$*(*$gng^{-1} = e \implies n = e$*) i.e.* $n \in Z(G)$*. So,* $G/Z(G)$ *is either* $\mathbb{Z}_p$ *or* $\mathbb{Z}_1$ *cyclic. So,* G *is Abelian.*

□

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

Solution 1.12. *Let* $G =< \frac{a}{b}, \frac{c}{d} >$. *Claim :* $G =< \frac{gcd(ad,bc)}{bd} >$. $\frac{a}{b} = \frac{ad}{gcd(ad,bc)} \frac{gcd(ad,bc)}{bd}$ *and* $\frac{c}{d} = \frac{bc}{gcd(ad,bc)} \frac{gcd(ad,bc)}{bd}$. *On the other hand, by Bezout's identity* $u\frac{a}{b} + v\frac{c}{d} = \frac{gcd(ad,bc)}{bd}$. *Now, use induction.*

$\square$

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

Solution 1.13. *(from stackexchange)*
S_n *acts on* $\mathbb{R}^n$ *by the equation*

$$\sigma.e_i = e_{\sigma(i)},$$

where $\{e_i | i = 1, 2, ..., n\}$ *is the standard basis of* $\mathbb{R}^n$ *and* $\sigma \in S_n$. *Therefore we have a group morphism*

$$\varphi : S_n \to GL_n(\mathbb{R})$$

defined by $\varphi(\sigma)(e_i) = e_{\sigma(i)}$. *It is easy to check that* φ *is one-one. Note that* $\varphi(S_n) \subset \mathbb{O}(n)$, *for* $\langle \varphi(\sigma)(e_i), \varphi(\sigma)(e_j) \rangle = \langle e_i, e_j \rangle$.
Now any finite group is a subgroup of S_n. $\square$

G14: *Prove that the group* $\mathrm{GL}(2,\mathbb{R})$ *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* $\mathbb{C}$.*)*

Solution 1.14. *Use the hint. We have a cyclic subgroup of order* n *generated by the* n*-th root of unity* μ_n *in* $\mathbb{C}$. *Take it's image in* $GL(2,\mathbb{R})$.

$\square$

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?*

Solution 1.15. $H_1 =< (1,3),(1,7) >=< (1,3),(0,4) >=< (1,-1),(0,4) >$. $\mathbb{Z}^2/H_1 = \mathbb{Z}_4$ *with the generator* $(0,1) + H_1$ *of order* 4 *(easy to show order divides* 4*, but order isn't* 2*).*
$H_2 =< (2,0),(0,2) > \mathbb{Z}^2/H_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$. *Not isomorphic by comparing the order.* $\square$

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.

Solution 1.16. *The first proof is trivial by definition of normal subgroup:* $hN = Nh$.
$n_1h_1n_2h_2 = n_1n_2'h_1'h_2 = n_3h_3 \in NH$.
$(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$. $\square$

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 Hom* (G, H) *of homomorphisms from* G *to* H *as a direct sum of cyclic groups.*

Solution 1.17. *We use the fact*

$$Hom(\mathbb{Z}_n, \mathbb{Z}_m) = \{\texttt{element of } \mathbb{Z}_m \texttt{ with order dividing } n\} = \mathbb{Z}_(gcd(n,m))$$

$$Hom(G,H) = Hom(\mathbb{Z}_2, H) \oplus Hom(\mathbb{Z}_6, H) \oplus Hom(\mathbb{Z}_{30}, H) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10}.$$

$\square$

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?*

Solution 1.18. *We need to calculate the Smith Normal form of the matrix(row/column swap, $R_i \to R_i + kR_j$, $C_i \to C_i + kC_j$, multiply by -1)* $\begin{pmatrix} 15 & 3 & 0 \\ 3 & 7 & 4 \\ 18 & 14 & 8 \end{pmatrix}$.

$$\begin{pmatrix} 15 & 3 & 0 \\ 3 & 7 & 4 \\ 12 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 3 & 0 \\ 3 & 7 & 4 \\ 12 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 3 & 0 \\ 0 & 4 & 4 \\ 12 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 4 \\ 12 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 4 \\ 0 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 4 & 4 \\ 0 & 4 & 4 \\ 0 & -12 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 1 & 1 \\ 0 & 4 & 4 \\ 0 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 3 \\ 4 & 4 & 0 \\ 0 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 4 & 0 & -12 \\ 0 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -12 \\ 0 & -12 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

(a) *So,* $G = \mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$.

