

Part A.

1. (a) Note that $ab = e$ implies that $a^{-1}(ab) = a^{-1}$ (by multiplying by a^{-1} on the left). Then $b = a^{-1}$. But now, by multiplying by a on the right, we get that $ba = a^{-1}a$. Finally we see that $ba = e$, as required. \square
- (b) Let $G = \{e, a, b, c\}$ be a group of order 4. By contradiction, suppose that $ab \neq ba$. Then we must have $ab = e$ and $ba = c$ (or vice versa). Note that here we are using that the only solution in G of an equation of the form $ax = a$ is $x = e$. But then, this contradicts part (a). Thus if $x, y \in G$, then $xy = yx$. That is, every group of order 4 is abelian. \square
- (c) First we show that $o(bab^{-1}) = \infty$ iff $o(a) = \infty$:
 To this end, suppose that $o(bab^{-1}) = \infty$, but $o(a) = m < \infty$. Then $(bab^{-1})^m = ba^m b^{-1} = beb^{-1} = e$. But this contradicts the fact that $o(bab^{-1}) = \infty$. Thus, if $o(bab^{-1}) = \infty$, then $o(a) = \infty$.
 Now suppose that $o(a) = \infty$, but $o(bab^{-1}) = n < \infty$. Then $(bab^{-1})^n = e$, by definition. Hence $ba^n b^{-1} = e$. It follows from the last equation that $a^n = e$, a contradiction. Therefore, $o(bab^{-1}) = \infty$ iff $o(a) = \infty$. By contrapositive, we also have that $o(bab^{-1}) < \infty$ iff $o(a) < \infty$.
 To finish up the proof, we show that if bab^{-1} and a both have finite order, then $o(bab^{-1}) = o(a)$. Let $o(bab^{-1}) = m$ and $o(a) = n$ ($m, n \in \mathbb{Z}$). First note that $(bab^{-1})^n = ba^n b^{-1} = beb^{-1} = e$, since $o(a) = n$. Thus, by definition of m , $m \leq n$. Now observe that $(bab^{-1})^m = e$ implies that $ba^m b^{-1} = e$ and this implies that $a^m = e$. Thus, by definition of n , $n \leq m$. Therefore $m = n$, as required. \square

2. Let $x, y, z \in \{1, 2, \dots, n\}$.

\sim **is reflexive:** Clearly $x \sim x$ since $\sigma^0(x) = x$.

\sim **is symmetric:** Suppose $x \sim y$. Then there exists $k \in \mathbb{Z}$ such that $\sigma^k(x) = y$. Thus $\sigma^{-k}(y) = x$, and therefore $y \sim x$.

\sim **is transitive:** Suppose $x \sim y$ and $y \sim z$. Then there exist $k, l \in \mathbb{Z}$ such that $\sigma^k(x) = y$ and $\sigma^l(y) = z$. Thus $\sigma^{k+l}(x) = \sigma^l \sigma^k(x) = \sigma^l(y) = z$, and therefore $x \sim z$.

3. First of all we note that every element of both R and S has a unique representation. This is trivial for R , but for S we need to look at

$$a + b\sqrt{2} = c + d\sqrt{2}$$

Since this forces $a - c = (d - b)\sqrt{2}$, which if $d - b \neq 0$ implies $\sqrt{2} = \frac{a - c}{d - b} \in \mathbb{Z}$, which is a contradiction. Hence, $d = b$, and $a = c$ as well.

Let us assume for a minute that φ is a homomorphism.

Now suppose $\varphi\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) = 0 = 0 + 0\sqrt{2}$. Then $a = 0$ and $b = 0$ (using the uniqueness of the representation). Hence $\ker(\varphi) = 0$, and φ is one-to-one. Next, φ is clearly onto, for all elements of S are of the form $a + b\sqrt{2} = \varphi\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right)$; hence $\text{im}(\varphi) = S$.

