Part A. Solve five of the following eight problems:

1. Let \( R = \{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \} \) and \( S = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \)

Define \( \varphi : R \rightarrow S \) by \( \varphi \left( \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \right) = a + b\sqrt{2} \). Prove that \( \varphi \) is a ring isomorphism.

You may assume that \( R \) and \( S \) are commutative rings and that \( \varphi \) is a well-defined function.

2. (a) Let \( G_1 \) and \( G_2 \) be groups and consider their direct product \( G_1 \times G_2 \). Prove that \( G_1 \times G_2 \) is Abelian if and only if both \( G_1 \) and \( G_2 \) are Abelian.

(b) The dihedral group \( D_n \) of order \( 2n \) \((n \geq 3)\) has a subgroup \( H \) of order \( n \) consisting of rotations, and several subgroups of order 2. Prove that \( D_n \) cannot be isomorphic to the direct product of \( H \) and any of the groups of order 2.

3. Let \( G \) be a cyclic group of order 8. Prove that \( G \) has exactly one element of order 2. Is there a non-Abelian group of order 8 with this property?

4. Let \( G \) be a group and \( a, b \in G \). Assume that \(|a| = 12\), \(|b| = 22\) and \( \langle a \rangle \cap \langle b \rangle \neq \{e\} \), prove that \( a^6 = b^{11} \).

5. An (additive) Abelian group \( G \) is said to be divisible if for every element \( a \in G \), and every \( k \in \mathbb{Z} \setminus \{0\} \), there is an element \( x \in G \) such that \( kx = a \).

Show that \( \mathbb{Q} \) is divisible but that \( \mathbb{Z} \) is not.

6. Recall that the center of a group \( G \) is the subset \( Z(G) = \{ a \in G \mid ax = xa \text{ for all } x \in G \} \).

(a) Prove that \( Z(G) \) is a subgroup of \( G \);

(b) Prove that \( Z(G) \) is normal in \( G \).

7. Let \( v \) be a fixed vector in \( \mathbb{R}^n \). Show that the set of all matrices \( A \in M_n(\mathbb{R}) \) such that \( Av = 0 \) is a left ideal of \( M_n(\mathbb{R}) \).

8. (a) Find the characteristic of the ring \( \mathbb{Z}_4 \oplus 4\mathbb{Z} \) (which, using a different notation, is \( \mathbb{Z}_4 \times 4\mathbb{Z} \)).

(b) Let \( R \) be a commutative ring of characteristic 2. Prove that the set of all idempotents in \( R \) is a subring of \( R \).

Remark: \( x \in R \) is an idempotent iff \( x^2 = x \).

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Let \( T : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \) be a linear transformation given by \( T(x_1, x_2) = (x_1 + x_2, -3x_1 - 3x_2) \).
   
   (a) Determine whether or not \( T \) is invertible.
   
   (b) Determine whether or not the vector \( w = (2, 5) \) is in the range of \( T \).
   
   (c) Find the dimension of the kernel of \( T \).

2. Suppose that \( B = P^{-1}AP \) (where \( A, B \) and \( P \) are square matrices of the same size, and \( P \) is invertible) and that \( x \) is an eigenvector of \( A \) corresponding to an eigenvalue \( \lambda \). Show that \( P^{-1}x \) is an eigenvector of \( B \) corresponding also to \( \lambda \).

3. The following \( 3 \times 3 \) matrix depends on \( c \):
   
   \[
   A = \begin{bmatrix}
   1 & 1 & 2 & 4 \\
   3 & c & 2 & 8 \\
   0 & 0 & 2 & 2
   \end{bmatrix}.
   \]
   
   (a) For each \( c \), find a basis for the column space of \( A \).
   
   (b) For each \( c \), find a basis for the null space of \( A \).
   
   (c) For each \( c \), find the complete solution to \( Ax = \begin{bmatrix} 1 \\ c \\ 0 \end{bmatrix} \).

4. Given \( A = \begin{bmatrix} 0 & 1 \\ -2 & -3 \end{bmatrix} \), find \( A^{12} \).

5. Suppose that \( A \) is an invertible matrix and similar to \( B \). Show that \( B \) is invertible, and that \( A^{-1} \) is similar to \( B^{-1} \).

6. Justify your answer to each part.
   
   (a) Let \( A \) be a fixed \( 3 \times 3 \) matrix, and let \( V \) be the set of all \( 3 \times 3 \) matrices \( B \) such that \( AB = BA \). Is \( V \) a subspace of \( M_{3 \times 3}(\mathbb{R}) \)?
   
   (b) Let \( N \) be the set of all continuous functions on \([-1, 1]\) so that \( f(x) < 0 \) for \( x \in [-1, 1] \). Is \( N \) a subspace of \( C[-1, 1] \)?
   
   (c) Let \( V \) and \( V' \) be vector spaces, and let \( T : V \rightarrow V' \) be a linear transformation. Is the kernel of \( T \) a subspace of \( V \)?

7. Let \( V \) be a vector space, and \( u, v_1, v_2, \ldots, v_n, w \in V \). Suppose that \( u \in \text{Span}\{v_1, v_2, \ldots, v_n, w\} \), but \( u \notin \text{Span}\{v_1, v_2, \ldots, v_n\} \). Show that \( w \in \text{Span}\{u, v_1, v_2, \ldots, v_n\} \).

8. Let \( f(t) = 2, g(t) = -2t - 1, \) and \( h(t) = 7t^2 - 2t + 7 \). Consider the inner product
   
   \[
   <p(t), q(t)> = p(-1)q(-1) + p(0)q(0) + p(1)q(1)
   \]
   
   in the vector space \( \mathcal{P}_2 \) (note that \( f(t), g(t), h(t) \in \mathcal{P}_2 \)). Use the Gram-Schmidt process to determine an orthogonal basis for the subspace of \( \mathcal{P}_2 \) spanned by the polynomials \( f(t), g(t), \) and \( h(t) \).
Part A.

1. Let \( A = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \) and let \( B = \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} \). First we show that \( \varphi \) preserves the two operations. We want to show:

\[
\varphi(A + B) = \varphi(A) + \varphi(B) \quad \text{and} \quad \varphi(AB) = \varphi(A)\varphi(B).
\]

for all \( A, B \in R \).

We have

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

and

\[
\varphi(AB) = \varphi \left( \begin{bmatrix} ac + 2bd & ad + bc \\ 2ad + 2bc & ac + 2bd \end{bmatrix} \right) = ac + 2bd + (ad + bc)\sqrt{2} = \varphi(A)\varphi(B).
\]

To show \( \varphi \) is one-to-one, note that \( \ker(\varphi) = \{ A \in R \mid \varphi(A) = 0 \} \). So, if \( A = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \) is such that \( \varphi(A) = 0 \), then \( a + b\sqrt{2} = 0 \). Hence, \( a = b = 0 \) because \( \sqrt{2} \notin \mathbb{Q} \). It follows that \( A = 0 \), for all \( A \in \ker(\varphi) \), and thus \( \ker(\varphi) = \{0\} \).

Finally, we show \( \varphi \) is onto. For \( y = a + b\sqrt{2} \in S \), we have \( y = \varphi(A) \) where \( A = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \in R \).

Thus the image of \( \varphi \) is all of \( S \). \( \square \)

2. (a) Let \((a_1, a_2), (b_1, b_2)\) be arbitrary elements in \( G_1 \times G_2 \). Thus \( a_1, b_1 \in G_1 \) and \( a_2, b_2 \in G_2 \).

Then \( (a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2) \) and \( (b_1, b_2)(a_1, a_2) = (b_1a_1, b_2a_2) \).

It follows that \( (a_1, a_2)(b_1, b_2) = (b_1, b_2)(a_1, a_2) \) if and only if \( a_1b_1a_2b_2 = b_1a_1b_2a_2 \), which is true if and only if \( a_1b_1 = b_1a_1 \) and \( a_2b_2 = b_2a_2 \).

(b) Let \( R \) be a rotation in \( 360/n \) degrees of a regular \( n \)-gon. Then, the rotation subgroup of order \( n \) of \( D_n \) is \( \langle R \rangle \). Let \( H \) denote a subgroup of order 2 (generated by any reflection).

Since both subgroups are cyclic, they are also both abelian. Hence, using part (a) we get that \( \langle R \rangle \times H \) is also abelian.

Since \( |\langle R \rangle \times H| = 2n \) and \( \langle R \rangle \cap H = \{e\} \) then \( \langle R \rangle \times H \cong D_n \), but this contradicts the fact that \( D_n \) is not abelian. \( \square \)

3. Every cyclic group of order 8 is isomorphic to \( \mathbb{Z}_8 \). The orders of elements in \( \mathbb{Z}_8 \) are

\[
|0| = 1 \quad |1| = 8 \quad |2| = 4 \quad |3| = 8 \quad |4| = 2 \quad |5| = 8 \quad |6| = 4 \quad |7| = 8
\]

It follows that there is exactly one element in \( \mathbb{Z}_8 \) having order 2.
The non-abelian groups of order 8 are $D_4$ and $Q_8$. We know that $D_4$ contains three non-trivial reflections (all of them having order 2), hence this cannot be our example. Let us look at the orders of elements in $Q_8$,

$$|1| = 1 \quad |i| = |−i| = |j| = |−j| = |k| = |−k| = 4 \quad |−1| = 2$$

So, $Q_8$ has the desired property.

4. First we note that $⟨a⟩ \cap ⟨b⟩$ is a subgroup of the groups $⟨a⟩$ and $⟨b⟩$, thus (Lagrange’s Theorem) $|⟨a⟩ \cap ⟨b⟩|$ divides $|⟨a⟩| = 12$ and $|⟨b⟩| = 22$. So, $|⟨a⟩ \cap ⟨b⟩|$ divides gcd(12, 22) = 2. Since $⟨a⟩ \cap ⟨b⟩ \neq \{e\}$, then $|⟨a⟩ \cap ⟨b⟩| \neq 1$, and so $|⟨a⟩ \cap ⟨b⟩| = 2$. Hence, there is exactly one non-identity element in $⟨a⟩ \cap ⟨b⟩$, call it $x$, and $|x| = 2$.

Working similarly to problem 3 above, or using that the number of elements of order 2 in a cyclic group equals $φ(2) = 1$, we get that the only element of order 2 in $⟨a⟩$ must be $x$. Since $|a^6| = 2$ (using $|a| = 12$) then $a^6 = x$. We get that $b^{11} = x$ in the same way.

5. Let $a \in \mathbb{Q}$, and $k \in \mathbb{Z} \setminus \{0\}$. We want to find an element $x \in \mathbb{Q}$ such that $kx = a$.

Just solving for $x$ in $kx = a$ we get $x = \frac{a}{k}$, which is a rational (recall that $k \neq 0$). Done.

Now we want to find $a \in \mathbb{Z}$, and $k \in \mathbb{Z} \setminus \{0\}$ such that there is no element $x \in \mathbb{Z}$ such that $kx = a$.

The idea would be to force $x$ to be a rational that is not an integer. So, let us take $a = 3$ and $k = 2$. This forces $x = \frac{3}{2} \not\in \mathbb{Z}$.

6. **Solution 1.** (a) First note that $e \in Z(G)$ since $e \cdot x = x \cdot e$, for all $x \in G$. Now let $m, n \in Z(G)$, and $x \in G$. Then, using associativity a few times, we get

$$x(mn) = (xm)n = (mx)n = m(nx) = (mn)x$$

therefore $mn \in Z(G)$.

Let $n \in Z(G)$, and $x \in G$. Since $x$ and $n$ commute we have $x = nxn^{-1}$ and thus $n^{-1}x = xn^{-1}$, which means that $n^{-1}$ commutes with $x$. Therefore $n^{-1} \in Z(G)$. It follows that $Z(G) \leq G$.

(b) To show that $Z(G)$ is normal in $G$, let $m \in Z(G)$ and $x \in G$. Then $xm = mx$ and thus $xmx^{-1} = m \in Z(G)$. □

**Solution 2.** For every $x \in G$ consider the function $\phi_x : G \rightarrow G$ defined by $\phi_x(g) = xgx^{-1}$.

This function is an automorphism of $G$, as

(i) $\phi_x(gh) = x(gh)x^{-1} = xgx(x^{-1}h)x^{-1} = (xgx^{-1})(xhx^{-1}) = \phi_x(g)\phi_x(h)$.

(ii) $\text{Ker}(\phi_x) = \{g \in G; xgx^{-1} = e\} = \{g \in G; xg = x\} = \{g \in G; g = e\} = \{e\}$.

(iii) For any given $g \in G$, $\phi_x(x^{-1}gx) = g$.

recall that $\text{Aut}(G)$ is a group under composition. We define the function $\phi : G \rightarrow \text{Aut}(G)$ by $\phi(x) = \phi_x$. This is a homomorphism, as

$$\phi_{xy}(g) = (xy)g(xy)^{-1} = xgyy^{-1}x^{-1} = x(ygy^{-1})x^{-1} = \phi_x(ygy^{-1}) = \phi_x(\phi_y(g)) = (\phi_x \circ \phi_y)(g)$$

for all $g \in G$.

Finally,

$$\text{Ker}(\phi) = \{x \in G; \phi_x = e\} = \{x \in G; \phi_x(g) = g, \text{ for all } g \in G\} = \{x \in G; xgx^{-1} = g, \text{ for all } g \in G\} = Z(G)$$

Since $\text{Ker}(\phi) = Z(G)$ and the domain of $\phi$ is $G$ then $Z(G) \leq G$. 
7. Let \( I = \{A \in M_n(\mathbb{R}); Av = 0\} \). Clearly \( I \subseteq M_n(\mathbb{R}) \), and \( O \in I \) (zero matrix, that is).
   Let \( A, B \in I \), then
   \[
   (A - B)v = Av - Bv = 0 - 0 = 0
   \]
   so, \( A - B \in I \).
   Now let \( a \in I \) and \( B \in M_n(\mathbb{R}) \), then
   \[
   (BA)v = B(Av) = B0 = 0
   \]
   and thus \( BA \in I \).

8. (a) We know that \( \text{char}(\mathbb{Z}_4) = 4 \), since \( 4a \equiv 0 \pmod{4} \), for all \( a \in \mathbb{Z}_4 \) and that there is no positive integer \( k < 4 \) such that \( ka \equiv 0 \pmod{4} \), for all \( a \in \mathbb{Z}_4 \).
   On the other hand, \( \text{char}(4\mathbb{Z}) = 0 \) since there is no positive integer \( n \) such that \( n(4l) = 0 \) for all \( 4l \in 4\mathbb{Z} \).
   Now let \( (a, 4l) \in \mathbb{Z}_4 \oplus 4\mathbb{Z} \). Then \( n(a, 4l) = (na, 4nl) \) for any positive integer \( n \). The observation above implies that there is no way to get a 0 in the second component of \( (na, 4nl) \), thus there is no positive integer \( n \) such that \( n(a, 4l) = (0, 0) \in \mathbb{Z}_4 \oplus 4\mathbb{Z} \). Hence, \( \text{char}(\mathbb{Z}_4 \oplus 4\mathbb{Z}) = 0 \).

(b) Let \( R \) be a commutative ring with \( \text{char}(R) = 2 \). Then \( 2x = 0 \) for all \( x \in R \) (note that this is equivalent to \( x = -x \) for all \( x \in R \)).
   Recall that \( x \in R \) is an idempotent if \( x^2 = x \). Let \( S = \{x \in R | x^2 = x\} \) be the set of all idempotents in \( R \). Clearly \( S \neq \emptyset \) since \( 0 \in S \) (for \( 0^2 = 0 \)).
   Let \( x, y \in S \) (thus \( x^2 = x \) and \( y^2 = y \)). Then
   \[
   (x - y)^2 = (x - y)(x - y) = x^2 - xy - yx + y^2 = x^2 - 2xy + y^2
   \]
   (since \( R \) is commutative). But this is equivalent to \( (x - y)^2 = x^2 + y^2 = x + y = x - y \), since \( y = -y \). Hence \( x - y \in S \).
   Moreover, \( (xy)^2 = x^2y^2 \) (since \( R \) is commutative), which is equivalent to \( (xy)^2 = xy \).
   Therefore \( xy \in S \) and \( S \) is a subring of \( R \), by the Subring Test.
   Note that if rings were considered to always have a one, then we would also have that \( 1 \in S \), as \( 1^2 = 1 \). \( \square \)
Part B.

1. (a) We want to find the standard matrix of $T$ (that is, the matrix of $T$ relative to the standard basis for $\mathbb{R}^2$). For that, we compute $T(1,0) = (1,-3)$ and $T(0,1) = (1,-3)$, and therefore the standard matrix of $T$ is $A = \begin{bmatrix} 1 & 1 \\ -3 & -3 \end{bmatrix}$.

Then $\det A = 0$, so the matrix $A$ is singular (NOT invertible), which implies that the linear transformation $T$ is NOT invertible.

(b) Recall that the range of a function $T$ is the set of all images $T(x)$. So, a vector $w = (2,5)$ is in the range of $T$ if the equation $T(x) = w$ has solutions. This equation is equivalent to the system

\[
\begin{align*}
x_1 + x_2 &= 2 \\
-3x_1 - 3x_2 &= 5
\end{align*}
\]

where we wrote $x = (x_1, x_2)$, and used the formula for $T$. We can easily see that the above system is inconsistent (it has no solutions), thus $w = (2,5)$ is NOT the range of $T$.

(c) \[
\ker T = \{(x_1, x_2) \in \mathbb{R}^2 \mid T(x_1, x_2) = (0,0)\} = \{(x_1, x_2) \in \mathbb{R}^2 \mid (x_1 + x_2, -3x_1 - 3x_2) = (0,0)\} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 = 0 \text{ and } -3x_1 - 3x_2 = 0\} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 = 0\} = \{(x_1, -x_1) : x_1 \in \mathbb{R}\} = \text{Span}\{(1, -1)\}\] Special Solution

Therefore $\dim(\ker T) = 1$. $\blacksquare$

2. If $x$ is an eigenvector of $A$ corresponding to $\lambda$, then $Ax = \lambda x$, and $x \neq 0$. Since $P$ is invertible it cannot be the zero matrix, thus $Px \neq 0$. Then we have

\[B(P^{-1}x) = ((P^{-1}AP)P^{-1})x = (P^{-1}A)x = P^{-1}(Ax) = P^{-1}(\lambda x) = \lambda(P^{-1}x)\]

which shows that $P^{-1}x$ is an eigenvector of $B$ corresponding to $\lambda$. $\blacksquare$

3. (a) Call the columns of this matrix $C_1, C_2, C_3,$ and $C_4$.

We notice that $2C_1 + C_2 = C_4$, and thus $\text{Span}\{C_1, C_2, C_3, C_4\} = \text{Span}\{C_1, C_2, C_3\}$. Also, since $C_3 \notin \text{Span}\{C_1, C_2\}$ then $C_3$ will be in the basis of the column space we will find. The only thing left to check is whether $C_1$ and $C_2$ are linearly independent. But this is easy, as their first component is the same. It follows that we have two cases:

(i) When $c = 3$ we get that $C_1 = C_2$ and thus $\{C_1, C_3\}$ is a basis for the column space.

(ii) When $c \neq 3$ we get that $C_1$ and $C_2$ are linearly independent, and thus a basis is given by $\{C_1, C_2, C_3\}$, or any three column vectors in $\mathbb{R}^3$, as these three columns generate the whole space $\mathbb{R}^3$ (column vectors).

A different solution for part (a) follows:

(a) Elimination gives

\[
\begin{bmatrix}
1 & 1 & 2 & 4 \\
0 & c-3 & -4 & -4 \\
0 & 0 & 2 & 2
\end{bmatrix}
\]

which gives two cases: $c = 3$ and $c \neq 3$. If $c \neq 3$, then $c - 3$ is a pivot. Hence,

\[
\begin{bmatrix}
1 & 1 & 2 & 4 \\
0 & c-3 & -4 & -4 \\
0 & 0 & 2 & 2
\end{bmatrix} \rightarrow \begin{bmatrix}
1 & 0 & 0 & 2 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1
\end{bmatrix}
\]
which implies that a basis for the column space $C(A)$ is the first three columns of $A$:

\[
\begin{bmatrix}
1 & 3 & 1 \\
0 & 0 & c \\
0 & 0 & 2
\end{bmatrix}
\]

If $c = 3$, then $c - 3 = 0$, so

\[
\begin{bmatrix}
1 & 1 & 2 & 4 \\
0 & 0 & 0 & 2 \\
0 & 0 & 2 & 2
\end{bmatrix}
\rightarrow
\begin{bmatrix}
1 & 1 & 0 & 2 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

so a basis for the column space is the first and third columns of $A$:

\[
\begin{bmatrix}
1 \\ 3 \\ 0
\end{bmatrix},
\begin{bmatrix}
2 \\ 2 \\ 2
\end{bmatrix}
\]

(b) Since the column space has dimension 2 or 3, depending on the value of $c$, we have to take cases:

(i) If $c \neq 3$, the column space has dimension 3, and thus the nullity must be equal to 1. Solving the homogeneous system gives the basis for the null space $N(A)$ as

\[
\begin{bmatrix}
-2 \\ 0 \\ -1 \\
0 \\ 1
\end{bmatrix}
\]

(ii) Here the nullity should be 2, as the dimension of the column space is 2 as well. Solving the homogeneous system gives the basis for the null space $N(A)$ as

\[
\begin{bmatrix}
-1 \\ -2 \\ 0 \\ -1 \\
1 \\ 0 \\ 1 \\ 1
\end{bmatrix}
\]

(c) Then again, given the two cases that naturally arise in this problem, we must consider two cases here as well. In either case we just look for a particular solution, to later attach to it those vectors in the null space... or, if you prefer, just solve the system that you get when you take the cases.

What is interesting here is that the particular solution is common to both cases:

\[
\mathbf{x}_p = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}
\]

Hence, the complete solutions are:

- $c \neq 3$
  \[
  \begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4
\end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \end{bmatrix}
  \text{ for any scalar } t.
  \]

- $c = 3$
  \[
  \begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4
\end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + s \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \end{bmatrix}
  \text{ for scalars } s \text{ and } t.
  \]

4. We need to first diagonalize $A$. The characteristic equation for $A$, gives

\[
0 = |A - \lambda I| = \lambda^2 + 3\lambda + 2 = (\lambda + 1)(\lambda + 2),
\]
so the eigenvalues of $A$ are -1 and -2.

For $\lambda = -1$: Solve $(A + I)v = 0$ to obtain that a basis for the eigenspace is $\{v_1\} = \left\{ \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$.

For $\lambda = -2$: Solve $(A + 2I)v = 0$ to obtain that a basis for the eigenspace is $\{v_2\} = \left\{ \begin{bmatrix} 1 \\ -2 \end{bmatrix} \right\}$.

We can form the invertible matrix $P = [v_1 \ v_2] = \begin{bmatrix} 1 & 1 \\ -1 & -2 \end{bmatrix}$, and with $D = \begin{bmatrix} -1 & 0 \\ 0 & -2 \end{bmatrix}$ we get $A = PDP^{-1}$. It follows that

$$A^{12} = PD^{12}P^{-1} = \begin{bmatrix} 1 & 1 \\ -1 & -2 \end{bmatrix} \begin{bmatrix} (-1)^{12} & 0 \\ 0 & (-2)^{12} \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -4094 & -4095 \\ 8190 & 8191 \end{bmatrix}.$$
but this is impossible because \( u \notin \text{Span}\{v_1, v_2, \ldots, v_n\} \). Therefore, we can write

\[
\mathbf{w} = d^{-1} \mathbf{u} - d^{-1} c_1 \mathbf{v}_1 - d^{-1} c_2 \mathbf{v}_2 - \cdots - d^{-1} c_n \mathbf{v}_n.
\]

Hence, \( \mathbf{w} \) can be written as a linear combination of \( u, v_1, v_2, \ldots, v_n \), and thus \( \mathbf{w} \) is an element in \( \text{Span}\{u, v_1, v_2, \ldots, v_n\} \).

8. We need first to find a basis for the space \( \text{Span}\{f(t), g(t), h(t)\} \). Since the equation \( \alpha(2) + \beta(-2t - 1) + \gamma(7t^2 - 2t + 7) = 0 \) has only the trivial solution \( \alpha = \beta = \gamma = 0 \), the set \( \{f(t), g(t), h(t)\} \) is linearly independent, and therefore forms a basis for \( \text{Span}\{f(t), g(t), h(t)\} \). So, we will apply the Gram-Schmidt process to the basis \( B = \{f(t), g(t), h(t)\} \).

Let

\[
\begin{align*}
p_1(t) &= f(t) = 2 \\
p_2(t) &= g(t) - \frac{<g, p_1>}{<p_1, p_1>} p_1(t) \\
p_3(t) &= h(t) - \frac{<h, p_1>}{<p_1, p_1>} p_1(t) - \frac{<h, p_2>}{<p_2, p_2>} p_2(t)
\end{align*}
\]

Then we have

\[
\begin{align*}
< g, p_1 > &= (1)(2) + (-1)(2) + (-3)(2) = -6 \\
< p_1, p_1 > &= (2)(2) + (2)(2) + (2)(2) = 12
\end{align*}
\]

and thus \( p_2(t) = -2t \).

Moreover, we have

\[
\begin{align*}
< h, p_1 > &= (16)(2) + (7)(2) + (12)(2) = 70 \\
< h, p_2 > &= (16)(2) + (7)(0) + (12)(-2) = 8 \\
< p_2, p_2 > &= (2)(2) + (0)(0) + (-2)(-2) = 8
\end{align*}
\]

implying that \( p_3(t) = 7t^2 - \frac{14}{3} \). The set \( \{p_1(t), p_2(t), p_3(t)\} \) is an orthogonal basis for the space \( \text{Span}\{f(t), g(t), h(t)\} \).
Part A. Solve five of the following eight problems:

1. Prove that the set
   
   \[ M = \left\{ \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} ; \ m, n \in \mathbb{Z} \right\} \]

   is isomorphic, as a ring, to the ring \( \mathbb{Z}[2] = \{ m + n\sqrt{2} | m, n \in \mathbb{Z} \} \).

2. (a) How many elements of order 7 does the group \( \mathbb{Z}_{21} \oplus \mathbb{Z}_{35} \) have? Justify your answer.
   (b) How many cyclic subgroups of order 7 does the group \( \mathbb{Z}_{21} \oplus \mathbb{Z}_{35} \) have? Justify your answer.