(b) $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4$

(c) *3 order 2 element:* $(6,0), (0,6), (6,6) \in C_{12} \times C_{12}$

□

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* $\mathrm{GL}(3, \mathbb{F})$.

(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 .*

Solution 1.19. (a) $\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & b_1 + b_2 + a_1 c_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{pmatrix}$.

Inverse of $\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix}$ *is* $\begin{pmatrix} 1 & -a_1 & a_1 c_1 - b_1 \\ 0 & 1 & -c_1 \\ 0 & 0 & 1 \end{pmatrix}$. *Non Abelian for the (1,3)th entry.*

(b) *We have* q *choices for each of* a, b *and* c. *So* q^3.

(c,d) $e = I_3, r = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, s = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

□

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.*

Solution 1.20. *Note that this result is true for Fields. Any subgroup of units of integral domain is a subgroup of it's quotient field's units. Thus the result follows. In general it follows from the roots of the polynomial* $x^n - 1$ *in Field or integral domain(at most* n *many roots).* □

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.

Solution 1.21. α, β *has same cycle types. Let* α *fix* i, j. *And* τ *be the conjugating element such that* $\tau\alpha\tau^{-1} = \beta$. *Then* $\tau(i), \tau(j)$ *is fixed by* β. *Let us assume,* τ *is not in* A_n. *Then* $\tau(i,j) \in A_n$ *and gives the same conjugation.* □

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.*

Solution 1.22. *They have the same cycle type. So, they are conjugate by the element* $(32)(24)$. □

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.*

Solution 1.23. *(a)* $(ab)^{mn} = a^{mn}b^{mn} = e$. *So,* $o(ab) \mid mn$.
$e = (ab)^{o(a,b)n} = a^{o(a,b)n}b^{o(a,b),n} = a^{o(a,b)n} \implies m \mid o(a,b)n \implies m \mid o(a,b)$.
Similarly, $n \mid (o(a,b)) \implies mn = o(a,b)$.

(b) *By the previous proof, if a is of order p and b is of order q(by Cauchy), ab is of order pq and it generates the group.*

(c) *No. Example* S_3.

$\square$

G24: *Let* $\varphi : G \to H$ *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.*

Solution 1.24. *Let* $h \in H, n' \in \varphi(N)$.
Surjective implies $h = \varphi(g), n' = \varphi(n) \implies hn'h^{-1} = \varphi(gng^{-1}) = \varphi(n_1) \in \varphi(N)$ *where* $n_1 \in N$.
Let $\phi : \mathbb{Z}_2 \to S_3$ *where* $a \mapsto (12)$. $\phi(Z_2) = \{e, (12)\}$ *is not normal in* S_3. $\square$

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.

Solution 1.25. *N is of index 2 implies normal(We can show explicitely too).* Q/N *is of order* 2 *i.e. is isomorphic to* $\mathbb{Z}_2$. $\square$

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

Solution 1.26. $\varphi(ab) = abab = aabb = \varphi(a)\varphi(b)$ *proves homomorphism.*
$\varphi(x) = x^2 = e \implies o(x) \mid 2$ *and* $o(x) \mid o(G) \implies o(x) \mid gcd(2, o(G)) = 1 \implies x = e$ *proves isomorphism.*
We can generalize this result to the power m and order of group n where $(m, n) = 1$. $\square$

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

Solution 1.27. *Let* $G =< a >, H =< b >$ *be two infinite cyclic group. Assume* (a^m, b^n) *generated* $G \times H$. $(a^m, b^n)^{k_1} = (a, e)$, $(a^m, b^n)^{k_2} = (e, b)$ *implies* $m, n = \pm 1$ *but that gives rise to a contradiction.* $\square$

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

Solution 1.28. *Let* $x \in G$ *be the only element of order* 2. *Let* $a \in G$ *be arbitary,* $axa^{-1} = g$. $g^2 = ax^2a^{-1} = e$ *i.e.* $g = e$ *or* $g = x$. *The first case gives a contradiction, the second gives* $x \in Z(G)$. $\square$

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

Solution 1.29. *Let* H_1, H_2 *be two different subgroup of order 5.* $H_1 \cap H_2 = \{e\}$ *since nontrivial intersection implies equal subgroups, so, their nonidentity elements must be different. i.e.* $1+4{\cdot}k$ *must be less than or equal to* 30, *where k is the no. of different subgroup. This implies* $k \le 7$.*(Syllow implies* $n_5 = 1, 6$*)* $\square$

G30: *Let* $H = \{1, -1, i, -i\}$ *be the subgroup of the multiplicative group* $G = \mathbb{C}^* = \mathbb{C}\backslash\{0\}$ *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.

