

Part A.

1. Let $x, y \in G$. Then $x * y = x + y + xy \in \mathbb{R}$. Suppose $x * y = -1$. Then $x + xy = -1 - y$, which implies $x(y + 1) = -(y + 1)$. Since $y \neq -1$, we have $y + 1 \neq 0$; hence $x = -1$, a contradiction. Therefore $x * y \in G$, and $*$ is a binary operation on G .

It remains to show that $(G, *)$ is a group. Let $x, y, z \in G$. Then

$$\begin{aligned} (x * y) * z &= (x + y + xy) + z + (x + y + xy)z \\ &= x + y + z + xy + yz + xz + xyz \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x * (y * z). \end{aligned}$$

Hence $*$ is associative.

We claim that 0 is an identity element for $(G, *)$. For $x \in G$ we have

$$x * 0 = x + 0 + x \cdot 0 = x = 0 + x + 0 \cdot x = 0 * x.$$

Finally, for $x \in G$ we claim that $x^{-1} = \frac{-x}{x+1}$ and that such x^{-1} belongs to G . We have

$$x * \frac{-x}{x+1} = x + \frac{-x}{x+1} + \frac{-x^2}{x+1} = \frac{x(x+1) - x - x^2}{x+1} = 0$$

and similarly

$$\frac{-x}{x+1} * x = 0.$$

Clearly x^{-1} belongs to \mathbb{R} . Moreover $x^{-1} \neq -1$, else $-x = -(x+1)$ which is impossible. Thus $x^{-1} \in G$.

2. First of all $e \in A_n$, and thus $A_n \neq \emptyset$. Let $\sigma = (a_1 b_1) \dots (a_k b_k)$ and $\tau = (c_1 d_1) \dots (c_l d_l)$ be two elements in A_n (and thus k and l are even). Then $\sigma\tau^{-1} = (a_1 b_1) \dots (a_k b_k)(c_l d_l) \dots (c_1 d_1)$ is also even and hence belongs to A_n . Thus A_n is a subgroup of S_n .

Now let $\sigma \in A_n$ as above, and suppose $\alpha \in S_n$. Write α as a product of m transpositions. Then $\alpha\sigma\alpha^{-1}$ can be written as a product of $m + k + m = 2m + k$ transpositions, which is even since k is even. Thus $\alpha\sigma\alpha^{-1} \in A_n$, and A_n is normal in S_n .

3. By contradiction, suppose that there is an onto homomorphism $\psi : \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \rightarrow \mathbb{Z}_8 \oplus \mathbb{Z}_6$. By the First Isomorphism Theorem, $(\mathbb{Z}_4 \oplus \mathbb{Z}_{12})/\ker \psi \approx \mathbb{Z}_8 \oplus \mathbb{Z}_6$. Since $4 \cdot 12 = 8 \cdot 6 = 48$, it follows that $|\ker \psi| = 1$. That is, ψ is one-to-one.

But then ψ must be an isomorphism. Note, however, that $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ cannot be isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_6$ since $\mathbb{Z}_8 \oplus \mathbb{Z}_6$ has an element of order 24 but $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ does not. Hence there can be no homomorphism from $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ onto $\mathbb{Z}_8 \oplus \mathbb{Z}_6$. \square

4. (a) Let $x, y \in G$. Then $\phi_a(xy) = a(xy)a^{-1} = (ax)(a^{-1}a)(ya^{-1}) = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$. Thus ϕ_a is a group homomorphism. Now assume that $\phi_a(x) = \phi_a(y)$, that is, $axa^{-1} = aya^{-1}$. Then by left and right cancellation, $x = y$, which implies that ϕ_a is one-to-one. Moreover, if $z \in G$ then $x = a^{-1}za \in G$ (since G is closed under inverses and group operation) and $\phi_a(x) = a(a^{-1}za)a^{-1} = z$, which shows that ϕ_a is onto. Therefore ϕ_a is an automorphism of G .