Now, in order to check that φ is a homomorphism, let

$$A = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}.$$

We have

$$\begin{aligned} \varphi(A + B) &= \varphi\left(\begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix}\right) \\ &= a + c + (b + d)\sqrt{2} \\ &= \varphi(A) + \varphi(B). \end{aligned}$$

Similarly,

$$\begin{aligned} \varphi(AB) &= \varphi\left(\begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix}\right) \\ &= ac + 2bd + (ad + bc)\sqrt{2} \\ &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= \varphi(A)\varphi(B). \end{aligned}$$

Hence the operations are preserved.

4. (a) True. Let $[a]$ be a nonzero element in \mathbb{Z}_n . Since $a \in \mathbb{Z} \setminus \{0\}$ it follows that $\gcd(a, n) = 1$ or $\gcd(a, n) = d \neq 1$.

In the first case, Bezout's lemma assures the existence of two integers, m and n , such that $am + bn = 1$. Hence, reducing both sides module n we obtain $am \equiv 1 \pmod{n}$, which means $[a][m] = [1]$ in \mathbb{Z}_n , and thus $[m]$ is the inverse of $[a]$ in \mathbb{Z}_n .

In the second case, $d \neq 1$ divides a and n , and thus $a = dk$ and $n = dq$, where $k, q \in \mathbb{Z}$. Note that $0 < k < a$ and $0 < q < n$.

Hence,

$$qa = q(dk) = (qd)k = nk$$

and thus qa is a multiple of n , i.e. $[q][a] = [0]$ in \mathbb{Z}_n . It follows that $[a]$ is a zero divisor in \mathbb{Z}_n because $0 < q < n$, which means that $[q] \neq [0]$ in \mathbb{Z}_n .

- (b) False. In \mathbb{Z} , the element 2 is neither invertible nor a zero divisor.

5. Let $g \in G$, since $|G| = n$, then $g^n = e$. using that ϕ is a homomorphism, and thus that $\phi(e) = 1$ (the identity of the multiplicative group \mathbb{C}^* we get that

$$1 = \phi(e) = \phi(g^n) = \phi(g)^n$$

and thus $\phi(g)$ is an n^{th} root of 1. It follows that $\phi(g) = e^{2k\pi i/n}$, for some $k = 1, 2, \dots, n$. In particular, the norm of the complex number $\phi(g)$ must be one, which means that $\phi(g)$ lays on the unit circle, for all $g \in G$.

6. Consider a generic element $(a, b) \in \mathbb{Z}_{21} \oplus \mathbb{Z}_{35}$. Since 7 is prime, it follows that the possibilities for the orders of a and b are 1 or 7.

Case 1 $|a| = 7$ and $|b| = 1$ or 7. Since \mathbb{Z}_{21} has a unique cyclic group of order 7 and any cyclic group of order 7 has six generators, there are six choices for a . Similarly, there are seven choices for b . This gives 42 choices for (a, b) .

Case 2 $|a| = 1$ and $|b| = 7$. Since \mathbb{Z}_{35} has a unique cyclic group of order 7 and any cyclic group of order 7 has six generators, there are six choices for b . There is only one choice for a . So, this case yields six more possibilities for (a, b) .

Thus $\mathbb{Z}_{21} \oplus \mathbb{Z}_{35}$ has 48 elements of order 7.

7. (a) Let $A = \text{Ann}(a)$. Since $0 = 0 \cdot a$, we have that $0 \in A$ and $A \neq \emptyset$. Let $x, y \in A$. Then $xa = 0, ya = 0$, and so $(x \pm y)a = xa \pm ya = 0$. Thus $x \pm y \in A$. Now let $r \in R$ and $x \in A$. Then $xa = 0$ and $(rx)a = r(xa) = r \cdot 0 = 0$ and so $rx \in A$. Hence A is an ideal of R . \square