Solution 1.30. $\square$

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* $\mathbb{Q}/\mathbb{Z}$.

Solution 1.31. *G is Abelian.*

(a) *Let* $H \le G$ *be the set containing finite order elements. Let* $h_1, h^2 \in H$. $(h_1h_2)^{o(h_1)o(h_2)} = h_1^{o(h_1)o(h_2)}h_2^{o(h_1)o(h_2)} = e$ *i.e.* $h_1h_2 \in H$. *Inverse has the same order.*

(b) *Let* $H \le G$ *be the desired subgroup.* $\dfrac{p}{q} + \mathbb{Z}$ *has order q. i.e.* $\mathbb{Q}/\mathbb{Z} \subseteq H$.

Let $r+\mathbb{Z}$ *be of finite order implies* $nr+\mathbb{Z} = \mathbb{Z}$ *implies* $nr \in \mathbb{Z}$ *implies* $nr = p \in \mathbb{Z}$ *implies* $r = \dfrac{p}{n} \in \mathbb{Q}$.

□

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

Solution 1.32. *Let n, m be the number of elements in the other 2 conjugacy classes. So, $\mid G \mid = 1+n+m$ with $n \mid o(G)$ and $m \mid o(G)$ implies $n \mid 1+m$, $m \mid 1+n$. Ultimately, we get 2 cases: $(n,m) = (1,1)$ and $(2,3)$. i.e. $\mathbb{Z}_3$ and S_3.* □

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.*

Solution 1.33. □

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.*

Solution 1.34. □

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.*

Solution 1.35. □

G36:

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

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

Solution 1.36. □

Problems Left: 30, 33, 34, 35, 36

Chapter 2

Ring Theory

2.1 Brief Discussion on Bezout Domain, PID, UFD, gcd, lcm

The concept of gcd and lcm can be generalized to UFDs. We use the definition $gcd(a,b) = d$ iff d divides a, b and $x \mid a,\ x \mid b \implies x \mid d$. Similarly, a, b divides the lcm and $a \mid x,\ b \mid x$ implies $lcm(a,b) \mid x$. We can show that $ab = gcd(a,b)lcm(a,b)$.

Theorem 2.1.1. *$ab = gcd(a,b)lcm(a,b)$ in UFD.*

Proof. Let $gcd(a,b) = d$. $a = da', b = db'$. We have some results from the definition of gcd.
$gcd(a', b') = 1$ since $u \mid a', b' \implies a' = ux_1, b' = ux_2 \implies a = dux_1, b = dux_2 \implies du \mid a, b \implies du \mid d \implies u$ is unit.
So, enough to prove $lcm(a,b) = da'b'$. Since both a, b divides $da'b'$ and $a, b \mid x \implies x = da'k_1 = db'k_2$
By uniqueness of factors $a'k_1 = b'k_2$. $gcd(a', b') = 1 \implies b' \mid k_1$ by irreducible factor decomposition argument. So, $x = da'b'k$ i.e. $da'b'$ divides x. So, $ab = d^2a'b' = gcd \cdot lcm$ □

Definition 1. *A integral domain is called Bezout domain if sum of any two principal ideals is principal. i.e. $(a,b) = (d)$ for any $a, b \in R$. The Bezout's identity holds for this case: $d = ua + vb$ for some $u, v \in R$. In general any finitely generated ideal is principal.*

A Bezout domain need not be Noetherian or UFD. For example ring of Algebraic integers is not UFD(any element is not irreducible since it's square root is also algebraic integer). Any PID is by definition Bezout domain. If R is a Bezout domain then TFAE:

- *R is PID*
- *R is Noetherian*
- *R is UFD*

So, a Bezout UFD is a PID. Example of non-Bezout UFD is $\mathbb{Z}[x]$. Consider $(2, x)$.
Now we will discuss a little bit about properties that hold in a PID(not necessarily in UFD):