- (b) Let $\phi_a, \phi_b \in \text{Inn}(G)$ and let $x \in G$. Then $(\phi_a \circ \phi_b)(x) = \phi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1}$. Thus $\phi_a \circ \phi_b = \phi_{ab} \in \text{Inn}(G)$, and $\text{Inn}(G)$ is closed.

It is easy to see that ϕ_e is the identity element for $\text{Inn}(G)$ (where e is the identity element of G) since $\phi_a \circ \phi_e = \phi_{ae} = \phi_a = \phi_{ea} = \phi_e \circ \phi_a$.

To this end, we note that since ϕ_a is bijective it has an inverse ϕ_a^{-1} . Moreover, $\phi_a^{-1}(x) = a^{-1}xa$, for all $x \in G$ [since $(\phi_a \circ \phi_a^{-1})(x) = x = (\phi_a^{-1} \circ \phi_a)(x)$]. Furthermore, $\phi_a^{-1}(x) = a^{-1}xa = a^{-1}x(a^{-1})^{-1}$. Thus $\phi_a^{-1} = \phi_{a^{-1}} \in \text{Inn}(G)$, and $\phi_{a^{-1}} \circ \phi_a = \phi_e = \phi_a \circ \phi_{a^{-1}}$, which implies that the inverse of ϕ_a in $\text{Inn}(G)$ is $\phi_{a^{-1}}$. Hence $\text{Inn}(G)$ is a group. \square

5. (a) Since R is a ring with unity 1, we know that $1+I$ is the unity in the quotient ring R/I . Then an arbitrary element $r+I \in R/I$ is a unit if and only if there exists an element $s+I \in R/I$ (thus $s \in R$) such that $(r+I)(s+I) = rs+I = 1+I$. But this is equivalent to $rs \in (1+I)$, which is equivalent to $rs - 1 \in I$.

So, we have shown that $r+I \in R/I$ is a unit if and only if there exists an element $s \in R$ such that $rs - 1 \in I$.

- (b) Let $a, b \in \mathbb{Z}$ such that $a \neq 0$ and $b \neq 0$. Then $(a, 0), (0, b) \in \mathbb{Z} \oplus \mathbb{Z}$ with $(a, 0) \neq (0, 0)$ and $(0, b) \neq (0, 0)$. Observe that $(a, 0)(0, b) = (a \cdot 0, 0 \cdot b) = (0, 0)$. Since $(0, 0)$ is the zero element in the ring $\mathbb{Z} \oplus \mathbb{Z}$, we have shown that $(a, 0)$ and $(0, b)$ are zero-divisors in $\mathbb{Z} \oplus \mathbb{Z}$, for all nonzero integers a and b .
- (c) We know that if R_1 and R_2 are rings and $a \in R_1$ and $b \in R_2$, then (a, b) is a unit in the ring $\mathbb{R}_1 \oplus \mathbb{R}_2$ if and only if a is a unit in R_1 and b is a unit in R_2 . Since the only units in \mathbb{Z} are 1 and -1 , we have that $(1, 1), (1, -1), (-1, 1)$ and $(-1, -1)$ are all the units in $\mathbb{Z} \oplus \mathbb{Z}$. \square

6. (a) Let $a \in R$ be an idempotent. So $a^2 = a$.

Then $(1-a)^2 = (1-a)(1-a) = 1 \cdot 1 - 1 \cdot a - a \cdot 1 + a^2 = 1 - 2a + a = 1 - a$. So $1-a$ is an idempotent element of R .

- (b) Let $f : R \rightarrow S$ be a ring homomorphism and let $a \in R$ such that $a^n = 0_R$ for some positive integer n . Then $f(a^n) = (f(a))^n$, which can be rewritten as $0_S = f(0_R) = (f(a))^n$, thus $f(a)$ is an idempotent element of S .
- (c) Now assume that R is an integral domain (that is, R is a commutative ring with unity, call it 1, and no zero-divisors) and let $a \in R$ be an idempotent. Then $a^2 = a$, or equivalently, $a(a-1) = 0$. Since R has no zero-divisors, the last equality implies that $a = 0$ or $a = 1$.
- (d) Let $0 \neq a \in R$ be a zero-divisor. Then there exists $0 \neq b \in R$ such that $ab = 0$, which implies that $aba = 0 \cdot a = 0$. Conversely, let $b \in R, b \neq 0$ such that $aba = 0$. Clearly $ba \in R$ by the closure property of R with respect to multiplication, $ba \neq 0$ and $0 = aba = a(ba)$, thus a is a zero-divisor. \square