   Note: You may prefer to use the notation \( \mathbb{Z}_{21} \times \mathbb{Z}_{35} \) instead of \( \mathbb{Z}_{21} \oplus \mathbb{Z}_{35} \). You are free to do so.

3. (a) Find all group homomorphisms from \( \mathbb{Z}_{42} \) to \( \mathbb{Z}_{12} \) (give formulas for each). How many homomorphisms are there from \( \mathbb{Z}_{42} \) onto \( \mathbb{Z}_{12} \)?
   (b) Are all the group homomorphisms in part (a) also ring homomorphisms?

4. Let \( G = GL(2, \mathbb{R}) \) and \( H = \{ A \in G ; \ det(A) = 3^k, k \in \mathbb{Z} \} \). Prove that \( H \) is a subgroup of \( G \). Moreover, show that \( H \leq G \).

5. Let \( n \in \mathbb{N} \). Prove that all ideals in \( \mathbb{Z}_n \) are principal.

6. Let \( R \) be a commutative ring with one. Prove that \( R \) is a field if and only if \( \{0\} \) and \( R \) are the only (two-sided) ideals in \( R \).

7. (a) Suppose that \( H \) is a normal subgroup of \( G \) with \( [G : H] = 24 \) and \( |H| = 11 \). If \( x \in G \) and \( x^{11} = e \), prove that \( x \in H \).
   (b) Let \( H = \{(1), (12)(34)\} \). Prove or disprove: \( H \) is normal in \( A_4 \).

8. Let \( G \) be a group. Assume that \( G \) is isomorphic to all its non-trivial subgroups. Prove that \( G \) is isomorphic to either \( \mathbb{Z} \) or \( \mathbb{Z}_p \), for some prime \( p \).

---

Part B is on the back!!!
Part B. Solve five of the following eight problems:

Notation: (a) \( M_n(K) \) is the set of \( n \times n \) matrices with entries in \( K \).
(b) \( P_n \) is the set of all polynomials (with real coefficients) with degree at most \( n \) (including the zero polynomial).

1. Let \( v \) be a fixed vector in \( \mathbb{R}^n \), where \( n > 1 \). Assume that \( M \in M_n(\mathbb{R}) \setminus \{0\} \) is such that \( Mv = 0 \). Prove that there exists a matrix \( N \in M_n(\mathbb{R}) \) such that \((MN)v \neq 0\).

2. Define \( T : M_2(\mathbb{C}) \rightarrow M_2(\mathbb{C}) \) by \( T(A) = A + A^T \).
   (a) Show that \( T \) is a linear transformation.
   (b) Show that the range of \( T \) is the set of all \( B \) in \( M_2(\mathbb{C}) \) with the property that \( B^T = B \).
   (c) Describe the kernel of \( T \).

3. Recall that the trace of a square matrix is the sum of the entries on the main diagonal. Let \( W \) be the subset of \( M_2(\mathbb{R}) \) of matrices with trace equal to 0.
   (a) Show that \( W \) is a subspace of \( M_2(\mathbb{R}) \).
   (b) Let \( S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \right\} \subseteq W \). Show that \( S \) is a basis for \( W \).

4. Let \( V \) be the space \( C[0,1] \) of real-valued continuous functions defined on \([0,1]\), and consider the inner product on \( V \) defined by

\[
\langle f, g \rangle = \int_0^1 f(t)g(t) \, dt.
\]

Let \( W \) be the subspace spanned by the polynomials \( p_1(t) = 1, p_2(t) = 2t - 1, \) and \( p_3(t) = 12t^2 \). Use the Gram-Schmidt process to find an orthogonal basis for \( W \).

5. Define \( T : \mathcal{P}_2 \rightarrow \mathbb{R}^2 \) by \( T(p) = \begin{bmatrix} p(0) \\ p(2) \end{bmatrix} \).
   (a) Show that \( T \) is a linear transformation.
   (b) Find the kernel of \( T \), and a basis for it.
   (c) Find the matrix for \( T \) relative to the standard bases for \( \mathcal{P}_2 \) and \( \mathbb{R}^2 \) respectively.

6. Let \( A \) be a square matrix. Prove or disprove the following statements:
   (a) The matrices \( A \) and \( A^T \) have the same eigenvalues, counting multiplicities.
   (b) If \( A \) is an \( n \times n \) diagonalizable matrix, then each vector in \( \mathbb{R}^n \) can be written as a linear combination of eigenvectors of \( A \).
   (c) If \( A \) is diagonalizable, then the columns of \( A \) are linearly independent.

7. Let \( T : \mathcal{P}_1 \rightarrow \mathcal{P}_1 \) be a linear transformation such that \( T(a + bt) = (−2a + b) + (a + 2b)t \).
   Find the eigenvalues of \( T \). Then choose one of the eigenvalues and find a basis for the corresponding eigenspace.

8. Show that \( B = \{ t - 1, t + 1 \} \) forms a basis for \( \mathcal{P}_1 \), and find the change-of-coordinates (i.e. change of basis) matrix from the standard basis \( C = \{1, t\} \) to the basis \( B \).
Part A.

1. Define \( f : \mathbb{Z}[2] \to M \) by \( f(m + n\sqrt{2}) = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \). We have

\[
\begin{align*}
f((m + n\sqrt{2}) + (r + s\sqrt{2})) &= f((m + r) + (n + s)\sqrt{2}) = \begin{bmatrix} m + r & n + s \\ 2(n + s) & m + r \end{bmatrix} \\
&= \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} + \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} = f(m + \sqrt{2}) + f(r + s\sqrt{2})
\end{align*}
\]

and

\[
\begin{align*}
f((m + n\sqrt{2})(r + s\sqrt{2})) &= f((mr + 2ns) + (ms + nr)\sqrt{2}) = \begin{bmatrix} mr + 2ns & ms + nr \\ 2(ms + nr) & mr + 2ns \end{bmatrix} \\
&= \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} = f(m + \sqrt{2})f(r + s\sqrt{2}).
\end{align*}
\]

Hence, \( f \) is a ring homomorphism.

Since \( \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \) iff \( m = n = 0 \), we have \( \ker f = \{ 0 \} \) and so \( f \) is one-to-one. If \( \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \in M \) then \( m, n \in \mathbb{Z} \), and then \( m + n\sqrt{2} \in \mathbb{Z}[2] \). Moreover,

\[
f(m + n\sqrt{2}) = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix}
\]

and thus \( f \) is onto. Hence \( f \) is an isomorphism of rings.

2. (a) Let \( (a, b) \in \mathbb{Z}_{21} \oplus \mathbb{Z}_{35} \). Then \( |(a, b)| = \text{lcm}(|a|, |b|) \). So, when \( |(a, b)| = 7 \) we have two cases:

Case 1: \(|a| = 7 \) and \(|b| = 1 \) or \(|b| = 7 \). 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 \( b \) (one for \(|b| = 1 \) and six for \(|b| = 7 \)). 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 \( 42 + 6 = 48 \) elements of order 7.

(b) Because each cyclic group of order 7 has six elements of order 7 and no two of the cyclic subgroups can have an element of order 7 in common, there must be \( 48/6 = 8 \) cyclic subgroups of order 7.

3. (a) We know that a homomorphism \( f : \mathbb{Z}_{42} \to \mathbb{Z}_{12} \) is determined by its action on a generator of \( \mathbb{Z}_{42} \). Assume that \( f(1) = a \), for some \( a \in \mathbb{Z}_{12} \). Then \(|a| \) divides \(|\mathbb{Z}_{12}| = 12 \) and \(|\mathbb{Z}_{42}| = 42 \) (why?), so \(|a| \) divides \( \gcd(12, 42) = 6 \).

Case 1: If \(|a| = 1 \), then \( a = 0 \).

Case 2: If \(|a| = 2 \), then \( a = 6 \).

Case 3: If \(|a| = 3 \), then \( a = 4 \) or \( a = 8 \).

Case 4: If \(|a| = 6 \), then \( a = 2 \) or \( a = 10 \).

Notice that if \( f(1) = a \), then \( f(x) = f(x \cdot 1) = xf(1) = xa \), for all \( x \in \mathbb{Z} \), because \( f \) is operation preserving. Therefore, the homomorphisms from \( \mathbb{Z}_{42} \) to \( \mathbb{Z}_{12} \) are:

\[
\begin{align*}
f_1(x) &= 0 \\
f_2(x) &= 6x \\
f_3(x) &= 4x \\
f_4(x) &= 8x \\
f_5(x) &= 2x \\
f_6(x) &= 10x
\end{align*}
\]
None of the above functions are onto, since none of the possible values for $a$ is a generator for $\mathbb{Z}_{42}$. Thus there are no homomorphisms from $\mathbb{Z}_{42}$ onto $\mathbb{Z}_{12}$.

(b) We want to check whether any of the homomorphisms between the (additive) groups $\mathbb{Z}_{42}$ and $\mathbb{Z}_{12}$ found in (a) are ring homomorphisms. If such an $f$ is then

$$a = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = a^2$$

Out of the six possible $a$’s listed above we get

$$0^2 = 0 \quad 6^2 = 0 \neq 6 \quad 4^2 = 4 \quad 8^2 = 4 \neq 8 \quad 2^2 = 4 \neq 2 \quad 10^2 = 4 \neq 10$$

and thus the only candidates to be ring homomorphisms are $f_1(x) = 0$ and $f_3(x) = 4x$. $f_1$ is clearly a homomorphism of rings, and

$$f_3(xy) = 4(xy) = 4^2(xy) = (4x)(4y) = f(x)f(y)$$

which means that $f_3$ is also a homomorphism of rings. \(\square\)

4. Since $\det(A) = 3^k \neq 0$, for all $A \in H$ then $H \subseteq G$. Moreover, $\det(I) = 1 = 3^0$, and thus the identity matrix lives in $H$.

Let $A, B \in H$ then $\det(AB^{-1}) = 3^k$ and $\det(B) = 3^t$, for some $k, t \in \mathbb{Z}$. Then

$$\det(AB^{-1}) = \det(A) \cdot \det(B^{-1}) = \det(A) \cdot \det(B)^{-1} = 3^k \cdot 3^{-t} = 3^{k-t}$$

Since $k-t \in \mathbb{Z}$, then $AB^{-1} \in H$. It follows that $H \leq G$.

In order to show that $H \leq G$ we let $A \in H$ (with $\det(A) = 3^k$) and $B \in G$ (with $\det(B) = n \neq 0$) and we want to show that $BAB^{-1} \in H$. Note that

$$\det(BAB^{-1}) = \det(B) \cdot \det(A) \cdot \det(B^{-1}) = \det(B) \cdot \det(A) \cdot \det(B)^{-1} = n \cdot 3^k \cdot 3^{-1} = 3^k$$

which implies that $BAB^{-1} \in H$. \(\square\)

5. We know that the subgroups of $(\mathbb{Z}_n, +)$ look like $\langle [d] \rangle$, where $d|n$. But

$$\langle [d] \rangle = \{[dk]; k \in \mathbb{Z}\} = \{[dk] | [k] \in \mathbb{Z}_n\} = \{[dk]; [k] \in \mathbb{Z}_n\} = ([d])\mathbb{Z}_n = ([d])$$

where $([d])$ denotes the ideal generated by $[d]$.

Note that we are using that $\mathbb{Z}_n$ is a commutative ring with one to get that $([d])\mathbb{Z}_n = ([d])$.

6. ($\implies$) If $R$ is a field and $I \neq \{0\}$ is an ideal in $R$, then there exists $a \in I, a \neq 0$. Since $R$ is a field, every nonzero element is a unit, and therefore $1 = a^{-1}a \in I$, since $I$ is an ideal. Hence for all $r \in R$ we have $r = r \cdot 1 \in I$, and $I = R$.

($\impliedby$) $R$ is a commutative ring with one, so to show that $R$ is a field we only need to show that all nonzero elements in $R$ are units. Let $0 \neq a \in R$ and consider $I = (a)$, the principal ideal generated by $a$. Note that, since $R$ is a commutative ring with one, then $(a) = Ra$. $I \neq \{0\}$ since $0 \neq a \in I$. If $\{0\}$ and $R$ are the only ideals in $R$, then we must have $I = R$. But $R$ is a ring with one, hence $1 \in I$. In other words, there exists $r \in R$ such that $1 = ra$. Hence $r = a^{-1}$ (using that $R$ is a commutative ring), and thus $a$ is a unit. \(\square\)

7. (a) First note that $(xH)^{11} = x^{11}H = cH = H$, by hypothesis. Hence $|xH|$ divides 11. But since $G/H$ is a group of order 24, we must also have that $|xH|$ divides 24. Since $\gcd(11, 24) = 1$, it must be the case that $|xH| = 1$. That is, $xH = H$. It follows that $x \in H$, as required.

(b) As $(123)H(123)^{-1} = (123)H(132) = \{e, (14)(23)\} \neq H$, then $H$ is not normal in $A_4$. \(\square\)

8. If $G$ is isomorphic to all its non-trivial cyclic subgroups then it must be cyclic, as it would be isomorphic to all its non-trivial cyclic subgroups. Hence,

- If $G$ is infinite we are done, as $G \cong \mathbb{Z}$.
- If $G$ is finite then $G \cong \mathbb{Z}_n$, for some $n$. If $n$ were not prime, then there would be a prime $q$ dividing $n$. Consider $H = \langle \{q\} \rangle$. This is a subgroup of $\mathbb{Z}_n$ of order $n/q$. We get a contradiction because if $G$ were isomorphic to $H$ then $n = n/q$ and that is false. So, $n$ must be prime, and $G$ is isomorphic to $\mathbb{Z}_p$, for some prime $p$. \(\square\)
Part B.

1. Let \( \mathbf{v} \in \mathbb{R}^n \) and \( M \in M_n(\mathbb{R}) \setminus \{0\} \) be such that \( M\mathbf{v} = \mathbf{0} \). Since \( M \neq 0 \) then there is a vector \( \mathbf{w} \) such that \( M\mathbf{w} \neq \mathbf{0} \). Consider \( N \) to be any matrix mapping \( \mathbf{v} \) to \( \mathbf{w} \).

Why does such a matrix exist? One way to think about it is to create two matrices: \( A \) that maps \( \mathbf{v} \) to, let us say, \((1,0,\cdots, 0)\) and \( B \) (invertible) mapping \( \mathbf{w} \) to \((1,0,\cdots, 0)\). Then \( N = B^{-1}A \) would map \( \mathbf{v} \) to \( \mathbf{w} \).

It follows that \( (MN)\mathbf{v} = M(N\mathbf{v}) = M\mathbf{w} \neq \mathbf{0} \).

2. (a) We need to show that \( T \) preserves addition and scalar multiplication of matrices. Let \( A, B \in M_2(\mathbb{C}) \) and \( c \in \mathbb{C} \). Then we have

\[
T(A + B) = (A + B) + (A + B)^T = (A + B) + (A^T + B^T) = (A + A^T) + (B + B^T) = T(A) + T(B)
\]

and

\[
T(cA) = (cA) + (cA)^T = c(A) + c(A^T) = c(A + A^T) = cT(A).
\]

Therefore, \( T \) is a linear transformation.

(b) Let \( B \in M_2(\mathbb{C}) \) such that \( B^T = B \) (i.e. \( B \) is a symmetric matrix). Then consider \( A = \frac{1}{2}B \) and observe that

\[
A + A^T = \frac{1}{2}B + \left( \frac{1}{2}B \right)^T = \frac{1}{2}B + \frac{1}{2}B^T = \frac{1}{2}B + \frac{1}{2}B = B
\]

and thus \( T(A) = B \).

These calculations show that the range of \( T \) contains all matrices in \( M_2(\mathbb{C}) \) such that \( B = B^T \).

Moreover, notice that

\[
T(A)^T = (A + A^T)^T = A^T + (A^T)^T = A^T + A = T(A)
\]

and thus the range of \( T \) is exactly the set of all matrices in \( M_2(\mathbb{C}) \) such that \( B = B^T \).

(c) We have that

\[
\ker T = \{ A \in M_2(\mathbb{C}) : T(A) = 0 \}
\]

\[
= \{ A \in M_2(\mathbb{C}) : A + A^T = 0 \}
\]

\[
= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{C}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}
\]

\[
= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{C}) : \begin{bmatrix} 2a & b + c \\ 2d & c + b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}.
\]

Thus if \( A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \ker T \), then \( 2a = b + c = 2d = 0 \), or equivalently, \( a = d = 0 \) and \( c = -b \), for some \( b \in \mathbb{R} \). Therefore, \( \ker T = \left\{ \begin{bmatrix} 0 & b \\ -b & 0 \end{bmatrix} : b \in \mathbb{C} \right\} \).

\( \square \)

3. (a) Let \( A, B \in W \) and \( c \in \mathbb{R} \). Clearly, \( W \subseteq M_2(\mathbb{R}) \) and \( 0 \in W \). Now using that the trace is an additive function we get

\[
\text{tr}(A - B) = \text{tr}(A) - \text{tr}(B) = 0 - 0 = 0
\]

\[
\text{tr}(cA) = c \text{tr}(A) = c \cdot 0 = 0
\]
implies that $W$ is a subspace of $M_2(\mathbb{R})$.

(b) Since $M_2(\mathbb{R})$ has dimension four and there are matrices in $M_2(\mathbb{R}) \setminus W$ (for instance the identity matrix), then $\dim(W) \leq 3$. Note that $S$ contains three elements, all of them in $W$. Hence, if they were linearly independent then they would be forced to form a basis of $W$. But this is immediate, as

$$
\begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix}
= x \begin{bmatrix}
1 & 0 \\
0 & -1
\end{bmatrix}
+ y \begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}
+ z \begin{bmatrix}
0 & 0 \\
1 & 0
\end{bmatrix}
= \begin{bmatrix}
x & y \\
z & -x
\end{bmatrix}
$$

yields $x = y = z = 0$.

4. Let $q_1 = p_1$, and

$$
\langle p_2, q_1 \rangle = \int_0^1 (2t - 1)(1) \, dt = (t^2 - t)\bigg|_0^1 = 0
$$

So, $p_2$ and $q_1$ are already orthogonal. Hence, $p_2 = q_2$. Now we compute

$$
\langle p_3, q_1 \rangle = \int_0^1 (12t^2)(1) \, dt = (4t^3)\bigg|_0^1 = 4
$$

$$
\langle q_1, q_1 \rangle = \int_0^1 (1)(1) \, dt = t\bigg|_0^1 = 1
$$

$$
\langle p_3, q_2 \rangle = \int_0^1 (12t^2)(2t - 1) \, dt = 2
$$

$$
\langle q_2, q_2 \rangle = \int_0^1 (12t^2) \, dt = \frac{1}{6}(2t - 1)^3\bigg|_0^1 = \frac{1}{3}
$$

Then, the projection of $p_3$ onto $W_2 = \text{span}\{q_1, q_2\}$ is given by

$$
\frac{\langle p_3, q_1 \rangle}{\langle q_1, q_1 \rangle} q_1 + \frac{\langle p_3, q_2 \rangle}{\langle q_2, q_2 \rangle} q_2 = 4 q_1 + \frac{2}{1/3} q_2 = 4 q_1 + 6 q_2
$$

Hence,

$$
q_3 = p_3 - (4 q_1 + 6 q_2)
$$

and thus $q_3(t) = 12 t^2 - 4 - 6(2t - 1) = 12 t^2 - 12 t + 2$. It follows that the orthogonal basis is $\{q_1, q_2, q_3\}$.

5. (a) Let $p, q \in P_2$ and $c \in \mathbb{R}$. Then

$$
T(p + q) = \begin{bmatrix}
(p + q)(0) \\
(p + q)(2)
\end{bmatrix}
= \begin{bmatrix}
p(0) \\
p(2)
\end{bmatrix}
+ \begin{bmatrix}
q(0) \\
q(2)
\end{bmatrix}
= T(p) + T(q)
$$

$$
T(cp) = \begin{bmatrix}
(c p)(0) \\
(c p)(2)
\end{bmatrix}
= \begin{bmatrix}
c(p(0)) \\
c(p(2))
\end{bmatrix}
= c \begin{bmatrix}
p(0) \\
p(2)
\end{bmatrix}
= cT(p).
$$

Hence, $T$ is a linear transformation.

(b) Using the definition of the kernel of a linear transformation, we have:

$$
\text{Ker}(T) = \left\{ p \in P_2 \mid T(p) = \begin{bmatrix}
p(0) \\
p(2)
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix} \right\}
$$

$$
= \left\{ a + bt + ct^2 \in P_2 \mid \begin{bmatrix}
a \\
a + 2b + 4c
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix} \right\}
$$

$$
= \left\{ a + bt + ct^2 \in P_2 \mid a = 0, a + 2b + 4c = 0 \right\}
$$
If \( a = 0 \), the equation \( a + 2b + 4c = 0 \) is equivalent to \( b + 2c = 0 \), or to \( b = -2c \), where \( c \) is free. Therefore, we arrive at:

\[
Ker(T) = \{(-2c)t + ct^2 \mid c \in \mathbb{R}\} = \text{Span}\{-2t + t^2\}
\]

which implies that \(-2t + t^2\) forms a basis for \( Ker(T) \).

(c) The standard basis for \( P_2 \) is \( \{1, t, t^2\} \), thus we need to compute the images under \( T \) of the polynomials \( 1, t \) and \( t^2 \).

\[
T(1) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad T(t) = \begin{bmatrix} 0 \\ 2 \end{bmatrix}, \quad T(t^2) = \begin{bmatrix} 0 \\ 4 \end{bmatrix}
\]

Therefore the matrix for \( T \) relative to the basis \( \{1, t, t^2\} \) for \( P_2 \) and the standard basis for \( \mathbb{R}^2 \) is \( \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 4 \end{bmatrix} \).

\[\square\]

6. (a) True. Matrices \( A \) and \( A^T \) have the same characteristic polynomial, because

\[
det(A^T - \lambda I) = det(A^T - (\lambda I)^T) = det(A - \lambda I)^T = det(A - \lambda I)
\]

and thus the same eigenvalues, counting multiplicities.

(b) True. If \( A \) is an \( n \times n \) diagonalizable matrix, then \( A \) has \( n \) linearly independent eigenvectors \( v_1, \ldots, v_n \) in \( \mathbb{R}^n \). Since \( \dim(\mathbb{R}^n) = n \), the set \( \{v_1, \ldots, v_n\} \) forms a basis for \( \mathbb{R}^n \), and therefore each vector in \( \mathbb{R}^n \) can be written as a linear combination of \( v_1, \ldots, v_n \).

(c) False. If \( A \) is a diagonal matrix with (at least one) 0 on the diagonal then the columns of \( A \) are not linearly independent (since a set of vectors containing the zero vector is linearly dependent).

\[\square\]

7. We find first \([T]_B\), the matrix of \( T \) relative to the standard basis \( B = \{1, t\} \) for \( P_1 \). Since \( T(1) = -2 + t \) and \( T(t) = 1 + 2t \), the \( B \)-matrix of \( T \) has the following form:

\[
[T]_B = \begin{bmatrix} -2 & 1 \\ 1 & 2 \end{bmatrix}
\]

The eigenvalues of \( T \) are exactly the eigenvalues of the matrix \( A = [T]_B \). The characteristic polynomial of \( A \) is \( \chi_A = \lambda^2 - 5 \), thus the eigenvalues of \( A \) (and hence the eigenvalues of \( T \)) are \( \lambda = \pm \sqrt{5} \).

For \( \lambda = \sqrt{5} \): \( A - \sqrt{5}I = \begin{bmatrix} -2 - \sqrt{5} & 1 \\ 1 & 2 - \sqrt{5} \end{bmatrix} \) and the equation \((A - \sqrt{5}I)x = 0\) amounts to

\[
(-2 - \sqrt{5})x_1 + x_2 = 0, \quad x_1 + (2 - \sqrt{5})x_2 = 0
\]

Observe that these two equations are equivalent.

So, \( x_2 = (2 + \sqrt{5})x_1 \), and \( x_1 \) free. The general solution to the equation \((A - \sqrt{5}I)x = 0\) is \( x = x_1 \begin{bmatrix} 1 \\ 2 + \sqrt{5} \end{bmatrix} \), with \( x_1 \in \mathbb{R} \).

This tells us that the eigenspace \( V_{\lambda = \sqrt{5}} \) is 1-dimensional, and that if \( \{p(t)\} \) is a basis for \( V_{\lambda = \sqrt{5}} \), then the \( B \)-coordinate vector of \( p(t) \) is \([p(t)]_B = \begin{bmatrix} 1 \\ 2 + \sqrt{5} \end{bmatrix} \).

Therefore, \( \{p(t) = 1 + (2 + \sqrt{5})t\} \) is a basis for the eigenspace \( V_{\lambda = \sqrt{5}} \) corresponding to the eigenvalue \( \lambda = \sqrt{5} \).

The computations for \( \lambda = -\sqrt{5} \) are similar. \(\square\)
8. We will denote the change-of-coordinates matrix from the standard basis $C$ to the basis $B$ by $P_{B \leftarrow C}$.

The set $B$ contains 2 vectors, and $\dim \mathcal{P}_1 = 2$, thus to show that $B$ forms a basis for $\mathcal{P}_1$ it suffices to show that it is a linearly independent set.

If $a(t - 1) + b(t + 1) = 0 = 0t + 1$, for some scalars $a$ and $b$, then $a + b = 0$ and $-a + b = 0$. Then $a = 0 = b$, implying that $B$ is linearly independent and, therefore, a basis for $\mathcal{P}_1$.

Recall that the change-of-coordinates matrix from the basis $C = \{1, t\}$ to the basis $B = \{t - 1, t + 1\}$ is given by $P_{B \leftarrow C} = [ [1]_B \ [t]_B ]$, so we need to find the $B$-coordinate vectors of the polynomials/vectors contained in the basis $C$.

Since $1 = -\frac{1}{2}(t - 1) + \frac{1}{2}(t + 1)$ we have $[1]_B = \begin{bmatrix} -1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{bmatrix}$.

Similarly, since $t = \frac{1}{2}(t - 1) + \frac{1}{2}(t + 1)$, it implies that $[t]_B = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$.