Theorem 2.1.2. *R is a PID. $(a) + (b) = (a,b) = (gcd(a,b))$ and $(a) \cap (b) = (lcm(a,b))$.*

Proof. One side inclusion is true for general UFDs.
Since $gcd(a,b) \mid a, b,\ a, b \in (gcd(a,b)) \implies (a,b) \subseteq (gcd(a,b))$.
On the other hand, let $(a,b) = (d)$ by definition of PID. $a, b \in (d) \implies d \mid a\ ,\ d \mid b$. So, by definition of gcd, $d \mid gcd(a,b) \implies (gcd(a,b)) \subseteq (d)$. This side is not true for UFD in general. Take $gcd(2, x) = 1$ in $\mathbb{Z}[x]$.
This also gives rise to the famous Bezout's identity $gcd(a,b) = ax + by$ for some $x, y \in R$.
$a, b \mid lcm(a,b) \implies lcm(a,b) \subseteq (a), (b)$. And $(a) \cap (b) = (m) \implies a, b \mid m \implies lcm(a,b) \mid m \implies (m) \subseteq (lcm(a,b))$. The second step uses the property of PID. □

2.2 Solution

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.*

Solution 2.1. *Let* $R = \mathbb{Z}[\sqrt{-3}]$

(a) *Let* $(a + b\sqrt{-3})(c + d\sqrt{-3}) = 0 \implies ac - 3bd + \sqrt{-3}(ad + bc) = 0 \implies \dfrac{a}{d} = \dfrac{3b}{c} = 3k$
This implies $3kd^2 + kc^2 = 0 \implies k = 0$ *or* $c = d = 0$. $k = 0 \implies a = b = 0$*, So, one of the factor is* 0.

(b) *Let* $(a+b\sqrt{-3})(c+d\sqrt{-3}) = 1 \implies (a-b\sqrt{-3})(c-d\sqrt{-3}) = 1 \implies (a^2+3b^2)(c^2+3d^2) = 1 \implies b = d = 0, a = c = \pm 1$*. So, the only units are* ± 1.

(c) $\alpha\beta = 2 \implies \bar{\alpha}\bar{\beta} = 2 \implies 4 =\mid \alpha \mid^2\mid \beta \mid^2$*. This gives us that one of them is a unit.*

(d) $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4$*. But 2 doesn't divide the elements individually.*

□

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.*

Solution 2.2. *Finite integral domains are fields. Finite fields are of prime powers.*

(a) $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$.

(b) *Not possible.*

□

R3.1: *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* $\mathbb{Q}(\sqrt{2})$.

R3.2: *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.*

Solution 2.3. *We only need to verify multiplication and inverse.*

1.a

$$\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + b_1a_2 \\ 2a_1b_2 + 2b_1a_2 & 2b_1b_2 + a_1a_2 \end{pmatrix} \in F$$

.

Let $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \implies a^2 - 2b^2 \neq 0.$

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}^{-1} = \frac{1}{a^2 - 2b^2} \begin{pmatrix} a & -b \\ -2b & a \end{pmatrix} \in F$$

1.b

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mapsto a + b\sqrt{2}$$

Check the multiplication.

2.a *Let $\varphi : R \to \mathbb{F}$ given by $\varphi(x) = -1, \varphi(y) = 2$. We show that kernel is M and image is full(clearly), FIT implies that $R/M \cong \mathbb{F} \implies M$ is maximal.*
$< x+1, y-2 >\subseteq ker(\varphi)$. Let $\varphi(f(x,y)) = 0$. $f(x,y) = h(y) + (x-1)g(x,y)$.
$f(-1,2) = 0 \implies h(2) = 0 \implies (y-2) \mid h(y)$. This proves that the kernel is $< x+1, y-2 >$.
Alternatively:

$$\frac{\mathbb{F}[x,y]}{(x+1,y-2)} \cong \frac{\mathbb{F}[x][y]/(y-2)}{(x+1,y-2)/(y-2)} \cong \frac{\mathbb{F}[x]}{(x-1)} \cong \mathbb{F}$$

2.b *$R/P \cong \mathbb{F}[x]$ integral domain implies P is prime.*
($\phi : R \to \mathbb{F}[x]$ with $x \mapsto x, y \mapsto -(x+1)$. $\phi(f(x,y)) = 0 \implies F(y)$ as a polynomial of y has a root at $(-x-1) \implies (y+x+1) \mid f$, this shows the kernel is equal to P).