7. (a) Assume that $G/Z(G)$ is cyclic and let $gZ(G)$ be a generator of $G/Z(G)$, for some $g \in G$. Let $a, b \in G$. Then $aZ(G) = (gZ(G))^i = g^iZ(G)$ and $bZ(G) = (gZ(G))^j = g^jZ(G)$ for some $i, j \in \mathbb{Z}$. But then $a = g^ix$ and $b = g^jy$ for some $x, y \in Z(G)$.

Thus we have

$$\begin{aligned}
 ab &= (g^ix)(g^jy) \\
 &= g^i(xg^j)y \\
 &= g^i(g^jx)y \\
 &= (g^jg^i)(yx) \\
 &= g^j(g^iy)x \\
 &= g^j(yg^i)x \\
 &= (g^jy)(g^ix) = ba,
 \end{aligned}$$

where we used that x and y commute with everything in G and that $g^ig^j = g^{i+j} = g^{j+i} = g^jg^i$. So we showed that $ab = ba$ for all $a, b \in G$, thus G is Abelian.

(b) Now assume that $|G| = p^3$, where p is a prime, that $Z(G) \neq \{e\}$ and that G is non-Abelian. Since $Z(G)$ is a subgroup of G , $|Z(G)|$ divides p^3 . Thus $|Z(G)|$ is equal to $1, p, p^2$ or p^3 (since p is a prime number). Since $Z(G)$ is non-trivial, $|Z(G)| \neq 1$. Moreover, since G is non-Abelian, $Z(G)$ is a proper subgroup of G , thus $|Z(G)| \neq p^3$. Finally, if $|Z(G)| = p^2$, then $|G/Z(G)| = p^3/p^2 = p$, and then $G/Z(G)$ must be cyclic (since any group of prime order is cyclic). But then part (a) implies that G is Abelian, which is a contradiction. Therefore the only possible case is $|Z(G)| = p$. \square

8. Let $G = \langle a \rangle$ with $|a| = n \geq 3$, and let m be an integer with $1 \leq m < n$. We claim that a^m is a generator of G if and only if a^{-m} is also a generator. In the forward direction we have $(a^m)^n = a^{mn} = e$, so $(a^{-m})^n = (a^{mn})^{-1} = e^{-1} = e$. If there is an integer k with $1 \leq k < n$ such that $(a^{-m})^k = e$, then $(a^{mk})^{-1} = e^{-1} = e$; hence $a^{mk} = (a^m)^k = e$, a contradiction. The converse is similar. Finally, note that for m as above, if a^m is a generator, then $a^m \neq a^{-m}$, since otherwise $a^{2m} = e = a^n$, yielding $|a^m| \leq 2 < n$, a contradiction. Thus the set of distinct generators of G is $\{a^m, a^{-m} \mid a^m \text{ is a generator}\}$, which clearly has an even number of elements.

Part B.

1. We use the formula

$$\mathbf{v}_i = \mathbf{u}_i - \frac{\mathbf{v}_1 \cdot \mathbf{u}_i}{\mathbf{v}_1 \cdot \mathbf{v}_1} \mathbf{v}_1 - \frac{\mathbf{v}_2 \cdot \mathbf{u}_i}{\mathbf{v}_2 \cdot \mathbf{v}_2} \mathbf{v}_2 - \dots - \frac{\mathbf{v}_{i-1} \cdot \mathbf{u}_i}{\mathbf{v}_{i-1} \cdot \mathbf{v}_{i-1}} \mathbf{v}_{i-1}$$