Then $P_{B \leftarrow C} = [ [1]_B \ [t]_B ] = \begin{bmatrix} -1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$.
Part A. Solve five of the following eight problems:

1. Let $G$ and $H$ be groups.
   (a) Prove that $S(G, H) = \{ f : G \to H; \text{ } f \text{ is a function} \}$ is a group with the operation $*$ defined by
   $$(f * g)(x) = f(x) * g(x)$$
   for all $x \in G$, where $*$ is the operation in $H$.
   (b) Prove that $S(G, H)$ is abelian if and only if $H$ is abelian.

2. (a) Can there be a group homomorphism from $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ onto $\mathbb{Z}_{12}$?
   (b) Can there be a group homomorphism from $\mathbb{Z}_{81}$ onto $\mathbb{Z}_3 \oplus \mathbb{Z}_3$?

3. (a) Let $a, b$ and $c$ be elements of a commutative ring with unity, and suppose that $a$ is a unit. Prove that $b$ divides $c$ in this ring if and only if $ab$ divides $c$ in this ring.
   (b) Let $a$ belong to a ring $R$. Let $S = \{ x \in R \mid ax = 0 \}$. Show that $S$ is a subring of $R$.

4. Let $G, H$ be groups and $\phi : G \to H$ be a homomorphism.
   (a) Prove that $\phi(g^i) = \phi(g)^i$, for all $i \in \mathbb{Z}$.
   (b) Show that if $\phi$ is an isomorphism and $G$ is cyclic, then $H$ is cyclic.

5. Prove the following claims for permutations in $S_n$.
   (a) $(a_1 a_2 \cdots a_k) = (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k)$, where $a_1, a_2, \ldots, a_k$ are distinct.
   Conclude that every permutation is the product of transpositions.
   (b) Any permutation can be written as a product of the transpositions $(12), (13), \cdots, (1n)$.

6. Let $S = \mathbb{R}\{ -1 \}$. Define $*$ on $S$ by $a * b = a + b + ab$. Show that $S$ is a group.

7. Show, in full detail, that $I = \{ p(x) \in \mathbb{R}[x]; \text{ } p(0) = p(1) = 0 \}$ is a principal ideal of $\mathbb{R}[x]$.

8. Let $d$ be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Q} \}$ is a field.

Part B is on the back!!!
Part B. Solve **five** of the following eight problems:

1. Let $\mathbb{P}_2$ be the vector space of real polynomials of degree 2 or less. Consider the basis $B = \{1, x, x^2\}$ and $B' = \{1, x + 1, x^2 + x + 1\}$ for $\mathbb{P}_2$.
   (a) Find the transition matrix from $B$ to $B'$.
   (b) Let $p(x) = 3 - x + 2x^2 \in \mathbb{P}_2$. Find the coordinates of $p(x)$ relative to $B'$.

2. Find an orthonormal basis for the subspace of $\mathbb{R}^4$ spanned by the vectors $u_1 = (0, 0, -1, 0)$, $u_2 = (1, 3, 0, 0)$, and $u_3 = (1, 0, 1, 1)$.

3. Find a square root of the matrix
   \[
   A = \begin{bmatrix}
   1 & 3 & -3 \\
   0 & 4 & 5 \\
   0 & 0 & 9
   \end{bmatrix}.
   \]

4. Let $V$ be an $n$-dimensional vector space and $W$ a subspace of $V$. Let $B' = \{b_1, b_2, \ldots, b_m\}$ be a basis for $W$. Prove that there exist vectors $b_{m+1}, b_{m+1}, \ldots, b_n$ in $V$ such that $B = \{b_1, b_2, \ldots, b_m, b_{m+1}, \ldots, b_n\}$ is a basis for $V$.

5. Gaussian elimination changes $Ax = b$ to a reduced $Rx = d$. The complete solution is
   \[
   x = \begin{bmatrix}
   4 \\
   0 \\
   0
   \end{bmatrix} + s \begin{bmatrix}
   2 \\
   1 \\
   0
   \end{bmatrix} + t \begin{bmatrix}
   5 \\
   0 \\
   1
   \end{bmatrix}.
   \]
   (a) What is the reduced row echelon form matrix $R$?
   (b) What is $d$?

6. Consider the linear transformation with matrix
   \[
   A = \begin{bmatrix}
   1 & 0 & -3 & 0 \\
   0 & 1 & 4 & 0 \\
   0 & 0 & 0 & 1
   \end{bmatrix}.
   \]
   Find a basis for the kernel and a basis for the image of the transformation.

7. Let $A$ be a nonzero $n \times n$ skew-symmetric real matrix.
   (a) Show that if $n$ is odd, then $A$ is not invertible.
   (b) What happens if $n$ is even? Justify your answer.

8. (a) Show that if $v$ is an eigenvector of the matrix product $AB$ and $Bv \neq 0$, then $Bv$ is an eigenvector of $BA$.
   (b) Suppose that $v$ is an eigenvector of $A$ corresponding to an eigenvalue $\lambda$. Show that $v$ is an eigenvector of $5I - 3A + A^2$, where $I$ is the identity matrix of the same size as $A$. What is the corresponding eigenvalue?
Part A. Solve five of the following eight problems:

1. Let $G$ and $H$ be groups.
   
   (a) Prove that
   
   $$S(G, H) = \{ f : G \to H ; \ f \text{ is a function} \}$$
   
   is a group with the operation $\ast$ defined by
   
   $$(f \ast g)(x) = f(x) \ast g(x)$$
   
   for all $x \in G$, where $\ast$ is the operation in $H$.
   
   (b) Prove that $S(G, H)$ is abelian if and only if $H$ is abelian.
   
   Solution.
   
   (a) Since this operation is weird, then we need to check everything about this group (to be).
   
   (i) Closure of $\ast$ in $S(G, H)$: We take $f, g \in S(G, H)$, we want to show that $f \ast g$ is an element of $S(G, H)$.
   
   First of all, note that since $f, g \in S(G, H)$ and $x \in G$ then both $f(x)$ and $g(x)$ are in $H$. Moreover $\ast$ being closed in $H$ forces $f(x) \ast g(x) \in H$. Hence, $(f \ast g)(x) \in H$ for all $x \in G$. So, $f \ast g$ takes elements in $G$ to elements in $H$, but is it a function? We need to check that images are unique! But this is immediate, as both $f$ and $g$ are functions, and thus $f(x)$ and $g(x)$ are uniquely defined... and also is their product. It follows that $S(G, H)$ is closed under $\ast$.
   
   (ii) Associativity: Let $f, g, h \in S(G, H)$, then for any $x \in G$ we get
   
   $$[f \ast (g \ast h)](x) = f(x) \ast (g \ast h)(x) = f(x) \ast [g(x) \ast h(x)]$$
   
   but now using that $\ast$ is associative in $H$ we get
   
   $$f(x) \ast [g(x) \ast h(x)] = [f(x) \ast g(x)] \ast h(x)$$
   
   which is $[(f \ast g) \ast h](x)$. Done.
   
   (iii) Identity? Let $f \in S(G, H)$ and let $e$ be the constant function $e(x) = e_H$, where $e_H$ is the identity of $H$. Note that
   
   $$(f \ast e)(x) = f(x) \ast e(x) = f(x) \ast e_H = f(x)$$
   
   for all $x \in G$, and thus $f \ast e = f$. Similarly, $e \ast f = f$. Hence, $e$ is the identity of $S(G, H)$.
   
   (iv) Inverses? Let $f \in S(G, H)$. We want to find $g \in S(G, H)$ such that $f \ast g = e$. Consider $g(x) = f(x)^{-1}$, where the inverse is taken in $H$. Then,
   
   $$(f \ast g)(x) = f(x) \ast g(x) = f(x) \ast f(x)^{-1} = e_H$$
   
   and thus $f \ast g = e$. Done.
   
   (b) This group is Abelian if $H$ is Abelian, as
   
   $$(f \ast g)(x) = f(x) \ast g(x) = g(x) \ast f(x) = (g \ast f)(x)$$
   
   for all $x \in G$.
   
   If $H$ is non-Abelian, then there are elements $a, b \in H$ such that $a \ast b \neq b \ast a$. Then, we define the constant functions $f(x) = a$ and $g(x) = b$, which are clearly in $S(G, H)$ and do not commute. Hence, $S(G, H)$ is Abelian if and only if $H$ is Abelian.

2. (a) Can there be a group homomorphism from $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ onto $\mathbb{Z}_{12}$?
(b) Can there be a group homomorphism from $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ onto $\mathbb{Z}_3 \oplus \mathbb{Z}_3$?

Solution.

(a) No. The largest possible order of an element in $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ is 6. But $\mathbb{Z}_{12}$ has an element of order 12 (any generator would do). Since the order of $\psi(x)$ divides the order of $x$, for all $x \in \mathbb{Z}_6 \oplus \mathbb{Z}_6$ then the largest order of an image under $\psi$ is 6. Hence, the elements of order 12 is $\mathbb{Z}_{12}$ are not in the range of $\psi$.

(b) No. The homomorphic image of a cyclic group is cyclic. Having an onto homomorphism from $\mathbb{Z}_{3} \to \mathbb{Z}_3 \oplus \mathbb{Z}_3$ would imply $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ is cyclic. A contradiction.

3. (a) Let $a, b$ and $c$ be elements of a commutative ring with unity, and suppose that $a$ is a unit. Prove that $b$ divides $c$ in this ring if and only if $ab$ divides $c$ in this ring.

(b) Let $a$ belong to a ring $R$. Let $S = \{ x \in R \mid ax = 0 \}$. Show that $S$ is a subring of $R$.

Solution.

(a) Let $R$ be a commutative ring with unity 1, and let $a$ be a unit in $R$.

Suppose that $b|c$ for some $b, c \in R$; that is, $c = br$ for some $r \in R$. Then $c = (a^{-1}a)(br) = (ab)(a^{-1}r)$ (we used here that $R$ is commutative, that $a^{-1}$ exists in $R$ and that multiplication is associative is a ring). But $R$ is closed under multiplication, thus $a^{-1}r \in R$, and then $ab|c$, as desired.

Conversely, suppose that $ab|c$ for some $b, c \in R$; that is $c = (ab)s$ for some $s \in R$. Since $R$ is commutative, it implies that $c = b(as)$, thus $b|c$ (since $as \in R$).

(b) First note that $0 \in S$ (since $a0 = 0$), thus $S \neq \emptyset$.

Let $x, y \in S$. Then $ax = 0 = ay$, and we have:

$$a(x - y) = ax - ay = 0 - 0 = 0$$

and

$$a(xy) = (ax)y = 0y = 0$$

thus $x - y \in S$ and $xy \in S$. Then by the Subring Test, $S$ is a subring of $R$.

4. Let $G, H$ be groups and $\phi : G \to H$ be a homomorphism.

(a) Prove that $\phi(g^i) = \phi(g)^i$, for all $i \in \mathbb{Z}$.

(b) Show that if $\phi$ is an isomorphism and $G$ is cyclic, then $H$ is cyclic.

Solution.

(a) For $i$ positive we get that $\phi(g^i) = \phi(g^{i-1}g) = \phi(g^{i-1})\phi(g)$. So, if we knew that $\phi(g^{i-1}) = \phi(g)^{i-1}$ then we would be done, as

$$\phi(g^i) = \phi(g^{i-1})\phi(g) = \phi(g)^{i-1}\phi(g) = \phi(g)^i$$

Note that we have just set an induction argument. That is, proving the $i$-case by assuming the $(i - 1)$-case. Since the case $i = 2$ holds trivially, then the induction is done.

For $i$ negative, let us first look at $\phi(g^{-1}) = \phi(g)^{-1}$. Then putting this case together with the positive $i$ case above will solve the case for all negative $i$'s.

Recall that $\phi(e) = e$. Then, $e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, which means that $\phi(g^{-1})$ is the inverse of $\phi(g)$. Done.

Now let us consider $-i$ for $i$ positive. We need to show that $\phi(g^{-i}) = \phi(g)^{-i}$:

$$\phi(g^{-i}) = \phi((g^i)^{-1}) = \phi(g^i)^{-1} = (\phi(g)^i)^{-1} = \phi(g)^{-i}$$

The case $i = 0$ is trivial.

(b) Assume that $G = \langle g \rangle$. We know, from part (a) that $\phi(g^i) = \phi(g)^i$. Since every element in the domain of $\phi$ looks like $g^i$, for some $i \in \mathbb{Z}$, then every element in the image of $G$ must look like $\phi(g)^i$. But since $\phi$ is onto then every element in $H$ looks like $\phi(g)^i$. It follows that $\phi(g)$ generates $H$. 
5. Prove the following claims for permutations in \( S_n \).

(a) \((a_1a_2 \cdots a_k) = (a_1a_k) \cdots (a_1a_3)(a_1a_2) = (a_1a_2)(a_2a_3) \cdots (a_{k-1}a_k).\)

Conclude that every permutation is the product of transpositions.

(b) Any permutation can be written as a product of the transpositions \((12), (13), \cdots, (1n)\).

Solution.

(a) Consider the functions \( \sigma = (a_1a_2 \cdots a_k) \) and \( \tau = (a_1a_k) \cdots (a_1a_3)(a_1a_2) \). We want to show \( \sigma = \tau \), so we need to show \( \sigma(x) = \tau(x) \), for all \( x \in \{1, 2, 3, \cdots, n\} \).

If \( x = a_i \) for some \( i \), then \( \sigma(a_i) = a_{i+1 \mod k} \). On the other hand, we have three cases:

(i) If \( x = a_1 \) then \( \tau(a_1) = a_2 \), as \( a_2 \) only appears in the far-most right transposition only. This is consistent with having \( \sigma(a_1) = a_2 \).

(ii) If \( x = a_k \) then \( \tau(a_k) = a_1 \), as \( a_k \) only appears in the far-most left transposition only. This is consistent with having \( \sigma(a_k) = a_1 \).

(iii) If \( x \neq a_1, a_k \) then \( a_i \) appears exactly once in the transpositions of \( \tau \). Hence, \( a_i \) will be fixed by whatever is to the right of \( (a_1a_k) \cdots (a_1a_{i+1})(a_1a_1) \) (in the product of transpositions of \( \tau \)). Now it is easy to see that \( a_i \) will be first moved to \( a_1 \) and then to \( a_{i+1} \). Since \( a_{i+1} \) does not appear anymore in this product then \( \tau(a_i) = a_{i+1} \), which is consistent with what \( \sigma \) does.

If \( x \neq a_i \) for all \( i \) then both \( \sigma \) and \( \tau \) fix this element.

Now consider the functions \( \sigma = (a_1a_2 \cdots a_k) \) and \( \tau = (a_1a_2)(a_2a_3) \cdots (a_{k-1}a_k) \). We want to show \( \sigma = \tau \), so we need to show \( \sigma(x) = \tau(x) \), for all \( x \in \{1, 2, 3, \cdots, n\} \).

If \( x = a_i \) for some \( i \), then \( \sigma(a_i) = a_{i+1 \mod k} \). On the other hand, we notice that every \( a_i \neq a_1, a_k \) appears exactly two cycles in \( \tau \). Hence, we need to take cases again:

(I) If \( x = a_1 \) then \( \tau(a_1) = a_2 \), as only the cycle \((a_1a_2)a_{2a_3} \cdots a_{k-1}a_k\) affects \( a_1 \). We are done because \( \sigma(a_1) = a_2 \).

(II) If \( x = a_k \), then the first transposition on the right sends \( a_k \) to \( a_{k-1} \), but then the next one sends \( a_{k-1} \) to \( a_{k-2} \), and so on, until reaching \( a_1 \). It follows that \( \tau(a_k) = a_1 \), which is exactly what \( \sigma \) does to \( a_k \).

(III) If \( x \neq a_1, a_k \) then the first cycle (on the right) that moves \( a_i \) is \((a_1a_{i+1})\), which sends \( a_i \) to \( a_{i+1} \). At this point there are no \( a_{i+1} \)'s on the cycles to the left of \((a_1a_{i+1})\), and thus \( \tau(a_i) = a_{i+1} \). Just like \( \sigma \).

Since every permutation is a product of cycles, and each cycle is a product of transpositions, then it follows that each permutation is a product of transpositions.

(b) If we can get all transpositions out of products of \((12), (13), \cdots, (1n)\) then, by part (a), we would be done.

We already have all transposition of the form \((ab)\), so let us consider \((ab)\), where \( a \) and \( b \) are both different from \( 1 \) and, of course \( a \neq b \). But that is easy, as

\[
(1a)(1b)(1a) = (ab)
\]

6. Let \( S = \mathbb{R} \setminus \{-1\} \). Define * on \( S \) by \( a * b = a + b + ab \). Show that \( S \) is a group.

Solution. See problem 6 in Spring ’08 exam and problem 1 in spring ’11 exam.

7. Show, in full detail, that \( I = \{p(x) \in \mathbb{R}[x] \mid p(0) = p(1) = 0\} \) is a principal ideal of \( \mathbb{R}[x] \).

Solution. Let \( p(x) \in \mathbb{R}[x] \). The factor theorem says that if \( p(\alpha) = 0 \), for some \( \alpha \in \mathbb{R} \) then \( p(x) = (x - \alpha)q(x) \), for some \( q(x) \in \mathbb{R}[x] \). Hence, using this theorem twice we can re-write \( I \) as

\[
I = \{p(x) \in \mathbb{R}[x] \mid p(x) = x(x-1)r(x), \text{ for some } r(x) \in \mathbb{R}[x]\}
\]

which is the set of all multiples (in \( \mathbb{R}[x] \)) of the polynomial \( t(x) = x(x-1) \). It follows that \( I \) is the principal ideal of \( \mathbb{R}[x] \) generated by \( t(x) = x(x-1) \), which is most of the times denoted \( t(x)\mathbb{R}[x] \).
8. Let \( d \) be a positive integer. Prove that \( \mathbb{Q}[\sqrt{d}] = \{ a + b\sqrt{d} | a, b \in \mathbb{Q} \} \) is a field.

**Solution.** If \( \sqrt{d} \in \mathbb{Q} \), then \( \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q} \) (by closure of \( \mathbb{Q} \)). On the other hand, if considering the elements of \( \mathbb{Q}[\sqrt{d}] \) with \( b = 0 \) we get \( \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{d}] \). It follows that, in this case, \( \mathbb{Q} = \mathbb{Q}[\sqrt{d}] \).

For \( \sqrt{d} \not\in \mathbb{Q} \). It suffices to show that \( \mathbb{Q}[\sqrt{d}] \) is a subfield of \( \mathbb{R} \). First we observe that

\[
0 = 0 + 0 \cdot d \in \mathbb{Q}[\sqrt{d}],
\]

so \( \mathbb{Q}[\sqrt{d}] \neq \emptyset \).

Let \( a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \), thus \( a_1, a_2, b_1, b_2 \in \mathbb{Q} \). Then

\[
(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}].
\]

Assume that \( a_2 + b_2\sqrt{d} \neq 0 \), i.e., \( a_2 \neq 0 \) and \( b_2 \neq 0 \). Then we observe that

\[
(a_2 + b_2\sqrt{d})^{-1} = \frac{1}{a_2 + b_2\sqrt{d}} = \frac{a_2 - b_2\sqrt{d}}{a_2^2 - db_2^2} = \frac{a_2}{a_2^2 - db_2^2} - \frac{b_2}{a_2^2 - db_2^2}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]
\]

since \( a_2^2 - db_2^2 \neq 0 \) (here using that \( d \) is not a square) and \( \frac{a_2}{a_2^2 - db_2^2}, \frac{-b_2}{a_2^2 - db_2^2} \in \mathbb{Q} \).

Then we have

\[
(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})^{-1} = (a_1 + b_1\sqrt{d}) \left( \frac{a_2}{a_2^2 - db_2^2} - \frac{b_2}{a_2^2 - db_2^2}\sqrt{d} \right)
\]

\[
= \frac{a_1a_2 - b_1b_2d}{a_2^2 - db_2^2} + \frac{-a_1b_2 + b_1a_2}{a_2^2 - db_2^2}\sqrt{d} \in \mathbb{Q}[\sqrt{d}].
\]

Then, by the subfield test, \( \mathbb{Q}[\sqrt{d}] \) is a subfield of \( \mathbb{R} \). Done.

---

**Part B is on the back!!!**
Part B. Solve five of the following eight problems:

1. Let $P_2$ be the vector space of real polynomials of degree 2 or less. Consider the basis $B = \{1, x, x^2\}$ and $B' = \{1, x + 1, x^2 + x + 1\}$ for $P_2$.
   (a) Find the transition matrix from $B$ to $B'$.
   (b) Let $p(x) = 3 - x + 2x^2 \in P_2$. Find the coordinates of $p(x)$ relative to $B'$.

Solution.
(a) To find the first column vector of the transition matrix, we must find scalars $a_1, a_2$ and $a_3$ such that

$$a_1(1) + a_2(x + 1) + a_3(x^2 + x + 1) = 1.$$ 

By inspection we see that the solution is $a_1 = 1, a_2 = 0, a_3 = 0$. Therefore,

$$[1]_{B'} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$ 

The second and third column vectors of the transition matrix can be found by solving the equations

$$b_1(1) + b_2(x + 1) + b_3(x^2 + x + 1) = x$$

and

$$c_1(1) + c_2(x + 1) + c_3(x^2 + x + 1) = x^2,$$

respectively. The solutions are given by $b_1 = -1, b_2 = 1, b_3 = 0$, and $c_1 = 0, c_2 = -1, c_3 = 1$. Hence, the transition matrix is

$$P_{B' \leftarrow B} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$ 

Remark: This can also be done by finding the inverse of $P_{B' \leftarrow B} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, which is obtained by ‘hanging’ the coordinates of the vectors $\{1, 1 + x, 1 + x + x^2\}$ in the standard basis.

(b) The coordinate vector of $p(x) = 3 - x + 2x^2$ relative to $B$ is given by

$$[p(x)]_B = \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix},$$

and therefore

$$[p(x)]_{B'} = P_{B' \leftarrow B}[p(x)]_B = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} -3 \\ 4 \end{bmatrix}$$

is the coordinate vector of $p(x) = 3 - x + 2x^2$ relative to $B'$.

Notice also that $3 - x + 2x^2 = 4(1) - 3(x + 1) + 2(x^2 + x + 1)$.

2. Find an orthonormal basis for the subspace of $\mathbb{R}^4$ spanned by the vectors $u_1 = (0, 0, -1, 0)$, $u_2 = (1, 3, 0, 0)$, and $u_3 = (1, 0, 1, 1)$.

Solution. Using the Gram-Schmidt process, we have that $v_1, v_2, v_3$ is an orthogonal basis, where $v_1 = u_1 = (0, 0, -1, 0)$, $v_2 = u_2 = (1, 3, 0, 0)$ (since $u_1 \cdot u_2 = 0$), and $v_3 = (1, 0, 1, 1) - \frac{1}{10}(0, 0, -1, 0) - \frac{1}{10}(1, 3, 0, 0) = \frac{9}{10}, -\frac{3}{10}, 0, 1)$.

We have $|v_1| = 1$, $|v_2| = \sqrt{10}$, and $|v_3| = \sqrt{3}$. Therefore an orthonormal basis is

$$\{(0, 0, -1, 0), \frac{1}{\sqrt{10}}(1, 3, 0, 0), \frac{3}{\sqrt{30}}, -\frac{3}{\sqrt{30}}, 0, 1\}.$$
3. Find a square root of the matrix
\[
A = \begin{bmatrix} 1 & 3 & -3 \\ 0 & 4 & 5 \\ 0 & 0 & 9 \end{bmatrix}.
\]

**Solution.** Since \( A \) is upper triangular, its eigenvalues are its diagonal entries, and \( A \) can thus be diagonalized (since it has distinct eigenvalues). Thus, we will have \( S^{-1}AS = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 9 \end{bmatrix} \), where \( S \) is a matrix whose columns are eigenvectors of \( A \) for the respective eigenvalues. The matrix \( B = S \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} S^{-1} \) will then be the square root of \( A \). Carrying out the computations, one obtains
\[
S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad S^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{giving } B = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{bmatrix}.
\]

**Remark:** Another approach to this problem would be to assume that a square root of \( A \), call it \( B \), is upper triangular (not so crazy to assume, as these matrices form a subring of \( M_3(\mathbb{C}) \)). Since \( \det(A) = 36 \) then \( \det(B) = 6 \). It follows that
\[
B = \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & 6/(ad) \end{bmatrix}.
\]
Easy computations show that \( a = 1 \) and \( d = 2 \). After that, all other values follow easily.

4. Let \( V \) be an \( n \)-dimensional vector space and \( W \) a subspace of \( V \). Let \( B' = \{b_1, b_2, \ldots, b_m\} \) be a basis for \( W \). Prove that there exist vectors \( b_{m+1}, b_{m+1}, \ldots, b_n \) in \( V \) such that \( B = \{b_1, b_2, \ldots, b_m, b_{m+1}, \ldots, b_n\} \) is a basis for \( V \).

**Solution.** Since \( V \) is \( n \)-dimensional, there exist a linearly independent set \( \{v_1, v_2, \ldots, v_n\} \) that spans \( V \). We wish to add some of the \( v_1, v_2, \ldots, v_n \) to \( B' \) to form a basis of \( V \). If \( v_1 \in \text{span}(B') \), then let \( S = B' \); otherwise, set \( S = \{b_1, b_2, \ldots, b_m, v_1\} \). Do this for each of the vectors \( v_2, v_3, \ldots, v_n \) (i.e., if \( v_k \in S \), then leave \( S \) unchanged; otherwise, add \( v_k \) to \( S \)). After each step, the set \( S \) is still linearly independent, since \( v_k \) was only added to the set if \( v_k \) was not in the span of the previous set of vectors. After \( n \) steps, \( v_k \in \text{span}(S) \) for all \( k = 1, 2, \ldots, n \). Since \( \{v_1, v_2, \ldots, v_n\} \) spanned \( V \), \( S \) spans \( V \), and thus, \( S \) is a basis for \( V \). So, letting \( b_{m+1}, b_{m+1}, \ldots, b_n \) be equal to the vectors from \( \{v_1, v_2, \ldots, v_n\} \) that were added to \( S \) and defining \( B = S \), we are done.