2.c *From the previous solution we can already see R/P is not a field. Alternatively, $P \subsetneq (x+1, y)$.*

□

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.*

R4. R - i.d. $k \subseteq R$, k field.

R is a finite dim^n vector space over k

To prove: R is a Fd.

Let $\dim^n_k R = n$

Let $r \neq 0, r \in R$.

$1, r, r^2, \dots, r^n$ are linearly dependent..

$a_0 + \dots + a_n r^n = 0$ with some $a_i \neq 0$

$a_0 = 0 \Rightarrow r(\dots) = 0 \Rightarrow r = 0$ since $(\dots) \neq 0 \Rightarrow \Leftarrow$

$\Rightarrow a_0 \neq 0$, $a_0 = r(\dots) \Rightarrow 1 = r\,\underbrace{(a_0^{-1})(\dots)}$ $\Rightarrow r$ unit.

Alternative Proof: let $r \neq 0, r \in R$.

Let $\varphi : R \to R$, $\varphi(x) = rx$ $\quad \ker\varphi = \{x : rx = 0\} = \{0\}$

$\left.\begin{array}{l}\varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(kx) = rkx = k\varphi(x)\end{array}\right\} \Rightarrow \varphi$ linear map $R \to R$

$\ker\varphi = \{0\}$ Rank nullity $\Rightarrow \text{rank}(\varphi) + \text{nullity}(\varphi) = \dim^n R$

$\Rightarrow \dim^n_k \text{Im}\,\varphi = \dim^n_k R \Rightarrow \text{Im}\,\varphi = R$

$\Rightarrow \varphi$ is surjective $\Rightarrow \exists\, a \in R$ s.t. $\varphi(a) = 1 \Rightarrow ra = 1$ unit.

Solution 2.4.

□

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.

(c) Define what is meant by the sum $I + J$ and the product IJ of the ideals I and J.

(d) If I and J are distinct maximal ideals, show that $I + J = R$ and $I \cap J = IJ$.

R5. R comm. with identity. $I, J \trianglelefteq R$.

$(I:J) = \{r \in R : rx \in I \ \forall x \in J\}$

(a) $a, b \in (I:J) \Rightarrow ax, bx \in I \ \forall x \in J$

$\Rightarrow (a+b)x \in I \ \forall x \in J \Rightarrow (a+b) \in (I:J)$

$r \in R$, $ax \in I \ \forall x \in J \Rightarrow rax \in I \ \forall x \in J \Rightarrow ra \in (I:J)$

$i \in I \Rightarrow ix \in I \ \forall x \in J \Rightarrow i \in (I:J) \Rightarrow I \trianglelefteq (I:J)$

(b) P is prime, $x \notin P$. To prove $(P:\langle x \rangle) = P$

$P \subseteq (P:\langle x \rangle)$ ✓

Let $y \in (P:\langle x \rangle) \Rightarrow yr \in P \ \forall r \in \langle x \rangle$

$\Rightarrow yx \in P$ but $x \notin P \Rightarrow y \in P \Rightarrow (P:\langle x \rangle) \subseteq P$

(c) $I+J = \{a+b : a \in I, b \in J\}$

$IJ = \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J\}$

(d) $I \neq J$ maximal.

$\Rightarrow I \subsetneq I+J \subseteq R \Rightarrow I+J = R$

To Prove: $I \cap J = IJ$

• $IJ \subseteq I \cap J$ always.

• $I \cap J = (I \cap J)(I+J) = (I \cap J)I + (I \cap J)J \subseteq IJ + IJ \subseteq IJ$

Alternately: let $x \in I \cap J$, $1 = a+b$ where $a \in I, b \in J$.

$x = xa + xb$, $xa \in IJ$, $xb \in IJ \Rightarrow x \in IJ$

Solution 2.5.

$\square$

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

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

R6: $\mathbb{F}_2[x]$.