with $v_1 = u_1 = \begin{bmatrix} 1 \\ 3 \\ 2 \\ 1 \end{bmatrix}$. We then obtain $v_2 = \begin{bmatrix} \frac{1}{3} \\ 0 \\ -\frac{1}{3} \\ \frac{1}{3} \end{bmatrix}$ and $v_3 = \begin{bmatrix} \frac{1}{5} \\ -\frac{3}{5} \\ \frac{3}{5} \\ \frac{1}{5} \end{bmatrix}$, which forms an orthogonal basis for W . Dividing by the magnitude of each vector we obtain an orthonormal basis for W :

$$\left\{ \frac{1}{\sqrt{15}} \begin{bmatrix} 1 \\ 3 \\ 2 \\ 1 \end{bmatrix}, \frac{\sqrt{3}}{3} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} \\ -1 \\ 1 \\ \frac{1}{2} \end{bmatrix} \right\}$$

2. First, we need to show that C is linearly independent.

$$\begin{aligned} \mathbf{0} &= c_1 A\mathbf{x}_1 + c_2 A\mathbf{x}_2 + c_3 A\mathbf{x}_3 + \dots + c_n A\mathbf{x}_n \\ &= Ac_1\mathbf{x}_1 + Ac_2\mathbf{x}_2 + Ac_3\mathbf{x}_3 + \dots + Ac_n\mathbf{x}_n \\ &= A(c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + c_3\mathbf{x}_3 + \dots + c_n\mathbf{x}_n). \end{aligned}$$

Since A is nonsingular, we obtain

$$\mathbf{0} = c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + c_3\mathbf{x}_3 + \dots + c_n\mathbf{x}_n.$$

Since B is a basis, it is linearly independent. Thus, $c_1 = c_2 = \dots = c_n = 0$, and C is linearly independent.

Next, we need to show that C spans \mathbb{R}^n . Given an arbitrary vector $\mathbf{y} \in \mathbb{R}^n$. Since A is nonsingular, we can define the vector \mathbf{w} to be the unique solution of $A\mathbf{w} = \mathbf{y}$. Since $\mathbf{w} \in \mathbb{R}^n$, we can write \mathbf{w} as a linear combination of vectors in basis B . So,

$$\mathbf{w} = c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + c_3\mathbf{x}_3 + \dots + c_n\mathbf{x}_n,$$

where $c_1, c_2, c_3, \dots, c_n$ are scalars. Thus,

$$\begin{aligned} \mathbf{y} &= A\mathbf{w} \\ &= A(c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + c_3\mathbf{x}_3 + \dots + c_n\mathbf{x}_n) \\ &= Ac_1\mathbf{x}_1 + Ac_2\mathbf{x}_2 + Ac_3\mathbf{x}_3 + \dots + Ac_n\mathbf{x}_n \\ &= c_1 A\mathbf{x}_1 + c_2 A\mathbf{x}_2 + c_3 A\mathbf{x}_3 + \dots + c_n A\mathbf{x}_n. \end{aligned}$$

So, C spans \mathbb{R}^n .

3. The kernel is the solution space of the homogeneous system $A\mathbf{x} = \mathbf{0}$. Performing Gaussian elimination on A gives the matrix

$$\begin{bmatrix} 1 & 3 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, a basis for the kernel of the linear transformation is $\{[2, -1, 1]\}$. Since the range is the column space of A , a basis for the range of the linear transformation is $\{[1, 0, 0], [1, 1, 0]\}$.

4. First, we need to find the eigenvalues and eigenvectors of A . The characteristic equation is found from

$$\begin{aligned} 0 &= \begin{vmatrix} 3 - \lambda & -5 \\ 1 & -3 - \lambda \end{vmatrix} \\ &= \lambda^2 - 4 \\ &= (\lambda + 2)(\lambda - 2). \end{aligned}$$

We find an eigenvector for each eigenvalue, obtaining:

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 5 \\ 1 \end{bmatrix}.$$

Thus, $A = QDQ^{-1}$, so

$$\begin{aligned} A^{2011} &= QD^{2011}Q^{-1} \\ &= \begin{bmatrix} 1 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} (-2)^{2011} & 0 \\ 0 & 2^{2011} \end{bmatrix} \begin{bmatrix} 1 & -5 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} -\frac{1}{4} \end{pmatrix} \\ &= \begin{bmatrix} 3 \cdot 2^{2010} & -5 \cdot 2^{2010} \\ 2^{2010} & -3 \cdot 2^{2010} \end{bmatrix} \end{aligned}$$

since

$$Q = \begin{bmatrix} 1 & 5 \\ 1 & 1 \end{bmatrix}, \quad \text{and } D = \begin{bmatrix} -2 & 0 \\ 0 & 2 \end{bmatrix}.$$

5. The matrix has characteristic polynomial $\lambda^4 \cdot (\lambda - 15)$ giving the eigenvalues 0 and 15.

Another way to do this is to realize that this matrix has rank 1, and thus $\lambda = 0$ is an eigenvalue of multiplicity 4 (as this is a 5×5 matrix). In order to find the other eigenvalue

we notice that this matrix times the vector $\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ yields $\begin{bmatrix} 15 \\ 15 \\ 15 \\ 15 \\ 15 \end{bmatrix}$ and thus $\lambda = 15$ is the fifth eigenvalue.

6. Set $\det \begin{bmatrix} -2 & \lambda & 3 \\ 1 & 2 & \lambda \\ 1 & 11 & 18 \end{bmatrix} = 0 = \lambda^2 + 4\lambda - 45$ which has roots: -9 and 5 ; hence the matrix is non-singular for all values of λ *other* than those roots.

7. (a) It is easy to check that $\text{rank}(A) = 2$. Thus, the column space of A spans \mathbb{R}^2 ; hence $A\mathbf{x} = \mathbf{b}$ has at least one solution for all vectors in \mathbb{R}^2 . Note: the solution will not be unique because the rank of A does not equal 3 (clearly impossible for this underdetermined system which will be impossible to obtain 3 pivots upon row reduction!)

- (b) Since solutions to systems represent the scalars for linear combinations of the columns of the coefficient matrix, by inspection one solution is $\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$. Upon reduction of the augmented system, we obtain the complete parameterized infinite solution (since we MUST have a free variable): $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + t \cdot \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$.

- (c) 2 of course.

8. *Solution.*

(a) T is linear, as

$$T(p+q) = \begin{bmatrix} (p+q)(-1) \\ (p+q)(0) \\ (p+q)(1) \end{bmatrix} = \begin{bmatrix} p(-1) + q(-1) \\ p(0) + q(0) \\ p(1) + q(1) \end{bmatrix} = \begin{bmatrix} p(-1) \\ p(0) \\ p(1) \end{bmatrix} + \begin{bmatrix} q(-1) \\ q(0) \\ q(1) \end{bmatrix} = T(p) + T(q)$$

The matrix for T , A , is given by the image of the columns for the basis for P_2 , namely

$\{1, x, x^2\}$; hence $A = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$. All matrices represent linear transformations,

so linearity is given. $\det(A) = \begin{vmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{vmatrix} \neq 0$; hence the linear transformation is invertible.

$$(b) A^{-1} = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2} \begin{bmatrix} 1 & 2 & 0 \\ -1 & 0 & 1 \\ 1 & -2 & 1 \end{bmatrix}; \text{ hence}$$

$$\begin{aligned} A^{-1} &= \frac{1}{2} \begin{bmatrix} 0 & 2 & 0 \\ -1 & 0 & 1 \\ 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 2b \\ -a + c \\ a - 2b + c \end{bmatrix} \\ &= \begin{bmatrix} b \\ \frac{c-a}{2} \\ \frac{a-2b+c}{2} \end{bmatrix}. \end{aligned}$$

Thus,

$$T^{-1} \left(\begin{bmatrix} a \\ b \\ c \end{bmatrix} \right) = b + \left(\frac{c-a}{2} \right) x + \left(\frac{a-2b+c}{2} \right) x^2.$$