5. Gaussian elimination changes \( Ax = b \) to a reduced \( Rx = d \). The complete solution is
\[
x = \begin{bmatrix} 4 \\ 0 \\ 0 \end{bmatrix} + s \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 5 \\ 0 \\ 1 \end{bmatrix}.
\]

(a) What is the reduced row echelon form matrix \( R \)?
(b) What is \( d \)?

**Solution.** Since \( R \) is in reduced row echelon form, we must have
\[
d = \begin{bmatrix} 4 \\ 0 \\ 0 \end{bmatrix}.
\]
The other two vectors provide solutions to the homogeneous system, and show that \( R \) has rank 1. Since \( R \) is in reduced row echelon form, the bottom two rows must be all 0, and the top row must be orthogonal to the vectors
\[
\begin{bmatrix}
2 \\
1 \\
0
\end{bmatrix}
\quad \begin{bmatrix}
5 \\
0 \\
1
\end{bmatrix}
\]
A few computations show that this vector could be \([1 \ -2 \ -5]^T\). Hence,
\[
R = \begin{bmatrix}
1 & -2 & -5 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}.
\]

6. Consider the linear transformation with matrix
\[
A = \begin{bmatrix}
1 & 0 & -3 & 0 \\
0 & 1 & 4 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}.
\]
Find a basis for the kernel and a basis for the image of the transformation.

**Solution.** Set \( Ax = 0 \). Then the solution space is \( \left\{ \begin{bmatrix} 3z \\ -4z \\ z \\ 0 \end{bmatrix} \mid z \in \mathbb{R} \right\} \). Therefore it is of dimension 1, and a basis is \( \left\{ \begin{bmatrix} 3 \\ -4 \\ 1 \\ 0 \end{bmatrix} \right\} \).

Since \( A \) is \( 3 \times 4 \), the image is a subspace of \( \mathbb{R}^3 \). Moreover, the dimension of the image is 3 since the dimension of the kernel is 1. A 3-dimensional subspace of \( \mathbb{R}^3 \) must be \( \mathbb{R}^3 \) itself, so we may use the standard basis \( \{[100]^T, [010]^T, [001]^T \} \).

7. Let \( A \) be a nonzero \( n \times n \) skew-symmetric matrix.

   (a) Show that if \( n \) is odd, then \( A \) is not invertible.

   (b) What happens if \( n \) is even? Justify your answer.

**Solution.**

(a) Since the matrix \(-A\) is obtained from \( A \) by multiplying each of the rows of \( A \) by \(-1\), and there are an odd number of rows, \( \det(-A) = (-1)^n \det(A) = -\det(A) \). Since \( A \) is skew-symmetric, \( \det(A) = \det(A^T) = \det(-A) = -\det(A) \). Thus, \( \det(A) = 0 \), and \( A \) is not invertible.

(b) If \( n \) is even, then it could go either way. For example, the matrix
\[
A = \begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}
\]

is a \( 2 \times 2 \) skew-symmetric matrix that is invertible. However, the matrix
\[
A = \begin{bmatrix}
0 & 1 & 0 & 1 \\
-1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0
\end{bmatrix}
\]
is skew-symmetric, but is clearly not invertible.
8. (a) Show that if \( v \) is an eigenvector of the matrix product \( AB \) and \( Bv \neq 0 \), then \( Bv \) is an eigenvector of \( BA \).

(b) Suppose that \( v \) is an eigenvector of \( A \) corresponding to an eigenvalue \( \lambda \). Show that \( v \) is an eigenvector of \( 5I - 3A + A^2 \), where \( I \) is the identity matrix of the same size as \( A \). What is the corresponding eigenvalue?

Solution.

(a) Suppose that \( Bv \neq 0 \) and \( ABv = \lambda v \) for some \( \lambda \in \mathbb{R} \). Then \( A(Bv) = \lambda v \). Left-multiply each side by \( B \), and obtain \( BA(Bv) = B(\lambda v) = \lambda (Bv) \). This equation says that \( Bv \) is an eigenvector of \( BA \), because \( Bv \neq 0 \).

(b) Suppose that \( Av = \lambda v \), with \( v \neq 0 \). Then

\[
(5I - 3A + A^2)v = 5v - 3Av + A(Av) \\
= 5v - 3\lambda v + \lambda^2 v \\
= (5 - 3\lambda + \lambda^2)v.
\]

Hence \( v \) is an eigenvector of \( 5I - 3A + A^2 \) with eigenvalue \( 5 - 3\lambda + \lambda^2 \).
Part A. Solve five of the following eight problems:

1. Let $G = \{x \in \mathbb{R} \mid x \neq -1\}$. For $x, y \in G$ let $x \ast y = x + y + xy$. Prove that $\ast$ is a binary operation on $G$ and that $(G, \ast)$ is a group.

2. Consider the group $S_n$ of permutations on $n$ elements ($n \geq 3$), and let $A_n$ denote the set of even permutations in $S_n$. Prove that $A_n$ is a normal subgroup of $S_n$.

3. Prove that there is no ring homomorphism from $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ onto $\mathbb{Z}_8 \oplus \mathbb{Z}_6$.

4. (a) Let $G$ be a group, and let $a \in G$. Prove that the function $\phi_a : G \to G$, defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is an automorphism of $G$ (it is called the inner automorphism of $G$ induced by $a$).

(b) Let $G$ be a group and $\text{Inn}(G) = \{\phi_a \mid a \in G\}$ be the set of all inner automorphisms of $G$. Prove that $\text{Inn}(G)$ is a group under the operation of function composition.

5. (a) Let $R$ be a commutative ring with unity 1 and let $I$ be an ideal of $R$. Prove that $r + I$ is a unit (invertible) in $R/I$ if and only if there is an element $s$ in $R$ such that $rs - 1 \in I$.

(b) Show that the ring $\mathbb{Z} \oplus \mathbb{Z}$ has infinitely many zero-divisors.

(c) Find all units in the ring $\mathbb{Z} \oplus \mathbb{Z}$.

6. Let $R$ be a ring. Recall that $a \in R$ is called a nilpotent element if $a^n = 0$ for some $n \in \mathbb{Z}^+$ and it is called an idempotent element if $a^2 = a$.

(a) Show that if $a$ is an idempotent, then $1 - a$ is also an idempotent.

(b) If $f : R \to S$ is a ring homomorphism and $a \in R$ is nilpotent, prove that $f$ carries the element $a$ to a nilpotent element in the ring $S$.

(c) If $R$ is an integral domain, prove that the only idempotents in $R$ are 0 and 1.

(d) Show that $0 \neq a \in R$ is a zero-divisor if and only if $aba = 0$ for some $b \neq 0$.

7. Let $G$ be a group and let $Z(G) = \{g \in G \mid gx = xg, \ \forall x \in G\}$.

(a) Show that if $G/Z(G)$ is cyclic then $G$ is Abelian.

(b) Show that if $G$ is non-Abelian with $|G| = p^2$, where $p$ is a prime, and $Z(G) \neq \{e\}$, then $|Z(G)| = p$.

8. Suppose $G$ is a cyclic group with at least 3 elements. Without using the Euler $\phi$ function, prove that $G$ has an even number of generators.

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Let

\[ W = \text{span} \begin{bmatrix} 1 \\ 3 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \\ 1 \end{bmatrix} \].

Find an orthonormal basis for \( W \).

2. Suppose that \( A \) is a square matrix of size \( n \) and \( B = \{x_1, x_2, x_3, \ldots, x_n\} \) is a basis of \( \mathbb{R}^n \). Show that if \( A \) is nonsingular, then \( C = \{Ax_1, Ax_2, Ax_3, \ldots, Ax_n\} \) is a basis of \( \mathbb{R}^n \).

3. Find a basis for both the kernel and the range of the linear transformation represented by

\[ A = \begin{bmatrix} 1 & 3 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \]

4. Given the matrix

\[ A = \begin{bmatrix} 3 & -5 \\ 1 & -3 \end{bmatrix}, \]

find \( A^{2011} \).

5. Find the eigenvalues of the matrix

\[ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}. \]

6. Find all values of \( \lambda \) so that the following matrix is nonsingular:

\[ \begin{bmatrix} -2 & \lambda & 3 \\ 1 & 2 & \lambda \\ 1 & 11 & 18 \end{bmatrix}. \]

7. Given the \( 2 \times 3 \) matrix

\[ A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}. \]

(a) For which vectors \( b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \) does \( Ax = b \) have at least one solution?

(b) Solve \( Ax = \begin{bmatrix} 3 \\ 5 \end{bmatrix} \).

(c) What is the rank of \( A \)?

8. Consider the function \( T : P_2 \rightarrow \mathbb{R}^3 \) defined by \( T(p(x)) = \begin{bmatrix} p(-1) \\ p(0) \\ p(1) \end{bmatrix} \)

(a) Prove that \( T \) is an invertible linear transformation.

(b) Find \( T^{-1} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \)
Part A. Solve five of the following eight problems:

1. Let \( G = \{ x \in \mathbb{R} \mid x \neq -1 \} \). For \( x, y \in G \) let \( x \cdot y = x + y + xy \). Prove that \( \cdot \) is a binary operation on \( G \) and that \((G, \cdot)\) is a group.

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

   It remains to show that \((G, \cdot)\) is a group. Let \( x, y, z \in G \). Then
   \[
   (x \cdot y) \cdot z = (x + y + xy) + z + (x + y + xy)z
   = x + y + z + xy + yz + xz + xyz
   = x + (y + z + yz) + x(y + z + yz)
   = x \cdot (y \cdot z).
   \]

   Hence \( \cdot \) is associative.

   We claim that 0 is an identity element for \((G, \cdot)\). For \( x \in G \) we have
   \[
   x \cdot 0 = x + 0 + x \cdot 0 = x = 0 + x + 0 \cdot x = 0 \cdot x.
   \]

   Finally, for \( x \in G \) we claim that \( x^{-1} = \frac{-x}{x + 1} \) and that such \( x^{-1} \) belongs to \( G \). We have
   \[
   x \cdot \frac{-x}{x + 1} = x + \frac{-x}{x + 1} + \frac{-x^2}{x + 1} = \frac{x(x + 1) - x - x^2}{x + 1} = 0
   \]
   and similarly
   \[
   \frac{-x}{x + 1} \cdot x = 0.
   \]

   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. Consider the group \( S_n \) of permutations on \( n \) elements \((n \geq 3)\), and let \( A_n \) denote the set of even permutations in \( S_n \). Prove that \( A_n \) is a normal subgroup of \( S_n \).

   Solution. First of all \( e \in A_n \), and thus \( A_n \neq \emptyset \). Now consider \( \sigma = (a_1 \ b_1) \ldots (a_k \ b_k) \) and \( \tau = (c_1 \ d_1) \ldots (c_l \ d_l) \) where \( k \) and \( l \) are even (meaning that \( \sigma, \tau \in A_n \)). Then \( \sigma \tau^{-1} = (a_1 \ b_1) \ldots (a_k \ b_k)(c_1 \ d_1) \ldots (c_l \ d_l) \) 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 \( \alpha \) 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. Prove that there is no ring homomorphism from \( \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \) onto \( \mathbb{Z}_8 \oplus \mathbb{Z}_6 \).

   Proof. By contradiction, suppose that there is an onto homomorphism \( \psi : \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \to \mathbb{Z}_8 \oplus \mathbb{Z}_6 \).

   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 \( \ker \psi \) is a subgroup of \( \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \).

   But then \( \psi \) 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 \( \mathbb{Z}_8 \oplus \mathbb{Z}_6 \).

4. (a) Let \( G \) be a group, and let \( a \in G \). Prove that the function \( \phi_a : G \to G \), defined by \( \phi_a(x) = axa^{-1} \) for all \( x \in G \) is an automorphism of \( G \) (it is called the inner automorphism of \( G \) induced by \( a \)).
5. (a) Let \( R \) be a ring. 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 \( \phi_a \) 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 \( \phi_a \) 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 \( \phi_a \) is onto. Therefore \( \phi_a \) is an automorphism of \( G \).

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

It is easy to see that \( \phi_e \) 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 \( \phi_e \) is bijective it has an inverse \( \phi_e^{-1} \). Moreover, \( \phi_e^{-1}(x) = a^{-1}xa \), for all \( x \in G \) since \( (\phi_a \circ \phi_e^{-1})(x) = x = (\phi_a^{-1} \circ \phi_a)(x) \). 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 \( \phi_{a^{-1}} \circ \phi_a = \phi_e = \phi_e \circ \phi_a^{-1} \), which implies that the inverse of \( \phi_a \) in \( \text{Inn}(G) \) is \( \phi_{a^{-1}} \). Hence \( \text{Inn}(G) \) is a group. \( \square \)

5. (a) Let \( R \) be a commutative ring with unity 1 and let \( I \) be an ideal of \( R \). Prove that \( r + I \) is a unit (invertible) in \( R/I \) if and only if there is an element \( s \) in \( R \) such that \( rs - 1 \in I \).

(b) Show that the ring \( \mathbb{Z} \oplus \mathbb{Z} \) has infinitely many zero-divisors.

(c) Find all units in the ring \( \mathbb{Z} \oplus \mathbb{Z} \).

Solution.

(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. Let \( R \) be a ring. Recall that \( a \in R \) is called a \emph{nilpotent} element if \( a^n = 0 \) for some \( n \in \mathbb{Z}^+ \) and it is called an \emph{idempotent} element if \( a^2 = a \).

(a) Show that if \( a \) is an idempotent, then \( 1 - a \) is also an idempotent.

(b) If \( f : R \rightarrow S \) is a ring homomorphism and \( a \in R \) is nilpotent, prove that \( f \) carries the element \( a \) to a nilpotent element in the ring \( S \).

(c) If \( R \) is an integral domain, prove that the only idempotents in \( R \) are 0 and 1.

(d) Show that \( 0 \neq a \in R \) is a zero-divisor if and only if \( aba = 0 \) for some \( b \neq 0 \).

Solution.

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

Then \((1 - a)^2 = (1 - a)(1 - a) = 1 - 1 - a - a - 1 + a^2 = 1 - 2a + a = 1 - a \). So \( 1 - a \) is an idempotent element of \( R \).
(b) Let \( f : R \to S \) 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. Let \( G \) be a group and let \( Z(G) = \{ g \in G \mid gx = xg, \ \forall x \in G \} \).

(a) Show that if \( G/Z(G) \) is cyclic then \( G \) is Abelian.

(b) Show that if \( G \) is non-Abelian with \( |G| = p^3 \), where \( p \) is a prime, and \( Z(G) \neq \{ e \} \), then \( |Z(G)| = p \).

Solution.

(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 \( a = g^i x \) and \( b = g^j y \) for some \( x, y \in Z(G) \). Thus we have

\[
ab = (g^i x)(g^j y) = g^i(xg^j)y = g^i(g^j x)y = (g^j g^i)(yx) = g^j(g^i y)x = g^i (yg^i)x = (g^j y)(g^i x) = ba,
\]

where we used that \( x \) and \( y \) commute with everything in \( G \) and that \( g^i g^j = g^{i+j} = g^{i+j} = g^1 g^i \). 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. Suppose \( G \) is a cyclic group with at least 3 elements. Without using the Euler \( \phi \) function, prove that \( G \) has an even number of generators.

Solution. 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 \( (a^{-m})^n = (a^m)^{-1} = e^{-1} = e \). If there is an integer \( k \) with \( 1 \leq k < n \) such that \( (a^{-m})^k = e \), then \( (a^m)^{-k} = e^{-1} = e \); hence \( a^m = (a^{-m})^k = e \), 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 is on the back!!!
Part B. Solve five of the following eight problems:

1. Let

\[ W = \text{span} \left\{ \begin{bmatrix} 1 \\ 3 \\ 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} \right\}. \]

Find an orthonormal basis for \( W \).

We use the formula

\[ v_i = u_i - \frac{v_1 \cdot u_i}{v_1 \cdot v_1} v_1 - \frac{v_2 \cdot u_i}{v_2 \cdot v_2} v_2 - \cdots - \frac{v_{i-1} \cdot u_i}{v_{i-1} \cdot v_{i-1}} v_{i-1} \]

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

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

2. Suppose that \( A \) is a square matrix of size \( n \) and \( B = \{ x_1, x_2, x_3, \ldots, x_n \} \) is a basis of \( \mathbb{R}^n \). Show that if \( A \) is nonsingular, then \( C = \{ Ax_1, Ax_2, Ax_3, \ldots, Ax_n \} \) is a basis of \( \mathbb{R}^n \).

Solution. First, we need to show that \( C \) is linearly independent.

\[
0 = c_1 Ax_1 + c_2 Ax_2 + c_3 Ax_3 + \ldots + c_n Ax_n \\
= Ac_1 x_1 + Ac_2 x_2 + Ac_3 x_3 + \ldots + Ac_n x_n \\
= A \left( c_1 x_1 + c_2 x_2 + c_3 x_3 + \ldots + c_n x_n \right).
\]

Since \( A \) is nonsingular, we obtain

\[
0 = c_1 x_1 + c_2 x_2 + c_3 x_3 + \ldots + c_n x_n.
\]

Since \( B \) is a basis, it is linearly independent. Thus, \( c_1 = c_2 = \ldots = c_n = 0 \), and \( C \) is linearly independent.

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

\[
w = c_1 x_1 + c_2 x_2 + c_3 x_3 + \ldots + c_n x_n,
\]

where \( c_1, c_2, c_3, \ldots, c_n \) are scalars. Thus,

\[
y = Aw \\
= A \left( c_1 x_1 + c_2 x_2 + c_3 x_3 + \ldots + c_n x_n \right) \\
= Ac_1 x_1 + Ac_2 x_2 + Ac_3 x_3 + \ldots + Ac_n x_n \\
= c_1 Ax_1 + c_2 Ax_2 + c_3 Ax_3 + \ldots + c_n Ax_n.
\]

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

3. Find a basis for both the kernel and the range of the linear transformation represented by

\[
A = \begin{bmatrix} 1 & 3 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix}.
\]
**Solution.** The kernel is the solution space of the homogeneous system \( Ax = 0 \). 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. Given the matrix

\[
A = \begin{bmatrix}
3 & -5 \\
1 & -3
\end{bmatrix},
\]

find \( A^{2011} \).

**Solution.** First, we need to find the eigenvalues and eigenvectors of \( A \). The characteristic equation is found from

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

We find an eigenvector for each eigenvalue, obtaining:

\[
v_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 5 \\ 1 \end{bmatrix}.
\]

Thus, \( A = QDQ^{-1} \), so

\[
A^{2011} = QD^{2011}Q^{-1}
\]

\[
= \begin{bmatrix} 1 & 5 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} (-2)^{2011} & 0 \\ 0 & 2^{2011} \end{bmatrix} \begin{bmatrix} 1 & -5 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} -1 \\ 4 \end{bmatrix}
\]

\[
= \begin{bmatrix} 3 \cdot 2^{2010} & -5 \cdot 2^{2010} \\ 2^{2010} & -3 \cdot 2^{2010} \end{bmatrix}
\]

since

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

5. Find the eigenvalues of the matrix

\[
\begin{bmatrix}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5
\end{bmatrix}.
\]

**Solution.** 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 \( 5 \times 5 \) 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. Find all values of \( \lambda \) so that the following matrix is nonsingular:

\[
\begin{pmatrix}
-2 & \lambda & 3 \\
1 & 2 & \lambda \\
1 & 11 & 18
\end{pmatrix}.
\]

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

7. Given the \( 2 \times 3 \) matrix

\( A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \).

(a) For which vectors \( \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \) does \( A\mathbf{x} = \mathbf{b} \) have at least one solution?

(b) Solve \( A\mathbf{x} = \begin{bmatrix} 3 \\ 5 \end{bmatrix} \).

(c) What is the rank of \( A \)?

**Solution.**

(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. Consider the function \( T : P_2 \rightarrow \mathbb{R}^3 \) defined by \( T(p(x)) = \begin{bmatrix} p(-1) \\ p(0) \\ p(1) \end{bmatrix} \).

(a) Prove that \( T \) is an invertible linear transformation.

(b) Find \( T^{-1} \left( \begin{bmatrix} a \\ b \\ c \end{bmatrix} \right) \)

**Solution.**

(a) \( T \) is linear, as

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

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

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

Thus,

\[
T^{-1} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = b + \left( \frac{c - a}{2} \right) x + \left( \frac{a - 2b + c}{2} \right) x^2.
\]
Part A. Solve five of the following eight problems:

1. Let $G$ be a group.
   (a) If $a, b \in G$ and $ab = e$, prove that $ba = e$.
   (b) If $|G| = 4$, prove that $G$ is Abelian.
   (c) If $a, b \in G$, prove that $o(bab^{-1}) = o(a)$.

2. Let $\sigma \in S_n$ be a permutation. For $x, y \in \{1, 2, \ldots, n\}$ let $x \sim y$ if and only if $\sigma^k(x) = y$ for some $k \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation on the set $\{1, 2, \ldots, n\}$.
   
   Hint. Note that $\sigma$ is fixed; it is $k$ that changes.

3. Let $R = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}$ and $S = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \}$. Define $\varphi : R \to S$ by $\varphi \left( \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \right) = a + b\sqrt{2}$. Prove that $\varphi$ is a ring isomorphism. You may assume that $R$ is a commutative ring with identity using the usual matrix addition and multiplication, that $S$ is a commutative ring with identity using the usual addition and multiplication of real numbers.

4. True or False (prove or give a counterexample)
   (a) The elements in $\mathbb{Z}_n$ are either zero, invertible or zero divisors.
   (b) Part (a) is true for all rings.

5. Let $G$ be a group of (finite) order $n$, and $\phi : G \to \mathbb{C}^*$ a homomorphism of groups. Prove that $\phi(g)$ is an $n^{th}$ root of 1 (and thus, lays on the unit circle), for all $g \in G$.

6. How many elements of order 7 does the group $\mathbb{Z}_{21} \oplus \mathbb{Z}_{35}$ have? Justify your answer.

7. (a) Let $R$ be a commutative ring with $a \in R$. The annihilator of $a$ is defined by $\text{Ann}(a) = \{ x \in R \mid xa = 0 \}$.
   
   Prove that $\text{Ann}(a)$ is an ideal of $R$.
   (b) Show that the direct sum of two nonzero rings is never an integral domain.

8. Recall that the center of a group $G$ is the subset $Z(G) = \{ a \in G \mid ax = xa \text{ for all } x \in G \}$.
   (a) Prove that $Z(G)$ is a subgroup of $G$;
   (b) Prove that $Z(G)$ is a normal subgroup of $G$.

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Let $W$ be the subspace of $\mathbb{R}^4$ with basis $\left\{ \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$. Use the Gram-Schmidt process to find an orthonormal basis for $W$.

2. Show that $A \in M_{nn}$ is invertible if and only if 0 is not an eigenvalue of $A$.

3. Consider the linear transform $T : P^2 \rightarrow P^2$ defined by

$$T(a + bx + cx^2) = (a + b + c) + 2(b + c)x + 3cx^2.$$ 

Find the matrix of $T$ with respect to the basis $\{1, 1 + x, 3 + 4x + 2x^2\}$.

4. Let $U$ be the subspace of $\mathbb{R}^4$ spanned by $\{(1, 0, 1, 0), (-1, 2, 0, 1)\}$ and let $V$ be the subspace of $\mathbb{R}^4$ spanned by $\{(0, 2, 1, 1), (0, 0, 1, 1)\}$.

(a) Find a basis of $U \cap V$.

(b) Extend (a) to a basis for $U$.

5. Give the rank and nullity of the matrix

$$A = \begin{pmatrix} 1 & 0 & 1 & -2 & 5 \\ 0 & 1 & -1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$ 

6. Suppose that $W$ is a vector space with dimension 5, and $U$ and $V$ are subspaces of $W$, each of which has dimension 3. Prove that $U \cap V$ contains a nonzero vector.

7. Diagonalize

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

8. Let $\alpha, \beta, \gamma$ be real numbers. Evaluate the determinant

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

(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. □

(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 $(bab^{-1})^m = ba^mb^{-1} = beb^{-1} = e$. 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 $ba^mb^{-1} = e$ and this implies that $a^m = e$. Thus, by definition of $n, n \leq m$. Therefore $m = n$, as required. □

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

\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 $\varphi$ 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 $\varphi$ is one-to-one. Next, $\varphi$ 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 $\varphi$ 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

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

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

$$= \varphi(A) + \varphi(B).$$

Similarly,

$$\varphi(AB) = \varphi\left(\begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix}\right)$$

$$= ac + 2bd + (ad + bc)\sqrt{2}$$

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

$$= \varphi(A)\varphi(B).$$

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 modulo \(n\) 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 \(\phi\) 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 \(k = 1, 2, \cdots, n\). 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 in $R$ is not an integral domain.

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, $gng^{-1} = gg^{-1}n = n$, and thus $gZ(G)g^{-1} = Z(G)$, for all $g \in G$, and thus $Z(G) \leq G$. 

□
Part B.

1. We use the formula

\[ v_i = u_i - \frac{v_1 \cdot u_i}{v_1 \cdot v_1} v_1 - \frac{v_2 \cdot u_i}{v_2 \cdot v_2} v_2 - \ldots - \frac{v_{i-1} \cdot u_i}{v_{i-1} \cdot v_{i-1}} v_{i-1} \]

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 \( \Phi \) is bijective.

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

If \( \lambda = 0 \) were an eigenvalue of \( A \), then there would be an eigenvector of \( \Phi \), call it \( v \), such that \( \Phi(v) = 0 \). It follows that \( v \in Ker(\Phi) \). Hence, \( \Phi \) 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 \( Ker(\Phi) \) is trivial. The dimension formula

\[ \dim(Domain) - \dim(Kernel) = \dim(Range) \]

implies that \( \dim(Range) = n \), which means that \( \Phi \) 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

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

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, $B = \{(0,2,1,1),(1,0,1,0)\}$ 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 $4 \times 5$, we have $\text{rank} + \text{nullity} = 5$; thus $\text{nullity}(A) = 2$.