- (b) Let $R = S \oplus T$ be the direct sum of the nonzero rings S and T . Then for all $s \in S, s \neq 0$ and all $t \in T, t \neq 0$ we have $(s, 0)(0, t) = (0, 0)$. Thus $(s, 0)$ (and $(0, t)$) is a zero-divisor for R , implying R is not an integral domain. \square
8. (a) First note that $1 \in Z(G)$ since $1 \cdot x = x \cdot 1$ for all $x \in G$. Thus $Z(G)$ is nonempty. Let m and n be elements of $Z(G)$, and let $x \in G$. Since $xn = nx$, we have $x = nxn^{-1}$ and thus $n^{-1}x = xn^{-1}$. Therefore $xmn^{-1} = mxn^{-1} = mn^{-1}x$, and $mn^{-1} \in Z(G)$. Thus, $Z(G) \leq G$.
- (b) Let $n \in Z(G)$ and $g \in G$, then g and n commute (n is in the center!). Hence, $gn g^{-1} = gg^{-1}n = n$, and thus $gZ(G)g^{-1} = Z(G)$, for all $g \in G$, and thus $Z(G) \trianglelefteq G$.

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 $v_1 = u_1 = \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}$. We then obtain $v_2 = \begin{bmatrix} 3 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ and $v_3 = \begin{bmatrix} 1 \\ 0 \\ -3 \\ 10 \end{bmatrix}$, which

forms an orthogonal basis for W . Dividing by the magnitude of each vector we obtain an orthonormal basis for W :

$$\left\{ \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \frac{1}{\sqrt{10}} \begin{bmatrix} 3 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \frac{1}{\sqrt{110}} \begin{bmatrix} 1 \\ 0 \\ -3 \\ 10 \end{bmatrix} \right\}$$

2. Consider the linear transformation $\Phi : v \mapsto Av$. We know that A is invertible if and only if Φ is bijective.

(\Rightarrow): Assume A is invertible, i.e. Φ is bijective.

If $\lambda = 0$ were an eigenvalue of A , then there would be an eigenvector of Φ , call it v , such that $\Phi(v) = 0$. It follows that $v \in \text{Ker}(\Phi)$. Hence, Φ is not injective, and thus not bijective. Contradiction.

(\Leftarrow): Assume that 0 is not an eigenvalue of A .

It follows that there is no vector such that $\Phi(v) = 0$, and thus $\text{Ker}(\Phi)$ is trivial. The dimension formula

$$\dim(\text{Domain}) - \dim(\text{Kernel}) = \dim(\text{Range})$$

implies that $\dim(\text{Range}) = n$, which means that Φ is also onto. Done.

3. First, since $T(1) = 1$, $T(x) = 1 + 2x$, and $T(x^2) = 1 + 2x + 3x^2$, with respect to the standard basis $S = \{1, x, x^2\}$, the matrix of T ,

$$[T]_{S,S} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{pmatrix}.$$

Consider the basis $C = \{1, 1 + x, 3 + 4x + 2x^2\}$. The transition matrix from C to S is the matrix whose columns are the standard coordinates of the elements of C . So,

$$[T]_{S,C} = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then, the transition matrix from S to C is given by

$$[T]_{C,S} = \begin{pmatrix} 1 & -1 & \frac{1}{2} \\ 0 & 1 & -2 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Thus, the matrix P of T with respect to the basis C is given by

$$\begin{aligned} P &= \begin{pmatrix} 1 & -1 & \frac{1}{2} \\ 0 & 1 & -2 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}. \end{aligned}$$

4. (a) Any element $x \in U \cap V$ can be written as

$$x = a(1, 0, 1, 0) + b(-1, 2, 0, 1) = c(0, 2, 1, 1) + d(0, 0, 1, 1)$$

It follows that

$$a - b = 0 \quad 2b - 2c = 0 \quad a - c - d = 0 \quad b - c - d = 0$$

Since the first equation implies $a = b$ we get

$$a = b \quad 2a - 2c = 0 \quad a - c - d = 0$$

The second equation forces $a = c$, and thus

$$a = b \quad a = c \quad d = 0$$

It follows that the vectors in the intersection look like

$$x = a(1, 0, 1, 0) + a(-1, 2, 0, 1) = a(0, 2, 1, 1)$$

which forms the set $U \cap V = \langle (0, 2, 1, 1) \rangle$. So, a basis of $U \cap V$ would be $\{(0, 2, 1, 1)\}$.