ⓐ Irreducible poly of deg 3. Let $p(x)$ be a poly of deg 3. only factorization is of deg 1 + deg 2
$\Rightarrow$ $p(x)$ is reducible $\Leftrightarrow$ $\exists$ root in $\mathbb{F}_2$ of $f(x)$

$$\left.\begin{array}{lll} f(x) = x^3+x^2+1 & f(0)=1 & f(1)=1 \\ g(x) = x^3+x+1 & g(0)=1 & g(1)=1 \end{array}\right\} \Rightarrow f, g \text{ are irreducible.}$$

Let $x^3+ax^2+bx+c = p(x)$, $p(x)$ irr $\Rightarrow$ $p(0), p(1) \neq 0$ ie $p(0) = p(1) = 1$

$p(0) \neq 0 \Rightarrow c = 1$ $\quad p(1) = 1 \Rightarrow a+b = 1 \Rightarrow$ either $a=1$ $b=0$ $\to f(x)$
or $a=0$ $b=1$ $\to g(x)$

(b) $$\frac{\mathbb{F}_2[x]}{\langle f(x)\rangle} \longrightarrow \frac{\mathbb{F}_2[x]}{\langle g(x)\rangle}$$

Enough to Form a ring isomorphism $\mathbb{F}_2[x] \longrightarrow \mathbb{F}_2[x]$
s.t $f(x) \to g(x)$

Claim:
$$\begin{tikzcd} \mathbb{F}_2[x] \arrow[r] \arrow[rr, bend left] & \mathbb{F}_2[x] \arrow[r] & \dfrac{\mathbb{F}_2[x]}{\langle g(x)\rangle} \end{tikzcd}$$ has kernel $\langle f(x)\rangle$

$$f(x) \longrightarrow g(x) \longrightarrow 0$$

Factors through
$$\begin{tikzcd} \mathbb{F}_2[x] \arrow[r, "f \,\to\, g"] \arrow[d] & \mathbb{F}_2[x] \arrow[d] \\ \dfrac{\mathbb{F}_2[x]}{\langle f(x)\rangle} \arrow[r] & \dfrac{\mathbb{F}_2[x]}{\langle g(x)\rangle} \end{tikzcd}$$

$f(x) = x^3+x^2+1$

$$\begin{aligned} f(x+1) &= (x+1)^3 + (x+1)^2 + 1 \\ &= x^3+1+x(\cancel{x}+1) + \cancel{x^2}+\cancel{1}+\cancel{1} \\ &= x^3+x+1 \end{aligned}$$

So the morphism is $x + \langle f(x)\rangle \longrightarrow x+1 + \langle f(x)\rangle$

Solution 2.6. □

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.

Solution 2.7. □

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.*

Solution 2.8. *Remember the Eisenstein Criterion and Gauss Lemma. Let $p(x) = a_n x^n + \cdots + a_0$ be such that a prime p divides $a_0, \cdots, a_{n-1}, p \nmid a_n, p^2 \nmid a_0$ then the polynomial is irreducible over $\mathbb{Z}$ or $\mathbb{Q}$.*

(a) *Let $P_n(X) = X^n + 2$*

(b) *This is not true for $\mathbb{R}$. The maximum degree of irreducible polynomial over $\mathbb{R}$ is 2. E.g. $x^2 + 1$.*

$\square$

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

$$f(X) = (X-1)\left(X^2-1\right)\left(X^3-1\right)$$

(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 $M = R \backslash R^*$. 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 $I = \left\langle X^2+2, 5 \right\rangle \subseteq \mathbb{Z}[X]$ and let $J = \left\langle X^2+2, 3 \right\rangle$. 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 $f(X), g(X) \in F[X] \backslash \{0\}$. 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 $\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[T]$ by $\varphi(X) = T^2, \varphi(Y) = T^3$.
(a) Show that $\operatorname{Ker}(\varphi) = \left\langle Y^2 - X^3 \right\rangle$.
(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., $C\left(M_n(\mathbb{R})\right) = \{aI_n : a \in \mathbb{R}\}$.
R26. Let $R_1 = \mathbb{F}_p[X]/\left\langle X^2-2 \right\rangle$ and $R_2 = \mathbb{F}_p[X]/\left\langle X^2-3 \right\rangle$ 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 $\mathbb{Q}[X]/\left\langle X^2+2X-2 \right\rangle$.
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 $f: R\to S$ 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 $(q_1q_2)^*=q_2^*q_1^*$ and use $q^{**}=q, a^*=a$ for $a\in\mathbb{R}$.
(b) Show that the map

$$\mathbb{H}\to M_2(\mathbb{C}),\quad q=a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}\mapsto M(q):=\left[\begin{array}{cc} a+bi & c+di\\ -c+di & a-bi\end{array}\right]\quad i=\sqrt{-1},$$

is an $\mathbb{R}$-algebra homomorphism, and that $\|q\|^2=\det M(q)$.
R37. Let $\mathbb{H}\to M_2(\mathbb{C})$ be the ring homomorphism of part (b) of problem R40. Show that this induces an isomorphism