6. The dimension formula says that

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

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

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

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

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

which implies that $\text{dim}(U \cap V) \geq 1$, 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

$$
\chi_A(\lambda) = \text{det}(A - \lambda I) = \text{det}
\begin{pmatrix}
3 - \lambda & -2 & 2 \\
0 & 1 - \lambda & 2 \\
0 & 2 & 1 - \lambda
\end{pmatrix}
$$

$$
= (3 - \lambda) \text{det}
\begin{pmatrix}
1 - \lambda & 2 \\
2 & 1 - \lambda
\end{pmatrix}
$$

$$
= (3 - \lambda)[(1 - \lambda)^2 - 2^2]
$$

$$
= (3 - \lambda)(\lambda^2 - 2\lambda - 3)
$$

$$
= -(\lambda + 1)(\lambda - 3)^2.
$$
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

$$
-2y + 2z = 0 \\
-2y + 2z = 0 \\
2y - 2z = 0
$$

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 $\alpha, \beta, \gamma$ 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.
Part A. Solve five of the following eight problems:

1. True or False (prove or give a counterexample):
   Let $A, N, G$ be groups such that $A \leq N$ and $N \leq G$, then $A \leq G$.

2. Suppose you are given the operation $*$ on the set $G = \{x \in \mathbb{R} \mid x \neq -1\}$, defined by $a * b = ab + a + b$. Show that under this operation $G$ is a group.

3. Suppose that $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ is a group homomorphism with $\phi(7) = 6$.
   (a) Determine $\phi(x)$.
   (b) Determine the image of $\phi$.
   (c) Determine the kernel of $\phi$.

4. True or False (prove or give a counterexample): If a ring $R$ has more than two idempotent elements ($e$ is idempotent if $e^2 = e$), then $R$ is not an integral domain.

5. Let $N = \langle ([2], (123)) \rangle \triangleleft \mathbb{Z}_4 \times S_3$.
   (a) Find the order of the factor group $(\mathbb{Z}_4 \times S_3)/N$.
   (b) Find the order of the element $([3], (12))N$ in $(\mathbb{Z}_4 \times S_3)/N$. Is $(\mathbb{Z}_4 \times S_3)/N$ cyclic?

6. Let $G$ be a finite group of odd order. Prove that every element in $G$ has a square root (so you have to show that for all $g \in G$, there exists $x \in G$ such that $x^2 = g$).
   Hint: Show that the map $\theta : G \to G : g \to g^2$ is one-to-one.

7. Suppose that $a$ and $b$ are group elements that commute and have orders $m$ and $n$. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of $m$ and $n$. Show that this need not be true if $a$ and $b$ do not commute.

8. Let $R$ be a ring with 1, and let $U(R)$ be the set of all units in $R$.
   (a) Show that $U(R)$ is a group.
   (b) If $I$ is an ideal (left, right, or two-sided) in $R$ such that $I \cap U(R) \neq \emptyset$, show that $I = R$.

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Consider a system of equations $Ax = b$ where $A$ is $n \times k$. Give a proof or counterexample for the following:
   
   (a) For given $A$ and $b$, if $n = k$ then there is always at most one solution.
   
   (b) For given $A$ and $b$, if $n > k$ then there is always at least one solution.
   
   (c) For given $A$, if $n < k$ then there exists a vector $b$ for which the system has no solution.

2. Let $V$ be an $n$-dimensional vector space and $T : V \to V$ a linear transformation such that the image and kernel of $T$ are identical.
   
   (a) Prove that $n$ is even.
   
   (b) Give an example of such a linear transformation $T$.

3. Let $P_2$ be the set of all real polynomials of degree at most 2. It is given that the map
   
   $f : P_2 \to P_2 : p(x) \to p(x) - p'(x) + p''(x)$
   
   is a linear transformation and that $\beta = \{1, 1 + x, 1 + x + x^2\}$ is a basis for $P_2$. Find the matrix representation of $f$ with respect to the basis $\beta$.

4. Let $A$ be a square matrix with the property that the sum of the elements in each of its columns is 1. Show that $\lambda = 1$ is an eigenvalue of $A$.

5. Let $\theta : \mathbb{R}^2 \to \mathbb{R}^3$ be a linear transformation such that $\theta(2, -1) = (1, 0, 1)$ and $\theta(-5, 3) = (0, -1, 1)$. Find an expression for $\theta(x, y)$.

6. Let $W_1$ and $W_2$ be subspaces of a finite-dimensional vector space $V$. Prove the following:
   
   (a) $W_1 + W_2 = \{w_1 + w_2 : w_1 \in W_1, w_2 \in W_2\}$ is a subspace of $V$.
   
   (b) $W_1 \cap W_2$ is a subspace of $V$.
   
   (c) $\dim(W_1) + \dim(W_2) = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$.

7. Find all values of $\alpha$ for which the following matrix is nonsingular
   
   \[
   \begin{pmatrix}
   -2 & \alpha & 3 \\
   1 & 2 & \alpha \\
   1 & 11 & 18
   \end{pmatrix}
   \]

8. Suppose that $v_1$ and $v_2$ are arbitrary vectors in $\mathbb{R}^n$. Prove that
   
   $\text{span}\{v_1, v_2\} = \text{span}\{v_1 + v_2, v_1 - v_2\}$. 
Part A.

1. False: Consider $G = A_4$, $N$ to be the Klein group

$$N = \{ e, (12)(34), (13)(24), (14)(23) \}$$

and $A = \langle (12)(34) \rangle$. It is easy to see that $A \trianglelefteq N \trianglelefteq G$, but $A$ is not normal in $G$ because $(123)A(123)^{-1} = \langle (14)(23) \rangle \neq A$.

2. We need to check all the axioms of a group. First we realize that the product of any two elements of $\mathbb{R}$ yields an element of $\mathbb{R}$, thus closure is (almost) granted. We just need to check that the product of any two elements in $G$ is not $-1$. If $a * b = -1$ then

$$-1 = a + b(1 + a) \quad \text{or} \quad -(1 + a) = b(1 + a)$$

which forces either $1 + a = 0$ (impossible as $a \neq -1$) or $b = -1$ (then again impossible). It follows that $a * b \neq -1$, and thus we have closure for $G$.

In the search for an identity $e$ we set $a * e = a$, we get $a = a + e + ae$, which means that $e(1 + a) = 0$. But, since $a \neq -1$ then $e = 0$. So, $e = 0$ is the only candidate to be the identity for this product... but it is easy to check that $a * 0 = 0 * a = a$ for all $a \in G$, so we have found the identity.

Now let us find the inverse of an element $a$, we want to find $b$ such that $a * b = 0$.

It is easy to see that $a + b + ab = 0$ forces

$$b = -\frac{a}{1 + a}$$

which then again needs $a \neq -1$ to be well defined. Now note that this fraction can never be $-1$ (as $a$ and $1 + a$ are never equal to each other), thus the (right) inverse of any element in $G$ is well defined and an element of $G$. Now it is easy to check that $a * b = b * a = 0$ and thus every element in $G$ has a double-sided inverse.
The only thing left to check is associativity. This follows simply from
\[a \ast (b \ast c) = a \ast (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + bc + ab + ac + abc = (a + b + ab) + c + (a + b + ab)c = (a + b + ab) \ast c = (a \ast b) \ast c\]

Hence, \(G\) is a group. Moreover, it is easy to see that it is an Abelian group.

3. First note that since \(gcd(50, 7) = 1\) then 7 is a generator of \((\mathbb{Z}_{50}, +)\). Thus defining \(\phi(7)\) will determine uniquely ALL the values \(\phi\) takes in \(\mathbb{Z}_{50}\).

(a) In order to find the images we need to write any element in \(\mathbb{Z}_{50}\) as a multiple (modulo 50) of 7. Since,
\[50 + 7 \cdot (-7) = 1\]
then, using the homomorphism properties of \(\phi\) we get
\[\phi(1) = \phi(50 + 7 \cdot (-7)) = \phi(50) + \phi(7 \cdot (-7)) = \phi(0) - 7\phi(7) = -7\phi(7) = -42 = 3\]

where the last step was reduction modulo 15 (the images of \(\phi\) live in \(\mathbb{Z}_{15}\)).

It follows that for every integer \(x\),
\[\phi(x) = x\phi(1) = 3x \pmod{15}\]

(b) Since 3 divides 15 then the multiples of 3 (modulo 15) yields a proper subgroup of \(\mathbb{Z}_{15}\), which is
\[\phi(\mathbb{Z}_{50}) = \{0, 3, 6, 9, 12\}\]

which is isomorphic to \(\mathbb{Z}_5\).
(c) Since $15 = 3 \cdot 5$, then any $x$ that has a five in its prime factorization (divisible by 5) will be in $\text{Ker}(\phi)$. Hence, the kernel is the set of multiples of 5 modulo 50, that is

$$\text{Ker}(\phi) = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$$

which is isomorphic to $\mathbb{Z}_{10}$.

Note that the first isomorphism theorem would say, in this case, something like

$$\mathbb{Z}_{50}/\mathbb{Z}_{10} \cong \mathbb{Z}_5$$

4. TRUE: $e^2 = e$ implies $e(e - 1) = 0$, the two obvious solutions are $e = 0, 1$, if there were another solution, then $e$ and $e - 1$ would be both non-zero with product equal to zero. Hence, $e$ and $e - 1$ would be zero divisors.

5. Since $[2]$ has order 2 in $\mathbb{Z}_4$ and $(123)$ has order 3 in $S_3$, then $\sigma = ([2], (123))$ has order 6, and thus $|N| = 6$ (and cyclic).

(a) First of all notice that $N$ is normal in $G = \mathbb{Z}_4 \times S_3$, and that $|G| = 4 \cdot 6 = 24$. It follows that $G/N$ has $24/6 = 4$ elements.

(b) First notice that $([3], (12)) \notin N$. Since $2 \cdot [3] = [2]$ and $(12)^2 = e$, then $([3], (12))^2 = ([2], e) = ([2], (123))^3$, which lives in $N$. It follows that the order of $([3], (12))N$ in $G/N$ is 2.

Now, note that $([3], (123)) \notin N$, and that

$$([3], (123))([3], (12))^{-1} = ([0], (13)) \notin N$$

and thus $([3], (123))N \neq ([3], (12))N$. Moreover, since

$$([3], (123))^2 = ([2], (132)) = ([2], (123))^3 \in N$$

then $G/N$ contains at least two elements of order 2, thus it cannot be cyclic.

6. Consider $\theta : G \to G$ defined by $\theta(g) = g^2$. Let $|G| = n < \infty$. We want to show that $\theta$ is onto.

Using that $\gcd(n, 2) = 1$ we get $\alpha, \beta \in \mathbb{Z}$ such that $1 = 2\alpha + n\beta$, then

$$x = x^{2\alpha + n\beta} = x^{2\alpha}x^{n\beta} = x^{2\alpha}(x^n)^\beta = x^{2\alpha} = (x^\alpha)^2$$

for all $x \in G$. So, $\theta(x^\alpha) = x$. 

7. Let $G$ be the group that contains the elements $a$ and $b$. Consider $x = (ab)^{gcd(m,n)} \in G$. Since $lcm(m,n)gcd(m,n) = mn$ then

$$x^{lcm(m,n)} = ((ab)^{gcd(m,n)})^{lcm(m,n)} = ab^{mn} = a^mb^n = e$$

Hence, the order of $x$ is a divisor of $lcm(m,n)$. If the order $d$ of $x$ were less than that, then

$$e = x^d = ((ab)^{gcd(m,n)})^d = a^{d_{gcd}(m,n)}b^{d_{gcd}(m,n)}$$

which forces that the element $a^{d_{gcd}(m,n)} = b^{-d_{gcd}(m,n)}$ is in the intersection of the groups generated by $a$ and $b$. This forces $a^{d_{gcd}(m,n)} = b^{-d_{gcd}(m,n)} = e$, but this implies that $n|d \text{gcd}(m,n)$ and $m|d \text{gcd}(m,n)$, but since $d < lcm(m,n)$ we get a contradiction. Hence, the order of $x$ is exactly $lcm(m,n)$.

For the counterexample, consider $a = (123)$ and $b = (12)$, both elements in $S_3$. Since $S_3$ is not cyclic then there is no element of order 6 in this group.

8. Let $R$ be a ring with 1, and $U(R)$ be the set of all its units.

(a) We want to show that $U(R)$ is a multiplicative group. Since $R$ has a 1 and associativity of the multiplication is inherited from $R$, then we just need to check closure under multiplication and inverses.

Let $r, s \in U(R)$, then $ar = ra = 1$ and $bs = sb = 1$ for some $a, b \in R$. Then,

$$(ba)(rs) = b(ar)s = b \cdot 1 \cdot s = 1 \quad (rs)(ba) = r(sb)a = r \cdot 1 \cdot a = 1$$

which means that $rs$ is invertible in $R$.

Closure for inverses is straight out of the definition of inverses.

(b) Let $r \in I \cap U(R)$, then there is an element $a \in R$ such that $ar = ra = 1$. But since $I$ is an ideal (left/right/double-sided), then this forces that $1 \in I$, which immediately implies that all the elements in the ring are contained in $I$ (because of the “absorption” property of ideals).
Part B.

1. For these solutions consider a system of equations \(Ax = b\) where \(A\) is \(n \times k\).

(a) False. For \(n = k = 2\), the system
\[
\begin{bmatrix}
1 & -1 \\
1 & -1
\end{bmatrix} x = \begin{bmatrix} 0 \\ 0 \end{bmatrix}
\]
has infinitely many solutions (the subspace spanned by \((1, 1)\)).

(b) False. For \(n = 3\) and \(k = 2\), the system
\[
\begin{bmatrix}
1 & -1 \\
1 & 1 \\
1 & 1
\end{bmatrix} x = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}
\]
has no solutions (the first two equations force \(x = y = 0\) and the third asks for \(x + y = 1\)).

(c) True. Note that in this case no \(b\) is given, thus we need to look at this in a different way. Since \(A\) has more columns than rows, then the row dimension will always be less than the number of columns. But the row dimension is equal to the column dimension (and this is less than \(k\)), which forces the columns of \(A\) to be linearly dependent, and thus not a basis of \(\mathbb{R}^k\).

Now, the search for an \(x\) such that \(Ax = b\) can be read as the search for coefficients (the components of \(x\)) such that \(b\) is a linear combination of the columns of \(A\). But since the column dimension is less than \(k\) then there is always at least one \(b\) that will not be written as a linear combination of the columns of \(A\). This means that for that \(b\) the system has no solutions.

2. Let \(V\) be an \(n\)-dimensional vector space and \(T : V \to V\) a linear transformation such that the image and kernel of \(T\) are identical.

(a) Since \(V\) is finitely dimensional, then we can use the first isomorphism theorem to get a “dimension formula”, that is
\[
dim(V) = \dim(Ker(T)) + \dim(Im(T))
\]
Since the kernel and image are identical, then they have the same dimension \(k\), and thus \(n = 2k\).
(b) Consider \( T : \mathbb{R}^2 \to \mathbb{R}^2 \) defined by \( T(x,y) = (0, x) \). This map has \( \text{Ker}(T) = \langle (0,1) \rangle = \text{Im}(T) \).

3. We compute the images of the elements of \( \beta \),

\[
\begin{align*}
    f(1) &= 1 - 0 + 0 = 1 \\
    f(1 + x) &= (1 + x) - 1 + 0 = x \\
    f(1 + x + x^2) &= (1 + x + x^2) - (1 + 2x) + 2 = 2 - x + x^2
\end{align*}
\]

It follows that the matrix that represents \( f \) from the basis \( \beta \) to the standard basis of \( P_2 \) is given by

\[
\begin{bmatrix}
    1 & 0 & 2 \\
    0 & 1 & -1 \\
    0 & 0 & 1
\end{bmatrix}
\]

The change of basis matrix from basis \( \beta \) to the standard basis of \( P_2 \) is

\[
\begin{bmatrix}
    1 & 1 & 1 \\
    0 & 1 & 1 \\
    0 & 0 & 1
\end{bmatrix}
\]

Hence, the matrix that represents \( f \) from basis \( \beta \) to basis \( \beta \) is

\[
\begin{bmatrix}
    1 & 1 & 1 \\
    0 & 1 & 1 \\
    0 & 0 & 1
\end{bmatrix}^{-1}
\begin{bmatrix}
    1 & 0 & 2 \\
    0 & 1 & -1 \\
    0 & 0 & 1
\end{bmatrix} =
\begin{bmatrix}
    1 & -1 & 3 \\
    0 & 1 & -2 \\
    0 & 0 & 1
\end{bmatrix}
\]

4. Let \( A \) be an \( n \times n \) matrix such that the sum of the elements in each of its columns is 1. Note that the transpose of \( A \) is such that the sum of the elements in each of its rows is 1. It follows that if we consider the vector \( v \) with 1’s in all its components. The product \( A^Tv \) is equal to \( v \) because the components of the product are the sums of the elements in each row of \( A^T \). Thus \( v \) is an eigenvector of \( A^T \) with eigenvalue 1. But we know that an eigenvalue of \( A^T \) is also an eigenvalue of \( A \), and so we are done proving that 1 is an eigenvalue of \( A \).

In fact if \( \lambda \) is an eigenvalue of \( A^T \) then

\[
\det(A^T - \lambda I) = 0
\]
but
\[(A^T - \lambda I d)^T = (A^T)^T - (\lambda I d)^T = A - \lambda I d\]
and thus
\[\det(A - \lambda I d) = \det(A^T - \lambda I d) = 0\]
which means that \(\lambda\) is also an eigenvalue of \(A\).

5. Consider \(\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^3\) be a linear transformation such that \(\theta(2, -1) = (1, 0, 1)\) and \(\theta(-5, 3) = (0, -1, 1)\).

Let us write \((x, y)\) as a linear combination of \((2, -1)\) and \((-5, 3)\).
\[(x, y) = \alpha(2, -1) + \beta(-5, 3) = (2\alpha - 5\beta, -\alpha + 3\beta)\]
which yields
\[x = 2\alpha - 5\beta \quad y = -\alpha + 3\beta\]
and thus \(\beta = x + 2y\) and \(\alpha = 3x + 5y\). It follows that
\[(x, y) = (3x + 5y)(2, -1) + (x + 2y)(-5, 3)\]
and thus
\[\theta(x, y) = (3x + 5y)\theta(2, -1) + (x + 2y)\theta(-5, 3)\]
\[= (3x + 5y)(1, 0, 1) + (x + 2y)(0, -1, 1)\]
\[= (3x + 5y, -x - 2y, 4x + 7y)\]

6. Let \(W_1\) and \(W_2\) be subspaces of a finite-dimensional vector space \(V\).

(a) We first check that zero is in \(W_1 + W_2\), this is clear because \(0 + 0 = 0\) and \(0 \in W_1, 0 \in W_2\).

Now we check closure for sum. Let \(w_1 + w_2\) and \(v_1 + v_2\) be two elements of \(W_1 + W_2\). Then
\[(w_1 + w_2) + (v_1 + v_2) = (w_1 + v_1) + (w_2 + v_2)\]
which is in \(W_1 + W_2\) because \(w_1 + v_1 \in W_1\) and \(w_2 + v_2 \in W_2\) (closure of addition in these subspaces).

Finally we check closure under scalar multiplication. Let \(w_1 + w_2\) be an element of \(W_1 + W_2\), and \(\alpha \in \mathbb{R}\). Then,
\[\alpha(w_1 + w_2) = \alpha w_1 + \alpha w_2\]
which is in \(W_1 + W_2\) because \(\alpha w_1 \in W_1\) and \(\alpha w_2 \in W_2\) (closure of scalar multiplication in these subspaces).
(b) We first check that zero is in $W_1 \cap W_2$, this is clear because $0 \in W_1$ and $0 \in W_2$.

Now we check closure for sum. Let $w$ and $v$ be two elements of $W_1 \cap W_2$, then $w + v \in W_1$ and $w + v \in W_2$ (closure of addition in these subspaces), and thus $w + v \in W_1 \cap W_2$.

Finally we check closure under scalar multiplication. Let $w$ be an element of $W_1 \cap W_2$, and $\alpha \in \mathbb{R}$, then $\alpha w \in W_1$ and $\alpha w \in W_2$ (closure of scalar multiplication in these subspaces), and thus $\alpha w \in W_1 \cap W_2$.

(c) We first take a basis of $W_1 \cap W_2$, then we complete this basis to two other bases, one for $W_1$ and one for $W_2$. This can always be done by a known theorem (which requires the axiom of choice to be proved).

So, let

$$\{w_1, w_2, \ldots, w_k, w_{k+1}, \ldots, w_n\}$$

be a basis of $W_1$ (dimension of $W_1$ is $n$),

$$\{w_1, w_2, \ldots, w_k, v_{k+1}, v_{k+2}, \ldots, v_m\}$$

be a basis for $W_2$ (dimension of $W_2$ is $m$), and

$$\{w_1, w_2, \ldots, w_k\}$$

be a basis for $W_1 \cap W_2$ (dimension of $W_1 \cap W_2$ is $k$).

Since the union of the bases of $W_1$ and $W_2$ is a spanning set of $W_1 + W_2$, then

$$\text{span}\{w_1, w_2, \ldots, w_k, w_{k+1}, \ldots, w_n, v_{k+1}, v_{k+2}, \ldots, v_m\} = W_1 + W_2$$

But this set (with $n + (m - k)$ elements) must be linearly independent otherwise we get a contradiction with either the given bases being linearly dependent or we would find vectors not on the basis of $W_1 \cap W_2$ that should be in the intersection. So, the dimension of $W_1 + W_2$ is $n + (m - k)$, done.
7. We need to compute the determinant of this matrix

\[
\begin{vmatrix}
-2 & \alpha & 3 \\
1 & 2 & \alpha \\
1 & 11 & 18
\end{vmatrix} = \begin{vmatrix}
-2 & \alpha & 3 \\
1 & 2 & \alpha \\
1 & 9 & 18 - \alpha
\end{vmatrix}
\]

by subtracting \( R_2 \) from \( R_3 \)

\[
= \begin{vmatrix}
0 & \alpha + 4 & 3 + 2\alpha \\
1 & 2 & \alpha \\
0 & 9 & 18 - \alpha
\end{vmatrix}
\]

by adding \( 2R_2 \) to \( R_1 \)

\[
= - \begin{vmatrix}
\alpha + 4 & 3 + 2\alpha \\
9 & 18 - \alpha
\end{vmatrix}
\]

expansion into cofactors, using the first column

\[
= - [(\alpha + 4)(18 - \alpha) - (3 + 2\alpha)(9)]
= \alpha^2 + 4\alpha - 45
= (\alpha - 5)(\alpha + 9)
\]

So, the values for which the matrix is nonsingular are \( \alpha \neq 5, -9 \).

8. Since \( v_1 + v_2 \) and \( v_1 - v_2 \) are linear combinations of \( v_1 \) and \( v_2 \), then the subspace generated by the first two vectors is a subset of the subspace spanned by the latter two.

Now we will show that \( v_1 \) and \( v_2 \) are linear combinations of \( v_1 + v_2 \) and \( v_1 - v_2 \), and thus we will get the other inclusion that is needed to get

\[
\text{span} \{ v_1, v_2 \} = \text{span} \{ v_1 + v_2, v_1 - v_2 \}.
\]

It is easy to check that

\[
v_1 = \frac{1}{2}(v_1 + v_2) + \frac{1}{2}(v_1 - v_2)
\]

\[
v_2 = \frac{1}{2}(v_1 + v_2) - \frac{1}{2}(v_1 - v_2)
\]

We are done.
Part A. Solve five of the following eight problems:

1. Let $G = \{ x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1 \}$. Define the operation $*$ on $G$ by $a * b = a^{\ln b}$, for all $a, b \in G$.
   (a) Prove that $G$ is an abelian group under the operation $*$.
   (b) Show that $G$ is isomorphic to the multiplicative group $\mathbb{R}^\times$.

2. Let $G_1, G_2$ be groups.
   (a) If $H_1 \leq G_1$ and $H_2 \leq G_2$ prove that $H_1 \times H_2 \leq G_1 \times G_2$.
   (b) TRUE/FALSE: If $H \leq G_1 \times G_2$ then $H = H_1 \times H_2$ for some $H_1 \leq G_1$ and some $H_2 \leq G_2$. Prove your answer!

3. If $\phi : S_3 \rightarrow \mathbb{Z}_3$ is a group homomorphism, show that $\phi(g) = 0$ for all $g \in S_3$.

4. Define $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([x]_{mn}) = ([x]_m, [x]_n)$. Show that $f$ is well-defined, and that $f$ is bijective if and only if $\gcd(m, n) = 1$.

5. Let $H \leq G$ and for any $g \in G$ define $n_H(g)$ to be the least positive integer such that $g^{n_H(g)} \in H$. Show that $n_H(g)$ divides the order of $g$.

6. Let $R$ be a commutative ring. An element $r \in R$ is called nilpotent if $r^n = 0$ for some integer $n > 0$. Prove that $a + b$ is nilpotent if $a$ and $b$ are nilpotent elements of $R$.

7. Show that the set of matrices $A \in M_n(\mathbb{R})$ such that $Av = 0$ for some fixed $v \in \mathbb{R}^n$ is a left ideal of $M_n(\mathbb{R})$.

8. Let
   $$ S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R}) $$
   (a) Show that $S$ is a subring of $M_2(\mathbb{R})$, the ring of $2 \times 2$ matrices with real entries.
   (b) Show that $S$ and $\mathbb{C}$ are isomorphic rings.

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Recall that \( P_5 \) is the set containing the zero polynomial and all polynomials of degree at most five with real coefficients. Show that the derivative defines a linear transformation from \( P_5 \) to itself. Is it onto? Find the matrix for this map in the standard basis.

2. Show that
\[
U = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } a + b + c + d = 0 \right\} \subset M_2(\mathbb{R})
\]
is a subspace of \( M_2(\mathbb{R}) \). Find a basis for \( U \).

3. Find a basis for the orthogonal complement of the subspace \( W = \text{span}\{(1,2,-1,0), (0,1,1,3)\} \) of \( \mathbb{R}^4 \).

4. Let \( T \) be the linear transformation of \( \mathbb{R}^3 \) with standard matrix \[
\begin{bmatrix}
1 & 5 & 2 \\
2 & 1 & 3 \\
1 & 1 & 4
\end{bmatrix}
\]. Find the matrix of \( T \) with respect to the basis \( B = \{(1,1,1), (1,1,0), (1,0,0)\} \).