- (b) Since U has dimension two, then we need to find one more vector in U to complete $\{(0, 2, 1, 1)\}$ to a basis for U . Take $(1, 0, 1, 0)$ (taken from the given spanning set of U), which is clearly independent from $(0, 2, 1, 1)$. Hence, $\mathcal{B} = \{(0, 2, 1, 1), (1, 0, 1, 0)\}$ is a basis of U .

5. It is easily verified that A is row equivalent to the matrix

$$\begin{pmatrix} 1 & 0 & 1 & -2 & 5 \\ 0 & 1 & -1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which has rank 3; hence $\text{rank}(A) = 3$. Since A is 4×5 , we have $\text{rank} + \text{nullity} = 5$; thus $\text{nullity}(A) = 2$.

6. The dimension formula says that

$$\dim(U \oplus V) = \dim(U) + \dim(V) - \dim(U \cap V)$$

and since $U \oplus V < W$, then $\dim(U \oplus V) \leq 5$. It follows that

$$5 \geq \dim(U) + \dim(V) - \dim(U \cap V)$$

Since $\dim(U) = \dim(V) = 3$, then

$$5 \geq 3 + 3 - \dim(U \cap V)$$

which implies that $\dim(U \cap V) \geq 1$, and thus $U \cap V$ is nontrivial (meaning it is not just the zero vector).

7. We want to diagonalize $A = \begin{pmatrix} 3 & -2 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$.

The characteristic polynomial of A is

$$\begin{aligned} \chi_A(\lambda) = \det(A - \lambda I) &= \det \begin{pmatrix} 3 - \lambda & -2 & 2 \\ 0 & 1 - \lambda & 2 \\ 0 & 2 & 1 - \lambda \end{pmatrix} \\ &= (3 - \lambda) \det \begin{pmatrix} 1 - \lambda & 2 \\ 2 & 1 - \lambda \end{pmatrix} \\ &= (3 - \lambda)[(1 - \lambda)^2 - 2^2] \\ &= (3 - \lambda)(\lambda^2 - 2\lambda - 3) \\ &= -(\lambda + 1)(\lambda - 3)^2. \end{aligned}$$

It follows that the eigenvalues of A are $\lambda = -1$ and $\lambda = 3$.

What is the dimension of the eigenspace of $\lambda = 3$? We set the equation $Av = 3v$:

$$\begin{pmatrix} 3 & -2 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3x \\ 3y \\ 3z \end{pmatrix}$$

which forces

$$\begin{aligned} -2y + 2z &= 0 \\ -2y + 2z &= 0 \\ 2y - 2z &= 0 \end{aligned}$$

It follows that $y = z$ and thus the eigenspace of $\lambda = 3$ is spanned by $\{(1, 0, 0), (0, 1, 1)\}$. Hence, A is diagonalizable to the matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

8. Let α, β, γ be real numbers. We will start by subtracting row two from row three, we get

$$\begin{vmatrix} \sin^2 \alpha & \sin^2 \beta & \sin^2 \gamma \\ \cos^2 \alpha & \cos^2 \beta & \cos^2 \gamma \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} \sin^2 \alpha & \sin^2 \beta & \sin^2 \gamma \\ \cos^2 \alpha & \cos^2 \beta & \cos^2 \gamma \\ 1 - \cos^2 \alpha & 1 - \cos^2 \beta & 1 - \cos^2 \gamma \end{vmatrix}$$

but since $1 - \cos^2 x = \sin^2 x$, for all $x \in \mathbb{R}$. Then, the third row of the latter determinant is equal to its first row. Hence, the determinant is equal to zero.

Another way to see this is to realize that the sum of the first two rows equals the third, as $\sin^2 x + \cos^2 x = 1$, for all $x \in \mathbb{R}$. Hence, the three rows being linearly dependent forces the determinant to be zero.