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

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

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

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 $\mathbb{R}^3,(a_1,b_1,c_1)\cdot(a_2,b_2,c_2)=a_1a_2+b_1b_2+c_1c_2$, that is*

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

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

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

Therefore $R_q\in SO_3(\mathbb{R})=\{T\in M_3(\mathbb{R})\mid T^tT=I_3,\det T=1\}$.
R39. Show that the map $q\mapsto R_q$ is a homomorphism $\mathbb{H}_1\to SO(3,\mathbb{R})$, i.e., $R_{q_1q_2}=R_{q_1}R_{q_2}$. Show that it induces an isomorphism $SU_2/\pm 1\cong SO(3,\mathbb{R})$.

Chapter 3

Module Theory

M1:_Let_ $\mathbb{Z}\left[\frac{1}{2}\right]$ _denote the subring of_ $\mathbb{Q}$ _generated by_ $\mathbb{Z}$ _and_ $\frac{1}{2}$_. Is_ $\mathbb{Z}\left[\frac{1}{2}\right]$ _finitely generated as a_ $\mathbb{Z}$_-module? Justify your answer._

M2. Let $\mathbb{Z}\left[\frac{1}{2}\right]$ _denote the subring of_ $\mathbb{Q}$ _generated by_ $\mathbb{Z}$ _and_ $\frac{1}{2}$_. Prove or disprove:_ $\mathbb{Z}\left[\frac{1}{2}\right]$ _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_

$$\begin{aligned} 5x + 9y + 5z &= 0 \\ 2x + 4y + 2z &= 0 \\ x + y - 3z &= 0. \end{aligned}$$

Determine the elementary divisors of G _and write_ G _as a direct sum of cyclic groups._

M7. Let R _be a ring and let_ $f : M \to N$ _be a surjective homomorphism of_ R_-modules, where_ N _is a free_ R_-module. Show that there exists an_ R_-module homomorphism_ $g : N \to M$ _such that_ $f \circ g = 1_N$_. Show that_ $M = \mathrm{Ker}(f) \oplus \mathrm{Im}(g)$_._

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_ $f : M \to M$ _be an_ R_-module endomorphism which is idempotent, that is,_ $f \circ f = f$_. Prove that_ $M \cong \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$_._

M11. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$_, where_ d _is the greatest common divisor of_ n _and_ m_._

M12. Compute $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q})$ _and_ $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$_._

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_ $R : V \to W$ _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* $P : V \to W$ *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 $\varphi : S \to S'$ *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 $\mathrm{Spec}(\mathbb{C}[x])$ *(polynomial ring in one variable over the complex numbers).*
(c) Describe $\mathrm{Spec}(\mathbb{R}[x])$.

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

L3. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ 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 $T : \mathbb{C}^n \to \mathbb{C}^n$ be a nilpotent linear transformation.
(a) How is $\dim \operatorname{Ker} T$ related to the Jordan normal form of T ? How is the minimal polynomial related to the Jordan normal form?
(b) Let $T, S : \mathbb{C}^6 \to \mathbb{C}^6$ be nilpotent linear transformations such that S and T have the same minimal polynomial and $\dim \operatorname{Ker} T = \dim \operatorname{Ker} S$. Show that S and T have the same Jordan form.
(c) Show that there are nilpotent linear transformations $T, S : \mathbb{C}^8 \to \mathbb{C}^8$ such that S and T have the same minimal polynomial and $\dim \operatorname{Ker} T = \dim \operatorname{Ker} S$, 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 $\operatorname{Im}(T_i) = \operatorname{Ker}(T_{i+1})$ for $1 \le i \le n-1$. 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 $\operatorname{Ker} S = \operatorname{Ker} T$ 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 $T : V \to V$ 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 $I : V \to V$ 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 $T : V \to V$ 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.)