5. Let \( F : \mathbb{R}^4 \rightarrow \mathbb{R}^3 \) be any linear transformation such that
\[
\text{Ker } F = \left\{ (x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid \begin{array}{ll}
x_1 - 2x_2 + x_3 - x_4 = 0 \\
x_1 - x_2 - 2x_3 + x_4 = 0 \\
x_1 - 3x_2 + 4x_3 - 3x_4 = 0
\end{array} \right\}.
\]
(a) Find the dimension of \( \text{Ker } F \) and a basis for it.
(b) Give an example of such a linear transformation \( F \).
(c) For the example you gave in (b), find a basis for the range of \( F \).

6. A square matrix \( B \) is skew-symmetric if \( B^T = -B \). Suppose that the square matrix \( A \) is skew-symmetric and invertible. Prove that \( A^{-1} \) is also skew-symmetric.

7. Diagonalize the following matrix
\[
A = \begin{bmatrix}
1 & -2 & -1 \\
-1 & 1 & 1 \\
-1 & 0 & -1
\end{bmatrix}
\]
Then give a basis of \( \mathbb{R}^3 \) for which \( A \) ‘becomes’ diagonal.

8. Consider the subspace \( U = \{(x, y, z) \in \mathbb{R}^3 \mid 2x - y - 3z = 0 \} \subset \mathbb{R}^3 \) and the set of vectors \( S = \{(1, -1, 1), (4, 2, 2)\} \subset \mathbb{R}^3 \).
(a) Complete \( S \) to a basis in \( \mathbb{R}^3 \).
(b) Show that \( U = \text{span}(S) \).
Part A.

1. Let \( G = \{ x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1 \} \). Define the operation \( * \) on \( G \) by \( a * b = a^{\ln b} \), for all \( a, b \in G \).

   1. Prove that \( G \) is an abelian group under the operation \( * \).
   2. Show that \( G \) is isomorphic to the multiplicative group \( \mathbb{R}^\times \).

Solution.

1. First note that the product of any two elements in \( G \) is well defined, as \( x \mapsto \ln x \) is a well-defined function.

Since \( a^{\ln b} = 1 \) only when \( a = 1 \) or \( \ln b = 0 \) (which forces \( b = 1 \)), and \( 1 \not\in G \), then closure of \( * \) holds.

   The identity must be an element \( a \) (using \( e \) will get us into notation problems, as \( \ln x = \log_e x \)) such that \( b = a * b = a^{\ln b} \). If we apply \( \ln \) both sides we get

\[
\ln b = \ln a^{\ln b} = a^{\ln b} \ln a
\]

thus \( \ln a = 1 \), and thus \( a = e \). I guess that notation problem is solved by now.

   It is clear that \( b = b * e = e^{\ln b} \) for all \( b \in G \). Thus \( e \) is the identity of \( G \).

   The inverse of \( b \in G \) is found by solving \( e = a * b = a^{\ln b} \), which after applying \( \ln \) both sides yields \( 1 = \ln a \ln b \). This equation can always be solved in \( G \), as every non-zero real has a unique inverse in \( \mathbb{R}^\times \) and \( \ln : G \to \mathbb{R}^\times \) has an inverse function. We will use this in part 2.

   If \( a \) and \( b \) solve \( 1 = \ln a \ln b \) then it is easy to see that \( b * a \) must also be \( e \).

   Associativity follows from

\[
(a * b) * c = (a^{\ln b}) * c = (a^{\ln b})^{\ln c} = a^{\ln b \ln c} = a^{\ln b} \ln c = a^{\ln b \ln c} = a^{\ln (b * c)} = a * (b * c)
\]
So, $G$ is group. Let us check that it is Abelian. This follows from

\[
    a * b = a^{\ln b} = (e^{\ln a})^{\ln b} = e^{\ln a \ln b} = e^{\ln b \ln a} = (e^{\ln b})^{\ln a} = b^{\ln a} = b * a
\]

2. Consider $\ln : G \to \mathbb{R}^\times$. We know this function has an inverse, the restriction of $e^x$ to $\mathbb{R}^\times$. But, is this a homomorphism? Yes, it is!

\[
    \ln (a * b) = \ln \left( (e^{\ln a})^{\ln b} \right) = \ln b \ln a
\]

2. Let $G_1, G_2$ be groups.

1. If $H_1 \leq G_1$ and $H_2 \leq G_2$ prove that $H_1 \times H_2 \leq G_1 \times G_2$.

2. TRUE/FALSE : If $H \leq G_1 \times G_2$ then $H = H_1 \times H_2$ for some $H_1 \leq G_1$ and some $H_2 \leq G_2$. Prove your answer!

Solution.

1. Assume $H_1 \leq G_1$ and $H_2 \leq G_2$, thus $H_1 \times H_2$ is non-empty. Let $(h_1, h_2), (g_1, g_2) \in H_1 \times H_2$, then

\[
    (h_1, h_2)(g_1, g_2)^{-1} = (h_1, h_2)(g_1^{-1}, g_2^{-1}) = (h_1 g_1^{-1}, h_2 g_2^{-1})
\]

which is an element of $H_1 \times H_2$ because of closure of $H_1$ and $H_2$.

2. False: Consider $G = \mathbb{Z} \times \mathbb{Z}$, and $H$ the group generated by $(1, 1)$, which is clearly isomorphic to $\mathbb{Z}$.

Since a subgroup of $G$ of the form $H_1 \times H_2$ with $H_1, H_2 \leq \mathbb{Z}$ can be isomorphic to $\mathbb{Z}$ only if one of $H_1$ or $H_2$ is trivial, then our group $H$ must be contained in $\mathbb{Z}$, which is impossible, as $H$ is generated by $(1, 1)$.

3. If $\phi : S_3 \to \mathbb{Z}_3$ is a group homomorphism, show that $\phi(g) = 0$ for all $g \in S_3$. 
Solution. Since $S_3$ is generated by 2-cycles then we just need to see what $\phi$ does to these elements. Now, since 2-cycles have order two, then the order of their images under $\phi$ must have order two or one (divisors of 2). It follows that $\phi$ must send 2-cycles to the identity of $\mathbb{Z}_3$ because this group does not have element of order 2. Since every generator of $S_3$ is mapped to 0 then every element in $S_3$ is mapped to zero under $\phi$.

4. Define $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([x]_{mn}) = ([x]_m, [x]_n)$. Show that $f$ is well-defined, and that $f$ is bijective if and only if $gcd(m, n) = 1$.

Solution. Let $[x]_{mn} = [y]_{mn}$, that is $x = y + m\alpha$ for some $\alpha \in \mathbb{Z}$. Then,

$$f([x]_{mn}) = ([x]_m, [x]_n) = ([y + m\alpha]_m, [y + m\alpha]_n) = ([y]_m, [y]_n) = f([y]_{mn})$$

So, $f$ is well-defined.

In order to see if $f$ is onto we need to check if for $([a]_m, [b]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$ there is an $[x]_{mn} \in \mathbb{Z}_{mn}$ such that $f([x]_{mn}) = ([a]_m, [b]_n)$. In other words, we are looking for an $x \in \mathbb{Z}$ that solves the congruences

$$x \equiv a \pmod{m} \quad \quad \quad x \equiv b \pmod{n}$$

simultaneously.

We know that such an $x$ exists if $gcd(m, n) = 1$ because of the Chinese Remainder Theorem.

Since $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same number of elements, then assuming $gcd(m, n) = 1$ implies that $f$ is bijective.

If we assume that $f$ is bijective, then we get a unique solution modulo $n$ for the two congruences above. But, if $gcd(m, n) = d \neq 1$ then for $x$ a solution of the congruences above we get another solution (distinct from $x$ modulo $mn$), namely $y = x + \frac{mn}{d}$. This is a contradiction, so $d = 1$.

5. Let $H \leq G$ and for any $g \in G$ define $n_H(g)$ to be the least positive integer such that $g^{n_H(g)} \in H$. Show that $n_H(g)$ divides the order of $g$.

Solution. Note that we will not use the normality of $H$ for this proof. There are other proofs that might use it, though.

Let $H \leq G$ and for $g \in G$ define $n_H(g)$ as above. Let $m$ be the order of $g$.

Since $g^m = e$, then $g^m \in H$. It follows that $n_H(g) \leq m$, thus we can use the division (Euclidean) algorithm to get

$$m = n_H(g)q + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < n_H(g)$. 
Note that
\[ g^m = g^{n_H(g)q + r} = g^{n_H(g)q}g^r. \]
which implies
\[ (g^{n_H(g)q})^{-1}g^m = g^r. \]
Since both \( g^{n_H(g)q} \) and \( g^m \) live in \( H \), then so does \( g^r \). If \( r \) were non-zero then there would be a positive integer that is less than \( n_H(g) \) such that \( g^r \in H \). This is a contradiction, so \( r = 0 \) and thus \( n_H(g) \mid m \).

6. Let \( R \) be a commutative ring. An element \( r \in R \) is called nilpotent if \( r^n = 0 \) for some integer \( n > 0 \). Prove that \( a + b \) is nilpotent if \( a \) and \( b \) are nilpotent elements of \( R \).

**Solution.** Assume \( a^n = b^m = 0 \), then since the ring is commutative we get
\[
(a + b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}
\]
\[
= \sum_{k=0}^{n} \binom{m+n}{k} a^k b^{m+n-k} + \sum_{k=n+1}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}
\]
For \( 0 \leq k \leq n \), \( m + n - k > m \) and thus \( b^{m+n-k} = 0 \). Thus the first sum is \( n \) zero summands. Similarly, for \( n + 1 \leq k \leq m + n \) we get \( a^k = 0 \), which implies that the second sum is also zero. Hence, \((a + b)^{m+n} = 0\).

7. Show that the set of matrices \( A \in M_n(\mathbb{R}) \) such that \( Av = 0 \) for some fixed \( v \in \mathbb{R}^n \) is a left ideal of \( M_n(\mathbb{R}) \).

**Solution.** Fix \( v \in \mathbb{R}^n \). Let \( I = \{ A \in M_n(\mathbb{R}); \ Av = 0 \} \).
It is clear that the zero matrix is in \( I \), and thus \( I \) is non-empty. Now let \( A, B \in I \), then
\[
(A - B)v = Av - Bv = 0 - 0 = 0
\]
which means that \( A - B \in I \).
Now let \( A \in I \) and \( B \in M_n(\mathbb{R}) \), then
\[
(BA)v = B(Av) = B \cdot 0 = 0
\]
which means that \( BA \in I \).
It follows that \( I \) is a left ideal.
8. Let

\[ S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R}) \]

1. Show that \( S \) is a subring of \( M_2(\mathbb{R}) \), the ring of \( 2 \times 2 \) matrices with real entries.

2. Show that \( S \) and \( \mathbb{C} \) are isomorphic rings.

Solution.

1. \( S \) is non-empty as the zero matrix and the identity matrix are elements of \( S \).

Now take two elements in \( S \) and subtract them

\[
\begin{bmatrix} a & b \\ -b & a \end{bmatrix} - \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \begin{bmatrix} a - \alpha & b - \beta \\ -(b - \beta) & a - \alpha \end{bmatrix}
\]

which is an element of \( S \).

Similarly, the product of two elements of \( S \) is

\[
\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \begin{bmatrix} a\alpha - b\beta & a\beta + b\alpha \\ -(b\alpha + a\beta) & a\alpha - b\beta \end{bmatrix}
\]

which is also an element of \( S \).

2. Consider the map \( \phi : S \to \mathbb{C} \) defined by

\[ \phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a + bi \]

Since

\[
\phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \begin{bmatrix} a + \alpha & b + \beta \\ -(b + \beta) & a + \alpha \end{bmatrix}
\]

\[
= (a + \alpha) + (b + \beta)i
\]

\[
= (a + bi) + (\alpha + \beta i)
\]

and

\[
\phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} = \phi \begin{bmatrix} a\alpha - b\beta & a\beta + b\alpha \\ -(b\alpha + a\beta) & a\alpha - b\beta \end{bmatrix}
\]

\[
= (a\alpha - b\beta) + (a\beta + b\alpha)i
\]

\[
= (a + bi)(\alpha + \beta i)\]
then $\phi$ is a homomorphism of rings.

The kernel of $\phi$ is

$$Ker(\phi) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} ; \phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} ; a + bi = 0 \right\} = \{0\}$$

So, $\phi$ is one-to-one. Checking onto is easy, as for any $a + bi \in \mathbb{C}$

$$\phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a + bi$$
Part B.

1. Recall that $\mathcal{P}_5$ is the set containing the zero polynomial and all polynomials of degree at most five with real coefficients. Show that the derivative defines a linear transformation from $\mathcal{P}_5$ to itself. Is it onto? Find the matrix for this map in the standard basis.

Solution. Since for any pair of differentiable functions (including polynomials) $f$ and $g$, and any constant $C$ we have

$$(f + g)' = f' + g' \quad \text{and} \quad (Cf)' = Cf'$$

then the derivative behaves linearly. Moreover, since the derivative of a polynomial of degree at most five is of degree at most four, and $0' = 0$, then the function is from $\mathcal{P}_5$ to $\mathcal{P}_5$. Also, since there is no way to obtain $p(x) = x^5$ as the derivative of a polynomial of degree at most five (its anti-derivative has degree six), then $\phi$ is not onto.

The standard basis for $\mathcal{P}_5$ is $B = \{1, x, x^2, x^3, x^4, x^5\}$. Since

$\phi(1) = 0 \quad \phi(x) = 1 \quad \phi(x^2) = 2x \quad \phi(x^3) = 3x^2 \quad \phi(x^4) = 4x^3 \quad \phi(x^5) = 5x^4$

then the matrix of $\phi$ with respect to $B$ is

$$
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 \\
0 & 0 & 0 & 0 & 0 & 5 \\
0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

2. Show that

$$U = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } a + b + c + d = 0 \right\} \subset M_2(\mathbb{R})$$

is a subspace of $M_2(\mathbb{R})$. Find a basis for $U$.

Solution. Probably the easiest way to do this is to go ahead and re-write $U$ as the span of a set of vectors (which will turn out being its basis).
We use \(a + b + c + d = 0\) to get \(d = -a - b - c\). Thus an element of \(U\) looks like
\[
\begin{bmatrix}
  a & b \\
  c & d
\end{bmatrix}
= \begin{bmatrix}
  a & b \\
  c & -a - b - c
\end{bmatrix}
= \begin{bmatrix}
  a & 0 \\
  0 & -a
\end{bmatrix} + \begin{bmatrix}
  0 & b \\
  0 & -b
\end{bmatrix} + \begin{bmatrix}
  0 & 0 \\
  c & -c
\end{bmatrix}
= a\begin{bmatrix}
  1 & 0 \\
  0 & -1
\end{bmatrix} + b\begin{bmatrix}
  0 & 1 \\
  0 & -1
\end{bmatrix} + c\begin{bmatrix}
  0 & 0 \\
  1 & -1
\end{bmatrix}
\]
Since the coefficients \(a, b\) and \(c\) can take any values, then \(U\) is the span of
\[
\mathcal{B} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & -1 \end{bmatrix} \right\}
\]
which makes \(U\) a subspace of \(M_2(\mathbb{R})\).
The matrices in \(\mathcal{B}\) are clearly linearly independent, thus \(\mathcal{B}\) is a basis of \(U\).

3. Find a basis for the orthogonal complement of the subspace \(W = \text{span}\{(1, 2, -1, 0), (0, 1, 1, 3)\}\) of \(\mathbb{R}^4\).

Solution. Any vector that is orthogonal to every element of \(W\) must be orthogonal to both \((1, 2, -1, 0)\) and \((0, 1, 1, 3)\) (and vice-versa). Thus, a vector \((x, y, z, w) \in W^\perp\) must be a solution of the system of equations
\[
x + 2y - z = 0 \quad y + z + 3w = 0
\]
Solving for \(x\) in the first equation and for \(w\) in the second we get
\[
x = -2y + z \quad w = -\frac{y}{3} - \frac{z}{3}
\]
Thus, the vectors \((x, y, z, w) \in W^\perp\) look like
\[
(x, y, z, w) = \left(-2y + z, y, z, -\frac{y}{3} - \frac{z}{3}\right)
= \left(-2y, y, 0, -\frac{y}{3}\right) + \left(z, 0, z, -\frac{z}{3}\right)
= y\left(-2, 1, 0, -\frac{1}{3}\right) + z\left(1, 0, 1, -\frac{1}{3}\right)
\]
which says, given that \(y\) and \(z\) are free to roam all over \(\mathbb{R}\), that
\[
W^\perp = \text{span}\left\{ \left(-2, 1, 0, -\frac{1}{3}\right), \left(1, 0, 1, -\frac{1}{3}\right) \right\}
\]
Since the two vectors that span \(W^\perp\) are linearly independent (because one is not a multiple of the other), then they are a basis of \(W^\perp\).
4. Let $T$ be the linear transformation of $\mathbb{R}^3$ with standard matrix $\begin{bmatrix} 1 & 5 & 2 \\ 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix}$. Find the matrix of $T$ with respect to the basis $B = \{(1, 1, 1), (1, 1, 0), (1, 0, 0)\}$.

**Solution.** Let us denote the standard basis of $\mathbb{R}^3$ by $S$. The change of basis matrix (or transition matrix) from $B$ to $S$ is given by just "hanging" the vectors of $B$ to get $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

It follows that the matrix representing $T$ with respect to $B$ is $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 5 & 2 \\ 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Since $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{bmatrix}$
then the matrix representing $T$ with respect to $B$ is $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 5 & 2 \\ 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & 3 & -1 \end{bmatrix}$

5. Let $F : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ be any linear transformation such that $\text{Ker } F = \left\{ (x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \middle| \begin{array}{l} x_1 - 2x_2 + x_3 - x_4 = 0 \\ x_1 - x_2 - 2x_3 + x_4 = 0 \\ x_1 - 3x_2 + 4x_3 - 3x_4 = 0 \end{array} \right\}$.

1. Find the dimension of $\text{Ker } F$ and a basis for it.

2. Give an example of such a linear transformation $F$.

3. For the example you gave in (b), find a basis for the range of $F$.

**Solution.**
1. We need to solve the system given. The matrix that represents this (homogeneous) system is

\[ A = \begin{bmatrix}
1 & -2 & 1 & -1 \\
1 & -1 & -2 & 1 \\
1 & -1 & 4 & -3
\end{bmatrix} \]

Let us do some row operations in \( A \).

\[ A = \begin{bmatrix}
1 & -2 & 1 & -1 \\
1 & -1 & -2 & 1 \\
1 & -3 & 4 & -3
\end{bmatrix} \]

now we subtract \( R_1 \) from \( R_3 \) and \( R_2 \) \[ \rightarrow \begin{bmatrix}
1 & -2 & 1 & -1 \\
0 & 1 & -3 & 2 \\
0 & -1 & 3 & -2
\end{bmatrix} \]

now we add \( R_2 \) to \( R_3 \), and add 2\( R_2 \) to \( R_1 \) \[ \rightarrow \begin{bmatrix}
1 & 0 & -5 & 3 \\
0 & 1 & -3 & 2 \\
0 & 0 & 0 & 0
\end{bmatrix} \]

It follows that \( x_1 = 5x_3 - 3x_4 \) and that \( x_2 = 3x_3 - 2x_4 \). Thus the vectors in \( Ker(F) \) look like

\[(x_1, x_2, x_3, x_4) = (5x_3 - 3x_4, 3x_3 - 2x_4, x_3, x_4) = (5x_3, 3x_3, x_3, 0) + (-3x_4, -2x_4, 0, x_4) = x_3(5, 3, 1, 0) + x_4(-3, -2, 0, 1)\]

Since \( x_3 \) and \( x_4 \) have no restrictions then

\[ Ker(F) = \text{span}\{(5, 3, 1, 0), (-3, -2, 0, 1)\} \]

These vectors are linearly independent, thus they form a basis of \( Ker(F) \).

\[ \text{dim}(Ker(F)) = 2. \]

2. The map \( F : \mathbb{R}^4 \rightarrow \mathbb{R}^3 \) given by

\[ F(x_1, x_2, x_3, x_4) = (x_1 - 2x_2 + x_3 - x_4, x_1 - x_2 - 2x_3 + x_4, x_1 - 3x_2 + 4x_3 - 3x_4) \]

3. The range of \( F \) can be computed by looking at the column space of the matrix \( A \) used in part 1. of this problem. So, now we will do some column operations.
on $A$.

\[
A = \begin{bmatrix}
1 & -2 & 1 & -1 \\
1 & -1 & -2 & 1 \\
1 & -3 & 4 & -3
\end{bmatrix}
\]

now we subtract $C_1$ from $C_3$ and add $C_1$ to $C_4$

\[
\rightarrow \begin{bmatrix}
1 & -2 & 0 & 0 \\
1 & -1 & -3 & 2 \\
1 & -3 & 3 & -2
\end{bmatrix}
\]

now we add $\frac{2}{3}C_3$ to $C_4$, and $C_3$ to $C_2$

\[
\rightarrow \begin{bmatrix}
1 & -2 & 0 & 0 \\
1 & -4 & -3 & 0 \\
1 & 0 & 3 & 0
\end{bmatrix}
\]

Since $(1, 1, 1) = -\frac{1}{2}(-2, -4, 0) + \frac{1}{3}(0, -3, 3)$, then the column space is

\[
\text{span}\{(-2, -4, 0), (0, -3, 3)\} = \text{span}\{(1, 2, 0), (0, -1, 1)\}
\]

These two vectors are linearly independent, thus they form a basis of the range of $F$.

6. A square matrix $B$ is skew-symmetric if $B^T = -B$. Suppose that the square matrix $A$ is skew-symmetric and invertible. Prove that $A^{-1}$ is also skew-symmetric.

**Solution.** We know that $A^T = -A$ and that $A$ is invertible. Since $(A^T)^{-1} = (A^{-1})^T$, then $A^T$ is invertible. It follows that if we inverse both sides of $A^T = -A$ we get

\[
(A^{-1})^T = (A^T)^{-1} = (-A)^{-1} = -(A^{-1})
\]

which proves that $A^{-1}$ is also skew-symmetric.

7. Diagonalize the following matrix

\[
A = \begin{bmatrix}
1 & -2 & -1 \\
-1 & 1 & 1 \\
1 & 0 & -1
\end{bmatrix}
\]

Then give a basis of $\mathbb{R}^3$ for which $A$ ‘becomes’ diagonal.
Solution. We first find the characteristic polynomial of $A$.

$$
\chi_A(\lambda) = \det(A - \lambda I) = \begin{vmatrix}
1 - \lambda & -2 & -1 \\
-1 & 1 - \lambda & 1 \\
1 & 0 & -1 - \lambda \\
\end{vmatrix}
$$

$R_2 \mapsto R_2 + R_3$

$$
\begin{vmatrix}
1 - \lambda & -2 & -1 \\
0 & 1 - \lambda & -\lambda \\
1 & 0 & -1 - \lambda \\
\end{vmatrix}
$$

$C_3 \mapsto C_3 - C_2$

$$
\begin{vmatrix}
1 - \lambda & -2 & 1 \\
0 & 1 - \lambda & -1 \\
1 & 0 & -1 - \lambda \\
\end{vmatrix}
$$

$$
\begin{aligned}
&= -(1 - \lambda)^2(1 + \lambda) + 2 - (1 - \lambda) \\
&= -(1 - \lambda)^2(1 + \lambda) + (\lambda + 1) \\
&= (1 + \lambda)(1 - (1 - \lambda)^2) \\
&= (1 + \lambda)(2\lambda - \lambda^2) = \lambda(1 + \lambda)(2 - \lambda)
\end{aligned}
$$

It is easy to see that $\lambda = 0, -1, 2$ are the eigenvalues of $\chi_A(\lambda)$. Since the eigenvalues are distinct the matrix is diagonalizable.

We know that the base where $A$ ‘becomes’ diagonal is given by the eigenvectors of $A$. Let us find them.

For $\lambda = 0$

$$
[A|0] = \begin{bmatrix}
1 & -2 & -1 & 0 \\
-1 & 1 & 1 & 0 \\
1 & 0 & -1 & 0 \\
\end{bmatrix}
$$

now we subtract $R_3$ from $R_1$ and add $R_3$ to $R_2$

$$
\rightarrow \begin{bmatrix}
0 & -2 & -1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & -1 & 0 \\
\end{bmatrix}
$$

It follows that the eigenspace of $\lambda = 0$ is $\text{span}(1, 0, 1)$.

For $\lambda = -1$

$$
[A + I|0] = \begin{bmatrix}
2 & -2 & -1 & 0 \\
-1 & 2 & 1 & 0 \\
1 & 0 & 0 & 0 \\
\end{bmatrix}
$$

now we subtract $2R_3$ from $R_1$ and add $R_3$ to $R_2$

$$
\rightarrow \begin{bmatrix}
0 & -2 & -1 & 0 \\
0 & 2 & 1 & 0 \\
1 & 0 & 0 & 0 \\
\end{bmatrix}
$$
It follows that the eigenspace of $\lambda = -1$ is span$(0, 1, -2)$. For $\lambda = 2$

$$[A - 2I|0] = \begin{bmatrix} -1 & -2 & -1 & 0 \\ -1 & -1 & 1 & 0 \\ 1 & 0 & -3 & 0 \end{bmatrix}$$

now we add $R_3$ to $R_1$ and $R_2$

$$\rightarrow \begin{bmatrix} 0 & -2 & -4 & 0 \\ 0 & -1 & -2 & 0 \\ 1 & 0 & -3 & 0 \end{bmatrix}$$

It follows that the eigenspace of $\lambda = 2$ is span$(3, -2, 1)$. Thus, the basis of $\mathbb{R}^3$ where $A$ becomes

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

is

$$\mathcal{B} = \{(1, 0, 1), (0, 1, -2), (3, -2, 1)\}$$

8. Consider the subspace $U = \{(x, y, z) \in \mathbb{R}^3 | 2x - y - 3z = 0\} \subset \mathbb{R}^3$ and the set of vectors $S = \{(1, -1, 1), (4, 2, 2)\} \subset \mathbb{R}^3$.

1. Complete $S$ to a basis in $\mathbb{R}^3$.

2. Show that $U = \text{span}(S)$.

Solution.

1. If we show that $U = \text{span}(S)$ (part 2. of this problem), then a basis for the orthogonal complement of $U$ would complete $S$ to a basis of $\mathbb{R}^3$. Since $U$ is a plane through the origin in $\mathbb{R}^3$, then its orthogonal complement is given by its normal vector, which can be obtained by just looking at the coefficients of the equation that defines the plane, namely $N = (2, -1, -3)$.

So, $S \cup \{(2, -1, -3)\}$ is a basis of $\mathbb{R}^3$.

2. We plug the vectors in $S$ into $2x - y - 3z = 0$ (the equation that defines $U$) to check that these vectors belong to $U$, we get

$$2(1) - (-1) - 3(1) = 0 \quad 2(4) - (2) - 3(2) = 0$$

Thus $S \subset U$. Since the two vectors in $S$ are linearly independent and $U$ is a plane (dimension 2), then the vectors in $S$ must span all $U$. 


Part A. Do five of the following eight problems:

1. Show there are no integers \( n \) such that
   (a) \( S_2 \times S_5 \) is isomorphic to \( S_n \).
   (b) \( S_3 \times \mathbb{Z}/\mathbb{Z}_4 \) is isomorphic to \( S_n \).

2. Let \( G \) be a cyclic group of order 8. Prove that \( G \) has exactly one element of order 2. Does there exist a nonabelian group of order 8 with this property?

3. Prove that the map \( f : G \to G \), given by \( f(a) = a^{-1} \), is a group homomorphism if and only if the map \( g : G \to G \), given by \( g(a) = a^2 \), is a group homomorphism.

4. What is the order of \( \sigma = (1\ 10\ 4)(2\ 13)(1\ 12\ 8)(5\ 7)(6\ 9)(5\ 11) \)?

5. Let
   \[
   G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}
   \]
   Show that \( G \) is a group under matrix multiplication, and that
   \[
   H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\}
   \]
   is a subgroup of \( G \).

6. Let \( G \) be a group and \( H \) a subgroup of \( G \). Let \( N_H \) be the set of all \( x \in G \) such that \( xHx^{-1} = H \). Show that \( N_H \) is a subgroup of \( G \) containing \( H \), and that \( H \) is normal in \( N_H \). (The group \( N_H \) is called the normalizer of \( H \).)

7. Define a relation \( \sim \) on the set \( \mathbb{N} \) of natural numbers by \( a \sim b \) if and only if \( a^2 + b^2 \) is even. Prove that \( \sim \) is an equivalence relation.

8. Let \( F \) be a field and \( R \) any ring, and let \( \varphi : F \to R \) be a nonzero ring homomorphism. Prove that \( \ker(\varphi) = 0 \).
Part B. Solve five of the following eight problems:

1. Let \( v_1, v_2, v_3 \) be linearly independent vectors in a vector space \( V \). Show that the vectors \( v_1, 2v_1 + v_2, 3v_1 + 2v_2 + v_3 \) are also linearly independent.

2. Find explicitly a linear map \( f : \mathbb{R}^2 \rightarrow \mathbb{R}^3 \) such that \( f(2, 3) = (1, 2, 3) \) and \( f(1, 2) = (4, 5, 6) \). Is this linear function unique?

3. Give examples of three of the following:
   (a) Three vectors in \( \mathbb{R}^3 \) so that any two are linear independent, but the set of all three is linearly dependent.
   (b) Matrices \( M \) and \( N \) such that \( MN \neq NM \).
   (c) Linear maps
       \[
       f : \mathbb{R}^2 \rightarrow \mathbb{R}^4 \quad \quad \quad \quad \quad g : \mathbb{R}^4 \rightarrow \mathbb{R}^2
       \]
       such that \( g \circ f \) is invertible.
   (d) A matrix \( M \) such that \( M^3 = 0 \) but \( M^2 \neq 0 \).

4. Let \( P_2 = \{ p(x) = a + bx + cx^2 ; \ a, b, c \in \mathbb{R} \} \). Show that the map \( T : P_2 \rightarrow P_2 \) given by
   \[
   T(p) = \frac{d^2}{dx^2} ((x^2 + 1)p(x))
   \]
   is linear. Then find the matrix of \( T \) in the basis \( \{1, x, x^2\} \).

5. Consider the following vector subspaces of \( \mathbb{R}^3 \)
   \[
   A = \{(x, y, z) \in \mathbb{R}^3 \mid 2x + y + 3z = 0\}, \quad B = \text{span}\{(1, -2, 0)\}, \quad C = \text{span}\{(1, 1, -1)\}.
   \]
   Show that \( A \) is the direct sum of \( B \) and \( C \), that is \( A = B \oplus C \).

6. Consider the subspace \( U = \{(x, y, z) \in \mathbb{R}^3 \mid x + y - 2z = 0\} \subset \mathbb{R}^3 \) and the system of vectors \( S = \{v_1 = (1, 1, 1), v_2 = (5, -1, 2)\} \subset \mathbb{R}^3 \).
   (a) Show that \( U \) is the span of \( S \).
   (b) Complete \( S \) to a basis in \( \mathbb{R}^3 \).
7. Let $T$ be a linear operator on a vector space $V$, and let $x$ be an eigenvector of $T$ corresponding to the eigenvalue $\lambda$. For any positive integer $m$, prove that $x$ is an eigenvector of $T^m$ corresponding to the eigenvalue $\lambda^m$.

8. If an $n \times n$ matrix $A$ is diagonalizable, show that $\det(A)$ is equal to the product of the eigenvalues of $A$. 
Part A.

1. Show there are no integers $n$ such that

   (a) $S_2 \times S_5$ is isomorphic to $S_n$.
   (b) $S_3 \times \mathbb{Z}/\mathbb{Z}_4$ is isomorphic to $S_n$.

Solution:

(a) The order of $S_2 \times S_5$ is $2! \cdot 5! = 240$, which is not an $n$!

(b) The order of $G = S_3 \times \mathbb{Z}/\mathbb{Z}_4$ is $3! \cdot 4 = 4!$, so the only case to check is whether or not $G$ is isomorphic to $S_4$. However, the element $((123), 1) \in G$ has order 12, but there are no elements of order 12 in $S_4$. So, the groups cannot be isomorphic.

2. Let $G$ be a cyclic group of order 8. Prove that $G$ has exactly one element of order 2. Does there exist a nonabelian group of order 8 with this property?

Solution: A (multiplicative) cyclic group $G$ of order 8 can be written as

$$G = \{e, g, g^2, g^3, g^4, g^5, g^6, g^7\}$$

where $g^8 = e$.

It is easy to see that the orders of the non-trivial elements are

$$o(g) = 8 \quad o(g^2) = 4 \quad o(g^3) = 8 \quad o(g^4) = 2$$

$$o(g^5) = 8 \quad o(g^6) = 4 \quad o(g^7) = 8$$

Thus, $g^4$ is the only element of order two in $G$.

There are exactly two (non-isomorphic) non-abelian groups of order 8, namely $D_4$ and $Q_8$. If one thinks $D_4$ as the group of symmetries of a square, it is easy to see that the square admits 4 different reflections, these reflections have order two, so $D_4$ has at least 4 elements of order 2. On the other hand

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where $i^2 = j^2 = k^2 = -1$ (and some other multiplication rules that we don’t need right now). It follows that $x^2 = -1$ for all $x \in Q_8 \setminus \{\pm 1\}$. Hence, $-1$ is the only element of order two in $Q_8$. 
3. Prove that the map \( f : G \to G \), given by \( f(a) = a^{-1} \), is a group homomorphism if and only if the map \( g : G \to G \), given by \( g(a) = a^2 \), is a group homomorphism.

**Solution:** The easiest way to prove this could be to show that the two statements we want to show are equivalent are also equivalent with \( G \) being Abelian. First of all, if \( G \) is Abelian, then the two functions are clearly homomorphisms.

Now assume that \( f \) is a group homomorphism, then

\[
b^{-1}a^{-1} = (ab)^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}
\]

Since every element in a group is the inverse of some element in \( G \), then \( b^{-1}a^{-1} = a^{-1}b^{-1} \) forces \( G \) to be Abelian.

Finally, if \( g \) is a group homomorphism, then

\[
(ab)^2 = g(ab) = g(a)g(b) = a^2b^2
\]

Now we multiply \((ab)^2 = a^2b^2\) by \( a^{-1} \) by the left and \( b^{-1} \) by the right, then we get \( ba = ab \).

4. What is the order of \( \sigma = (1 \ 10 \ 4)(2 \ 13)(1 \ 12 \ 8)(5 \ 7)(6 \ 9)(5 \ 11) \)?

**Solution:** As the cycles are not disjoint we must first perform the multiplication of the cycles, we get

\[
\sigma = (1 \ 10 \ 4)(2 \ 13)(1 \ 12 \ 8)(5 \ 7)(6 \ 9)(5 \ 11) = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)
\]

Now that we have disjoint cycles we look at the order of each individual cycle, we get orders 5, 2, and 3. Thus the order of \( \sigma \) is \( 2 \cdot 3 \cdot 5 = 30 \) (as the orders are relatively prime).

5. Let

\[
G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \; ; \; a, b, c \in \mathbb{R}, \; ac \neq 0 \right\}
\]

Show that \( G \) is a group under matrix multiplication, and that

\[
H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \; ; \; b \in \mathbb{R} \right\}
\]

is a subgroup of \( G \).
**Solution:** First let us check closure of $G$.

\[
\begin{bmatrix}
a & b \\
0 & c
\end{bmatrix}
\begin{bmatrix}
d & e \\
0 & f
\end{bmatrix}
= \begin{bmatrix}
ad & ae + bf \\
0 & cf
\end{bmatrix}
\]

The product is in $G$ because its entries are in $\mathbb{R}$ and $(ad)(cf) \neq 0$, as $ac \neq 0$ and $df \neq 0$.

Note that if $a = c = d = f = 1$, then the diagonal entries of the product are also 1's. This shows closure of $H$.

Now note that

\[
\begin{bmatrix}
a & b \\
0 & c
\end{bmatrix}^{-1} = \begin{bmatrix}
a^{-1} & -ba^{-1}c^{-1} \\
0 & c^{-1}
\end{bmatrix}
\]

The inverse is in $G$ because its entries are in $\mathbb{R}$ and $a^{-1}c^{-1} \neq 0$, as $ac \neq 0$.

Note that if $a = c = 1$, then the diagonal entries of the inverse are also 1's. This shows the needed inverse property for $H$.

Associativity of $G$ follows directly from the associativity of $\mathbb{R}$.

Both $G$ and $H$ have identity equal to the identity $2 \times 2$ matrix. Hence, $G$ is a group and $H$ (clearly a subset of $G$) is a subgroup of $G$.

6. Let $G$ be a group and $H$ a subgroup of $G$. Let $N_H$ be the set of all $x \in G$ such that $xHx^{-1} = H$. Show that $N_H$ is a subgroup of $G$ containing $H$, and that $H$ is normal in $N_H$. (The group $N_H$ is called the normalizer of $H$.)

**Solution:** First of all, if $x \in H$, then $xHx^{-1} = H$ because of the closure of $H$. So, $H \subset N_H$.

Let $x, y \in N_H$, then

\[(xy)H(xy)^{-1} = x \left(yHy^{-1}\right)x^{-1} = xHx^{-1} = H\]

So, $N_H$ is closed.

Clearly the identity of $G$ is in $N_H$.

Now since $xHx^{-1} = H$ implies $x^{-1}Hx = H$ (because, for example, of the map $\varphi : G \to G$ defined by $\varphi(g) = xgx^{-1}$ being an isomorphism, and $\varphi^{-1}(g) = x^{-1}gx$).

Finally, if $x \in N_H$ then $xHx^{-1} = H$, implying that $H$ is normal in $N_H$. 
7. Define a relation ∼ on the set \( \mathbb{N} \) of natural numbers by \( a \sim b \) if and only if \( a^2 + b^2 \) is even. Prove that ∼ is an equivalence relation.

**Solution:** We need to show that ∼ is symmetric, reflexive and transitive. The first two are clear as if \( a^2 + b^2 \) is even then \( b^2 + a^2 \) is even, and \( a^2 + a^2 = 2a^2 \) being even.

Transitivity follows from the fact that the parity of \( a^2 + c^2 \) equals the parity of \( a^2 + c^2 + 2b^2 \), which is even, as it is the sum of the two even numbers \( (a^2 + b^2) \) and \( (b^2 + c^2) \).

8. Let \( F \) be a field and \( R \) any ring, and let \( \varphi: F \rightarrow R \) be a nonzero ring homomorphism. Prove that \( \ker(\varphi) = \{0\} \).

**Solution:** Since the kernel of \( \varphi \) is an ideal of the domain, then \( \ker(\varphi) \) is an ideal of the field \( F \). Since the only ideals in a field are \( \{0\} \) and the field itself, then \( \varphi \) is either 1 − 1 or the zero function. In this case, \( \varphi \) is a non-zero homomorphism, thus \( \ker(\varphi) = \{0\} \).
Part B. Solve five of the following eight problems:

1. Let $v_1, v_2, v_3$ be linearly independent vectors in a vector space $V$. Show that the vectors $v_1, 2v_1 + v_2, 3v_1 + 2v_2 + v_3$ are also linearly independent.

**Solution:** A linear combination of the vectors $v_1, 2v_1 + v_2, 3v_1 + 2v_2 + v_3$ equal to zero yields

$$
0 = \alpha v_1 + \beta (2v_1 + v_2) + \gamma (3v_1 + 2v_2 + v_3)
$$

$$
= (\alpha + 2\beta + 3\gamma)v_1 + (\beta + 2\gamma)v_2 + \gamma v_3
$$

So, using that $v_1, v_2, v_3$ be linearly independent vectors we get the system

$$
\begin{align*}
\alpha + 2\beta + 3\gamma &= 0 \\
\beta + 2\gamma &= 0 \\
\gamma &= 0
\end{align*}
$$

which has solution $\alpha = \beta = \gamma = 0$. Hence, the vectors $v_1, 2v_1 + v_2, 3v_1 + 2v_2 + v_3$ are linearly independent.

2. Find explicitly a linear map $f : \mathbb{R}^2 \to \mathbb{R}^3$ such that $f(2, 3) = (1, 2, 3)$ and $f(1, 2) = (4, 5, 6)$. Is this linear function unique?

**Solution:** First we write a generic element of $\mathbb{R}^2$ as a linear combination of the vectors $(2, 3)$ and $(1, 2)$,

$$(x, y) = \alpha(2, 3) + \beta(1, 2) = (2\alpha + \beta, 3\alpha + 2\beta)$$

So, $2\alpha + \beta = x$ and $3\alpha + 2\beta = y$. It follows that $\alpha = 2x - y$ and $\beta = -3x + 2y$. Thus,

$$(x, y) = (2x - y)(2, 3) + (-3x + 2y)(1, 2)$$

So,

$$f(x, y) = f[(2x - y)(2, 3) + (-3x + 2y)(1, 2)]$$

$$= f[(2x - y)(2, 3)] + f[(-3x + 2y)(1, 2)]$$

$$= (2x - y)f(2, 3) + (-3x + 2y)f(1, 2)$$

$$= (2x - y)(1, 2, 3) + (-3x + 2y)(4, 5, 6)$$

$$= (2x - y + 4(-3x + 2y), 2(2x - y) + 5(-3x + 2y), 3(2x - y) + 6(-3x + 2y))$$

$$= (-10x + 7y, -11x + 8y, -12x + 9y)$$
The construction of $f$ shows that the function is unique. Or, using that \{(2,3),(1,2)\} is a basis of $\mathbb{R}^2$ then the function, being defined on a basis, must be unique.

3. Give examples of three of the following:

(a) Three vectors in $\mathbb{R}^3$ so that any two are linear independent, but the set of all three is linearly dependent.
(b) Matrices $M$ and $N$ such that $MN \neq NM$.
(c) Linear maps $f: \mathbb{R}^2 \rightarrow \mathbb{R}^4$, $g: \mathbb{R}^4 \rightarrow \mathbb{R}^2$ such that $g \circ f$ is invertible.
(d) A matrix $M$ such that $M^3 = 0$ but $M^2 \neq 0$.

Solution:

(a) \{(1,0,0),(0,1,0),(1,1,0)\}

(b) Take, for example,

\[
M = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad N = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}
\]

(c) Consider

\[
f(x,y) = (x,y,0,0) \quad g(x,y,z,w) = (x,y)
\]

Then $g \circ f$ is the identity.

(d) Consider

\[
M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}
\]

4. Let $\mathcal{P}_2 = \{p(x) = a + bx + cx^2; \ a,b,c \in \mathbb{R}\}$. Show that the map $T: \mathcal{P}_2 \rightarrow \mathcal{P}_2$ given by

\[
T(p) = \frac{d^2}{dx^2} ((x^2 + 1)p(x))
\]

is linear. Then find the matrix of $T$ in the basis $\{1, x, x^2\}$.
Solution: Let us check linearity, we will use that the derivative is linear. Let \( \alpha \in \mathbb{R} \) and \( p(x), q(x) \in P_2 \).

\[
T(\alpha p(x) + q(x)) = \frac{d^2}{dx^2} \left[ (x^2 + 1)(\alpha p(x) + q(x)) \right] \\
= \frac{d^2}{dx^2} \left[ \alpha (x^2 + 1)p(x) + (x^2 + 1)q(x) \right] \\
= \frac{d^2}{dx^2} \left[ \alpha (x^2 + 1)p(x) \right] + \frac{d^2}{dx^2} \left[ (x^2 + 1)q(x) \right] \\
= \alpha \frac{d^2}{dx^2} \left[ (x^2 + 1)p(x) \right] + \frac{d^2}{dx^2} \left[ (x^2 + 1)q(x) \right] \\
= \alpha T(p(x)) + T(q(x))
\]

Now we look at the matrix in the standard basis

\[
T(1) = \frac{d^2}{dx^2} (x^2 + 1) = 2 \\
T(x) = \frac{d^2}{dx^2} (x^3 + x) = 6x \\
T(x^2) = \frac{d^2}{dx^2} (x^4 + x^2) = 12x^2 + 2
\]

So, the matrix is given by

\[
\begin{bmatrix}
2 & 0 & 2 \\
0 & 6 & 0 \\
0 & 0 & 12
\end{bmatrix}
\]

5. Consider the following vector subspaces of \( \mathbb{R}^3 \)

\[A = \{ (x, y, z) \in \mathbb{R}^3 \mid 2x+y+3z = 0 \}, \quad B = \text{span}\{(1, -2, 0)\}, \quad C = \text{span}\{(1, 1, -1)\}.\]

Show that \( A \) is the direct sum of \( B \) and \( C \), that is \( A = B \oplus C \).

Solution: First of all notice that \( (1, -2, 0) \) and \( (0, -3, 1) \) are linearly independent because one is not a multiple of the other. Also, since \( A \) is the solution set of a homogeneous linear equation in \( \mathbb{R}^3 \) then it is a plane, which is two-dimensional. So, if both \( (1, -2, 0) \) and \( (0, -3, 1) \) belong to \( A \) then the result follows.

Since both \( (1, -2, 0) \) and \( (0, -3, 1) \) clearly satisfy the equation \( 2x+y+3z = 0 \) then we are done.
6. Consider the subspace \( U = \{(x, y, z) \in \mathbb{R}^3 \mid x + y - 2z = 0\} \subset \mathbb{R}^3 \) and the system of vectors \( S = \{v_1 = (1, 1, 1), v_2 = (5, -1, 2)\} \subset \mathbb{R}^3 \).

   (a) Show that \( U \) is the span of \( S \).
   (b) Complete \( S \) to a basis in \( \mathbb{R}^3 \).

**Solution:**

(a) Just like the previous problem we first notice that \( v_1 \) and \( v_2 \) are linearly independent. Secondly, both vectors satisfy the equation that defines \( U \). Done.

(b) Note that \((1, 0, 0)\) is not a solution of the equation that defines \( U \), thus \((1, 0, 0)\) is not a linear combination of \( v_1 \) and \( v_2 \). So, \( \{(1, 0, 0), v_1, v_2\} \) is a linearly independent set in \( \mathbb{R}^3 \), it follows it is a basis (three linearly independent vectors in a three-dimensional space).

7. Let \( T \) be a linear operator on a vector space \( V \), and let \( x \) be an eigenvector of \( T \) corresponding to the eigenvalue \( \lambda \). For any positive integer \( m \), prove that \( x \) is an eigenvector of \( T^m \) corresponding to the eigenvalue \( \lambda^m \).

**Solution:** We know \( T(x) = \lambda x \). Note that
\[
T^m(x) = (T^{m-1} \circ T)(x) = T^{m-1}(\lambda x) = \lambda T^{m-1}(x)
\]
The result follows by just generalizing what is above to \( T^m(x) = \lambda^i T^{m-i}(x) \) for all \( i \) (or by using induction).

8. If an \( n \times n \) matrix \( A \) is diagonalizable, show that \( \det(A) \) is equal to the product of the eigenvalues of \( A \).

**Solution:** If \( A \) is diagonalizable, then there is a matrix \( P \) (change of basis) such that \( P A P^{-1} \) is a diagonal matrix \( D = \text{diag}(\lambda_1, \lambda_2, \cdots, \lambda_{n-1}, \lambda_n) \), where the \( \lambda_j \)'s are the eigenvalues of \( A \).

Since the determinant is a multiplicative function, then
\[
\det(D) = \det(P A P^{-1}) = \det(P) \det(A) \det(P^{-1}) = \det(P) \det(P^{-1}) \det(A)
\]
But, since \( \det(P^{-1}) = \det(P)^{-1} \), then \( \det(D) = \det(A) \). The result follows from the fact that the determinant of a diagonal matrix is given by the product of its diagonal entries.
Part A. Solve **five** of the following eight problems:

1. Let $\theta : \mathbb{Z} \to S_5$ be a group homomorphism such that $\theta(1) = (123)(45)$. Find $\theta(-4)$ and $\text{Ker} \, \theta$.

2. Let $G$ be the set of all real-valued functions defined on $\mathbb{R}$. Then $(G, +)$ is a group where $+$ stands for the usual addition of functions. Put $N = \{f \in G \mid f(2008) = 0\}$. Prove that $N \trianglelefteq G$ and $G/N \cong \mathbb{R}$.

3. **TRUE/FALSE**: $S_6 \cong S_3 \oplus S_5$. Prove your answer!

4. Let $G$ be a finite group and $k$ a natural number that is relatively prime to $|G|$. Prove that the map $\theta : G \to G : x \mapsto x^k$ is a bijection.

5. Let $G$ be a finite group, $N \trianglelefteq G$ and $H \leq G$ such that $|H|$ and $[G : N]$ are relatively prime. Prove that $H \leq N$.

6. Let $G = \mathbb{R} \setminus \{-1\}$. We define a binary operation $*$ on $G$ as follows:
   \[ a * b = ab + a + b \quad \text{for all} \quad a, b \in G \]
   It is given that $G$ is a group under this operation.
   (a) What is the identity element in $G$?
   (b) What is the inverse of $a \in G$?
   (c) Solve for $x : 2 * x * 3 = 7$

7. Let $R$ be a ring such that $a^2 = a$ for all $a \in R$.
   (a) Prove that $a + a = 0$ for all $a \in R$ (hint: consider $(a + a)^2$).
   (b) Prove that $R$ is commutative (hint: consider $(a + b)^2$).

8. Let $R$ be the set of all polynomials with real coefficients. Then $(R, +, \cdot)$ is a ring under the usual addition and multiplication of polynomials. Put $S = \{p(x) \in R \mid p'(0) = 0\}$ where $p'(x)$ is the usual derivative of $p(x)$ with respect to $x$.
   (a) Prove that $S$ is a subring of $R$.
   (b) Is $S$ an ideal of $R$?

---

Part B is on the back!!!
Part B. Solve five of the following eight problems:

1. Let $v_1, v_2, \ldots, v_k$ be linearly independent vectors in $\mathbb{R}^n$ and $A$ a non-singular $n \times n$ matrix. Prove that $Av_1, Av_2, \ldots, Av_k$ are linearly independent.

2. Let
   \[
   x_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 2 \\ 5 \\ 4 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}, \quad x_4 = \begin{pmatrix} 2 \\ 7 \\ 4 \end{pmatrix} \quad \text{and} \quad x_5 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}
   \]
   Find a subset of \{ $x_1, x_2, x_3, x_4, x_5$ \} that is a basis of $\text{span} \{ x_1, x_2, x_3, x_4, x_5 \}$.

3. Let $A$ and $B$ be similar $n \times n$ matrices. Prove that there exist $n \times n$ matrices $S$ and $T$ such that $S$ is non-singular, $A = ST$ and $B = TS$.

4. Let $T : \mathbb{R}^2 \to \mathbb{R}^3$ be a linear transformation such that $T \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ and $T \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Find $T \begin{pmatrix} x \\ y \end{pmatrix}$ for all $x, y \in \mathbb{R}$.

5. Let $V$ be the set of all polynomials of degree at most three. For $f(x), g(x) \in V$, we define the inner product of $f(x)$ and $g(x)$ as
   \[
   \langle f(x), g(x) \rangle = \int_0^1 f(x)g(x) \, dx
   \]
   Find a basis for the subspace $W$ of $V$ of all elements in $V$ that are orthogonal to $1 - x$.

6. Is the matrix $\begin{pmatrix} 1 & 0 & 0 \\ -2 & -1 & -3 \\ 2 & 2 & 4 \end{pmatrix}$ diagonalizable? Justify your answer!

7. Let $A$ be an $n \times n$ matrix, $\lambda, \mu$ two different eigenvalues of $A$, $x$ an eigenvector for $A$ corresponding to the eigenvalue $\lambda$ and $y$ an eigenvector for $A^T$ corresponding to the eigenvalue $\mu$. Prove that $x$ and $y$ are orthogonal.

8. Let $n$ be odd and $A$ an $n \times n$ matrix whose entries are real numbers. Prove that $A^2 + I \neq O$ where $I$ is the $n \times n$ identity matrix and $O$ is the $n \times n$ zero matrix (hint: determinants).
Part A.

1. Let $\theta : \mathbb{Z} \to S_5$ be a group homomorphism such that $\theta(1) = (123)(45)$. Find $\theta(-4)$ and $\text{Ker } \theta$.

**Solution.** $\theta$ is a homomorphism going from an additive group into a multiplicative group. Thus the homomorphism properties look like

$$\theta(n + m) = \theta(n)\theta(m) \quad \text{and} \quad \theta(-n) = \theta(n)^{-1}$$

So, as $\mathbb{Z}$ is cyclic with generator 1, and we know what $\theta(1)$ is, then

$$\theta(n) = \theta(1)^n = [(123)(45)]^n = (123)^n(45)^n$$

where the last step is obtained using that (123) and (45) are disjoint. Then,

$$\theta(-4) = (123)^{-4}(45)^{-4} = (321)^4(45)^4 = (321)$$

$$\text{Ker}(\theta) = \{n \in \mathbb{Z}; \ \theta(n) = e\}$$

$$= \{n \in \mathbb{Z}; \ [(123)(45)]^n = e\}$$

$$= \{n \in \mathbb{Z}; \ n \text{ is divisible by the order of } (123)(45)\}$$

$$= \{n \in \mathbb{Z}; \ 6 \text{ divides } n\} \quad \rightarrow \text{(the order of } (123)(45) \text{ is } 3 \cdot 2 = 6)$$

$$= 6\mathbb{Z}$$

2. Let $G$ be the set of all real-valued functions defined on $\mathbb{R}$. Then $(G, +)$ is a group where $+$ stands for the usual addition of functions. Put $N = \{f \in G \mid f(2008) = 0\}$. Prove that $N \trianglelefteq G$ and $G/N \cong \mathbb{R}$.

**Solution.** Consider the map $\phi : G \to \mathbb{R}$ defined by $\phi(f) = f(2008)$.

Let $f, g \in G$, then

$$\phi(f + g) = (f + g)(2008) = f(2008) + g(2008) = \phi(f) + \phi(g)$$

So, $\phi$ is a homomorphism of (additive) groups.

For any given $y \in \mathbb{R}$ consider the map $f_y : \mathbb{R} \to \mathbb{R}$ defined by $f_y(x) = y$ for all $x \in \mathbb{R}$. Since, $f_y \in G$ and $f_y(2008) = y$, then $\phi$ is onto.

It is easy to see that $\text{Ker}(\phi) = N$. Hence $N \trianglelefteq G$ and, by the first isomorphism theorem, $G/N \cong \mathbb{R}$. 
3. TRUE/FALSE : $S_6 \cong S_3 \oplus S_5$. Prove your answer!

**Solution.** False. Note that the element $((123), (12345)) \in S_3 \oplus S_5$ has order 15. On the other hand, $S_6$ does not have elements of order 15.

4. Let $G$ be a finite group and $k$ a natural number that is relatively prime to $|G|$. Prove that the map $\theta : G \to G : x \mapsto x^k$ is a bijection.

**Solution.** Since $|G| = n < \infty$, then we just need to show that $\theta$ is onto. We know that there are $\alpha, \beta \in \mathbb{Z}$ such that $1 = \alpha k + \beta n$, then

$$x = x^{\alpha k + \beta n} = x^{\alpha k} x^{\beta n} = x^{\alpha k} (x^n)^\beta = x^{\alpha k}$$

for all $x \in G$. So, $\theta(x^\alpha) = x$.

5. Let $G$ be a finite group, $N \trianglelefteq G$ and $H \leq G$ such that $|H|$ and $[G : N]$ are relatively prime. Prove that $H \leq N$.

**Solution.** Let $h \in H$, then the order of $hN \in G/N$ divides the order of $h$. It follows that the order of $hN$ is a common divisor of $[G : N]$ and $|H|$. Hence, the order of $hN$ is one, and thus $h \in N$.

6. Let $G = \mathbb{R} \setminus \{-1\}$. We define a binary operation $\ast$ on $G$ as follows :

$$a \ast b = ab + a + b \quad \text{for all } a, b \in G$$

It is given that $G$ is a group under this operation.

(a) What is the identity element in $G$?

(b) What is the inverse of $a \in G$?

(c) Solve for $x : 2 \ast x \ast 3 = 7$

**Solution.** First notice that the operation is commutative.

(a) We want to find $e$ such that $a = a \ast e = ae + a + e$ for all $a \in G$. It follows that

$$0 = ae + e = e(a - 1)$$

for all $a \in G$. It follows that $e = 0$. 
(b) We look for $b$ such that $0 = e = a * b = ab + a + b$. We solve for $b$ and we get

$$b = \frac{-a}{a + 1}$$

Note that we are using that $a + 1 \neq 0$, for all $a \in G$

(c) Since $2 * 3 = 2 \cdot 3 + 2 + 3 = 11$, then the equation becomes

$$11 \cdot x = 7$$

The inverse of 11 is

$$11^{-1} = \frac{-11}{12}$$

So,

$$x = \frac{-11}{12} \cdot 7 = \frac{-11}{12} \cdot 7 + \frac{-11}{12} \cdot 7 = \frac{-22}{3} + 7 = -\frac{1}{3}$$

7. Let $R$ be a ring such that $a^2 = a$ for all $a \in R$.

(a) Prove that $a + a = 0$ for all $a \in R$ (hint : consider $(a + a)^2$).

(b) Prove that $R$ is commutative (hint : consider $(a + b)^2$).

Solution.

(a) Using that $a^2 = a$ for all $a \in R$ we get

$$a + a = (a + a)^2 = a^2 + a + a + a^2 = 2(a + a)$$

So, $a + a = 0$, or $a = -a$.

(b) We now consider

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

So, $0 = ab + ba$. This together with part (a) imply $ab = ba$ for all $a, b \in R$

8. Let $R$ be the set of all polynomials with real coefficients. Then $(R, +, \cdot)$ is a ring under the usual addition and multiplication of polynomials. Put $S = \{p(x) \in R \mid p'(0) = 0\}$ where $p'(x)$ is the usual derivative of $p(x)$ with respect to $x$.

(a) Prove that $S$ is a subring of $R$.

(b) Is $S$ an ideal of $R$?
Solution.

(a) Let \( p, q \in S \), then

\[
(p - q)'(0) = p'(0) - q'(0) = 0
\]

and

\[
(pq)'(0) = p'(0)q(0) + p(0)q'(0) = 0
\]

So, both closure laws and the existence of additive inverses hold in \( S \). It is clear that \( S \) is nonempty, as the zero polynomial is in \( S \).

(b) Let \( p(x) = x^2 + 1 \in S \) and \( q(x) = x \in R \) we get that \( p(x)q(x) = x^3 + x \) and \( (pq)'(x) = 3x^2 + 1 \) which is nonzero at \( x = 0 \).

So, \( S \) is not an ideal of \( R \).
Part B.

1. Let \( v_1, v_2, \ldots, v_k \) be linearly independent vectors in \( \mathbb{R}^n \) and \( A \) a non-singular \( n \times n \) matrix. Prove that \( Av_1, Av_2, \ldots, Av_k \) are linearly independent.

Solution. Let \( \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{R} \) and consider

\[
0 = \alpha_1 Av_1 + \alpha_2 Av_2 + \cdots + \alpha_k Av_k
\]

which forces

\[
0 = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k
\]

because \( A \) is non-singular. But, since the \( v_i \)'s are linearly independent, then all the \( \alpha_i \)'s are zero.

2. Let

\[
\mathbf{x}_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} , \quad \mathbf{x}_2 = \begin{pmatrix} 2 \\ 5 \\ 4 \end{pmatrix} , \quad \mathbf{x}_3 = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} , \quad \mathbf{x}_4 = \begin{pmatrix} 2 \\ 7 \\ 4 \end{pmatrix} \text{ and } \mathbf{x}_5 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\]

Find a subset of \( \{ \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5 \} \) that is a basis of \( \text{span}\{ \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5 \} \).

Solution. Call \( S \) the space spanned by the \( \mathbf{x}_i \)'s.

Note that \( \mathbf{x}_4 - \mathbf{x}_2 = 2\mathbf{e}_2 \). Since we are in \( \mathbb{R} \), then we have \( \mathbf{e}_2 \in S \). Subtracting this from \( \mathbf{x}_5 \) we obtain \( \mathbf{e}_1 \in S \). Now that we have \( \mathbf{e}_1 \) and \( \mathbf{e}_2 \) we obtain \( \mathbf{e}_3 \) from either \( \mathbf{x}_4 \) or \( \mathbf{x}_2 \). It follows that \( S \) contains the canonical basis of \( \mathbb{R}^3 \), and thus \( S = \mathbb{R}^3 \).

Moreover, we obtained the canonical basis by only playing with \( \mathbf{x}_2, \mathbf{x}_4 \), and \( \mathbf{x}_5 \), then these three vectors define a basis of \( S \) (three generators in a space of dimension three).

3. Let \( A \) and \( B \) be similar \( n \times n \) matrices. Prove that there exist \( n \times n \) matrices \( S \) and \( T \) such that \( S \) is non-singular, \( A = ST \) and \( B = TS \).

Solution. Since \( A \) is similar to \( B \), then there is an invertible matrix \( P \) such that \( A = PBP^{-1} \).

Let \( S = P \) (invertible) and \( T = BP^{-1} \), then \( A = ST \) and \( B = TS \).
4. Let $T : \mathbb{R}^2 \to \mathbb{R}^3$ be a linear transformation such that $T \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ and $T \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Find $T \begin{pmatrix} x \\ y \end{pmatrix}$ for all $x, y \in \mathbb{R}$.

Solution. We need to write any vector $v = \begin{pmatrix} x \\ y \end{pmatrix}$ as a linear combination of $v_1 = \begin{pmatrix} 5 \\ 3 \end{pmatrix}$ and $v_2 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$.

So we set $v = \alpha v_1 + \beta v_2$, which yields the system of equations (the unknowns are $\alpha$ and $\beta$)

$$x = 5\alpha + 3\beta \quad y = 3\alpha + 2\beta$$

It follows that $\alpha = 2x - 3y$ and $\beta = 5y - 3x$. Hence,

$$T \begin{pmatrix} x \\ y \end{pmatrix} = T \left[ (2x - 3y) \begin{pmatrix} 5 \\ 3 \end{pmatrix} + (5y - 3x) \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right]$$

$$= (2x - 3y)T \begin{pmatrix} 5 \\ 3 \end{pmatrix} + (5y - 3x)T \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

$$= (2x - 3y) \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + (5y - 3x) \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} -x + 2y \\ 4x - 6y \\ 3x - 4y \end{pmatrix}$$

5. Let $V$ be the set of all polynomials of degree at most three. For $f(x), g(x) \in V$, we define the inner product of $f(x)$ and $g(x)$ as

$$\langle f(x), g(x) \rangle = \int_0^1 f(x)g(x) \, dx$$

Find a basis for the subspace $W$ of $V$ of all elements in $V$ that are orthogonal to $1 - x$.

Solution. Let $p(x) = \delta x^3 + ax^2 + bx + c \in W$. 

\[ \langle p(x), 1 - x \rangle = \int_0^1 p(x)(1 - x) \, dx \]
\[ = \int_0^1 -\delta x^4 + (\delta - a)x^3 + (a - b)x^2 + (b - c)x + c \, dx \]
\[ = \left( -\frac{\delta}{5}x^5 + \frac{\delta - a}{4}x^4 + \frac{a - b}{3}x^3 + \frac{b - c}{2}x^2 + cx + K \right) \bigg|_0^1 \]
\[ = -\frac{\delta}{5} + \frac{\delta - a}{4} + \frac{a - b}{3} + \frac{b - c}{2} + c \]

Since we want \( p(x) \) to be orthogonal to \( 1 - x \), then we are asking for
\[ -\frac{\delta}{5} + \frac{\delta - a}{4} + \frac{a - b}{3} + \frac{b - c}{2} + c = 0 \]
or
\[ c = -\left( \frac{\delta}{10} + \frac{a}{6} + \frac{b}{3} \right) \]

Thus,
\[ p(x) = \delta x^3 + ax^2 + bx - \left( \frac{\delta}{10} + \frac{a}{6} + \frac{b}{3} \right) \]
\[ = \delta \left( x^3 - \frac{1}{10} \right) + a \left( x^2 - \frac{1}{6} \right) + b \left( x - \frac{1}{3} \right) \]

Hence, a basis for \( W \) is
\[ \left\{ x^3 - \frac{1}{10}, x^2 - \frac{1}{6}, x - \frac{1}{3} \right\} \]

6. Is the matrix \[
\begin{bmatrix}
1 & 0 & 0 \\
-2 & -1 & -3 \\
2 & 2 & 4
\end{bmatrix}
\] diagonalizable? Justify your answer!

**Solution.** The characteristic polynomial of the matrix above (let’s call it \( A \)) is
\[
\chi_A(\lambda) = \left| \begin{array}{ccc}
1 - \lambda & 0 & 0 \\
-2 & -1 - \lambda & -3 \\
2 & 2 & 4 - \lambda
\end{array} \right| 
\]
\[ = (1 - \lambda) \left| \begin{array}{cc}
-1 - \lambda & -3 \\
2 & 4 - \lambda
\end{array} \right| 
\]
\[ = (1 - \lambda)(\lambda^2 - 3\lambda - 10) 
\]
\[ = (1 - \lambda)(\lambda - 5)(\lambda + 2) 
\]
Since all $A$'s eigenvalues are distinct, then $A$ is diagonalizable.

7. Let $A$ be an $n \times n$ matrix, $\lambda, \mu$ two different eigenvalues of $A$, $x$ an eigenvector for $A$ corresponding to the eigenvalue $\lambda$ and $y$ an eigenvector for $A^T$ corresponding to the eigenvalue $\mu$. Prove that $x$ and $y$ are orthogonal.

**Solution.** We know that $Ax = \lambda x$ (which implies $x^T A^T = \lambda x^T$) and that $A^T y = \mu y$.

Note that

$$
\lambda (x \cdot y) = \lambda (x^T y) \\
= (\lambda x^T) y \\
= (x^T A^T) y \\
= x^T (A^T y) \\
= x^T (\mu y) \\
= \mu (x^T y) \\
= \mu (x \cdot y)
$$

Since $\lambda \neq \mu$, then $\lambda (x \cdot y) = \mu (x \cdot y)$ forces $x \cdot y = 0$.

8. Let $n$ be odd and $A$ an $n \times n$ matrix whose entries are real numbers. Prove that $A^2 + I \neq O$ where $I$ is the $n \times n$ identity matrix and $O$ is the $n \times n$ zero matrix (hint : determinants).

**Solution.** If $A^2 + I = O$, then $A^2 = -I$, and thus $\det(A^2) = \det(-I)$. Since $n$ is odd $\det(-I) = -1$, then we get $\det(A)^2 = -1$, which forces $\det(A) \notin \mathbb{R}$. This contradicts the fact that the entries of $A$ are real.
Mathematics Department Qualifying Exam : Algebra  
Fall 2007

**Part A.** Solve five of the following eight problems:

1. **TRUE/FALSE:** Let $G$ be a group and $a, b \in G$. If $ab$ has order 3 then $ba$ has order 3.
   Prove your answer!

2. **TRUE/FALSE:** Let $R$ be an integral domain and $A$ a proper ideal of $R$. Then $R/A$ is an integral domain.
   Prove your answer!

3. **TRUE/FALSE:** $D_{12} \cong \mathbb{Z}_3 \oplus D_4$
   Prove your answer!

4. Let $G$ be a group and $H$ and $K$ finite subgroups of $G$ such that $|H|$ and $|K|$ are relatively prime. Prove that $H \cap K = \{1\}$.

5. Let $G$ be a group. Consider the map $f : G \to G : a \mapsto a^{-1}$. Prove that $G$ is abelian if and only if $f$ is a group homomorphism.

6. Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication and
   \[ H = \{ g \in \mathbb{R}^* | g^m \in \mathbb{Q} \text{ for some nonzero integer } m \} \]
   Prove that $H$ is a subgroup of $\mathbb{R}^*$.

7. Find an element of order 10 in $A_9$. Prove that the order is indeed 10.

8. Let $R$ be the set of $2 \times 2$-matrices with real entries:
   \[ R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\} \]
   Then $R$ forms a ring under matrix addition and matrix multiplication. Put
   \[ S = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in R \right\} \]
   - Prove that $S$ is a subring of $R$.
   - Is $S$ an ideal of $R$?

---

**Part B is on the back!!!**
Part B. Solve five of the following eight problems:

1. Let $A$ be an $n \times n$-matrix. Prove that $\det(AA^T) \geq 0$.

2. Let $u$ be a fixed vector in $\mathbb{R}^n$. Show that the set of all vectors in $\mathbb{R}^n$ that are orthogonal to $u$ is a subspace of $\mathbb{R}^n$.

3. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}$. Find a matrix $P$ such that $P^{-1}AP$ is a diagonal matrix.

4. Let $A$ be an $n \times n$-matrix and $\lambda$ and eigenvalue of $A$. Prove that $\lambda^k$ is an eigenvalue of $A^k$ for all positive integers $k$.

5. Let $L : V \to W$ be a linear transformation. If $\{v_1, v_2, \ldots, v_k\}$ spans $V$, show that $\{L(v_1), L(v_2), \ldots, L(v_k)\}$ spans range($L$).

6. Find an orthogonal basis for

$$S = \text{span}\left\{ \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}^T, \begin{bmatrix} 0 & 1 & -1 & 1 \end{bmatrix}^T, \begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}^T \right\}$$

7. Let $A$ and $B$ be symmetric $n \times n$-matrices. Prove that $AB$ is symmetric if and only if $AB = BA$.

8. Suppose that $\{v_1, v_2, \ldots, v_k\}$ is a set of linearly independent vectors in $\mathbb{R}^n$. Prove that

$$\{v_1, v_1 + v_2, v_1 + v_2 + v_3, \ldots, v_1 + v_2 + \cdots + v_k\}$$

is also linearly independent.
Part A.

1. TRUE/FALSE : Let $G$ be a group and $a, b \in G$. If $ab$ has order 3 then $ba$ has order 3.

Solution. Note that

$$(ba)^3 = b(ab)^2a = b(ab)^{-1}a = b(b^{-1}a^{-1})a = e$$

Then, the order of $ba$ is one or three. If it were one, then $b = a^{-1}$, which contradicts $ab$ having order 3.

2. TRUE/FALSE : Let $R$ be an integral domain and $A$ a proper ideal of $R$. Then $R/A$ is an integral domain.

Solution. False. For $n$ not a prime number, the ring $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

3. TRUE/FALSE : $D_{12} \cong \mathbb{Z}_3 \oplus D_4$

Solution. False. $D_{12}$ has 13 elements of order 2, but since $D_4$ has exactly 5 elements of order 2 and $\mathbb{Z}_3$ has none, then $\mathbb{Z}_3 \oplus D_4$ has just 5 elements of order 2.

4. Let $G$ be a group and $H$ and $K$ finite subgroups of $G$ such that $|H|$ and $|K|$ are relatively prime. Prove that $H \cap K = \{1\}$.

Solution. We know that the intersection of two subgroups, $H$ and $K$, is also a subgroup (that is a subgroup of both $H$ and $K$). So, the order of $H \cap K$ divides both $|H|$ and $|K|$, thus $|H \cap K|$ must be one, as $(|H|, |K|) = 1$.

5. Let $G$ be a group. Consider the map $f : G \to G : a \to a^{-1}$. Prove that $G$ is abelian if and only if $f$ is a group homomorphism.

Solution. We know that $(ab)^{-1} = b^{-1}a^{-1}$.

Assuming $f$ is a homomorphism

$$b^{-1}a^{-1} = (ab)^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}$$

Since every element in a group has an inverse, then $cd = dc$ for all $c, d \in G$
Assuming that $G$ is Abelian.

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$$

6. Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication and

$$H = \{ g \in \mathbb{R}^* | g^m \in \mathbb{Q} \text{ for some nonzero integer } m \}$$

Prove that $H$ is a subgroup of $\mathbb{R}^*$.

**Solution.** Let $g, h \in H$, then there are integers $n, m$ such that $g^n \in \mathbb{Q}$ and $h^m \in \mathbb{Q}$.

Now consider

$$(gh^{-1})^mn = (g^m)(h^{-1})^mn = (g^n)(h^m)^{-n}$$

which is in $\mathbb{Q}$ because $\mathbb{Q}^*$ is a multiplicative group.

Since $1 \in H$, then $H$ is a subgroup of $\mathbb{R}^*$.

7. Find an element of order 10 in $A_9$. Prove that the order is indeed 10.

**Solution.** Consider $\sigma = (12)(34)(56789)$.

Since

$$\sigma = (12)(34567) = (12)(34)(59)(58)(57)(56)$$

then $\sigma \in A_9$.

The order of $\sigma$ is 10 because the order of a product of disjoint cycles is the $lcm$ of the orders of the cycles. In our case, the order of $\sigma$ is $lcm(2, 5) = 10$.

8. Let $R$ be the set of $2 \times 2$-matrices with real entries:

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

Then $R$ forms a ring under matrix addition and matrix multiplication. Put

$$S = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in R \right\}$$

- Prove that $S$ is a subring of $R$.
- Is $S$ an ideal of $R$?

**Solution.** This is problem number 4 in part A in the exam of Spring 2007.
Part B.

1. Let $A$ be an $n \times n$-matrix with entries in $\mathbb{R}$. Prove that $\det(AA^T) \geq 0$.

Solution. We know that $\det(A) = \det(A^T)$, and that $\det(AB) = \det(A)\det(B)$. So,

$$\det(AA^T) = \det(A)\det(A^T) = \det(A)^2$$

Since $\det(A) \in \mathbb{R}$, then $\det(AA^T) = \det(A)^2 \geq 0$.

2. Let $u$ be a fixed vector in $\mathbb{R}^n$. Show that the set of all vectors in $\mathbb{R}^n$ that are orthogonal to $u$ is a subspace of $\mathbb{R}^n$.

Solution. Let $v$ and $w$ be two vectors that are orthogonal with $u$, and let $\alpha \in \mathbb{R}$. Then,

$$u \cdot (v - w) = u \cdot v - u \cdot u = 0 - 0 = 0$$

and

$$u \cdot (\alpha v) = \alpha (u \cdot v) = \alpha(0) = 0$$

Since the zero vector is orthogonal to $u$, then the set of orthogonal vectors to $u$ is non-empty.

3. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}$. Find a matrix $P$ such that $P^{-1}AP$ is a diagonal matrix.

Solution. We first look at the characteristic polynomial of $A$

$$\chi_A(\lambda) = \begin{vmatrix} 1 - \lambda & 3 \\ 2 & 2 - \lambda \end{vmatrix}$$

$$= (1 - \lambda)(2 - \lambda) - 6$$

$$= \lambda^2 - 3\lambda - 4$$

$$= (\lambda - 4)(\lambda + 1)$$

We know that there is a matrix $P$ such that

$$P^{-1}AP = \begin{bmatrix} -1 & 0 \\ 0 & 4 \end{bmatrix}$$

In order to find $P$ we need to find eigenvectors for the two eigenvalues of $A$. For $\lambda = -1$ we have to solve the equation $Av = -v$, which yields the system of equations

$$x + 3y = -x \quad \quad 2x + 2y = -y$$
which has solution space spanned by $(3, -2)$.

For $\lambda = 4$ we have to solve the equation $Av = 4v$, which yields the system of equations

\[
x + 3y = 4x \\
2x + 2y = 4y
\]

which has solution space spanned by $(1, 1)$.

It follows that

\[
P = \begin{bmatrix} 3 & 1 \\ -2 & 1 \end{bmatrix}
\]

4. Let $A$ be an $n \times n$-matrix and $\lambda$ and eigenvalue of $A$. Prove that $\lambda^k$ is an eigenvalue of $A^k$ for all positive integers $k$.

**Solution.** Let $v$ be an eigenvector of $A$ associated to the eigenvalue $\lambda$, that is $Av = \lambda v$.

Now note that

\[
A^k v = A^{k-1} (Av) = A^{k-1} (\lambda v) = \lambda (A^{k-1} v)
\]

Repeating the process above we see that $A^k v = \lambda^k v$.

5. Let $L : V \to W$ be a linear transformation. If $\{v_1, v_2, \ldots, v_k\}$ spans $V$, show that $\{L(v_1), L(v_2), \ldots, L(v_k)\}$ spans $\text{range}(L)$.

**Solution.** Let $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k \in V$. Then

\[
L(v) = L(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k) = \alpha_1 L(v_1) + \alpha_2 L(v_2) + \cdots + \alpha_k L(v_k)
\]

So, every element in the range of $L$ is a linear combination of the elements in the set $\{L(v_1), L(v_2), \ldots, L(v_k)\}$.

6. Find an orthogonal basis for

\[
S = \text{span}\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ -1 \\ 1 \end{bmatrix}^T, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}^T \right\}
\]

**Solution.** Note that $v_2 = \begin{bmatrix} 0 \\ 1 \\ -1 \\ 1 \end{bmatrix}^T$ and $v_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}^T$ are already orthogonal. So, what we want to do is to replace $v_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}^T$ with a vector in $S$ that is orthogonal to the last two.

Any element in $S$ looks like $v = \begin{bmatrix} x + z, \\ x + y, \\ z - y, \\ x + y + z \end{bmatrix}^T$ for some $x, y, z \in \mathbb{R}$.

Note that

\[
v \cdot v_2 = x + y + z - y + x + y + z = 2x + y + 2z
\]
and 
\[ \mathbf{v} \cdot \mathbf{v}_3 = x + z + z - y + x + y + z = 2x + 3z \]

Since we want \( \mathbf{v} \) to be orthogonal to both \( \mathbf{v}_2 \) and \( \mathbf{v}_3 \), then
\[ 2x + y + 2z = 0 = 2x + 3z \]

which forces \( y = z \), and thus we get \( 0 = 2x + 3z \). We now may take \( x = 3 \) and then \( y = z = -2 \). Finally,
\[ \mathbf{v} = \begin{bmatrix} 3 - 2, & 3 - 2, & 0, & 3 - 2 - 2 \end{bmatrix}^T = \begin{bmatrix} 1 & 1 & 0 & -1 \end{bmatrix}^T \]

So,
\[ \left\{ \begin{bmatrix} 1 & 1 & 0 & -1 \end{bmatrix}^T, \begin{bmatrix} 0 & 1 & -1 & 1 \end{bmatrix}^T, \begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}^T \right\} \]

is an orthogonal basis for \( S \).

Of course you may solve this using projections, but I thought this way was much more fun.

7. Let \( A \) and \( B \) be symmetric \( n \times n \)-matrices. Prove that \( AB \) is symmetric if and only if \( AB = BA \).

**Solution.** Assuming \( AB = BA \), \( A^T = A \) and \( B^T = B \).
\[ (AB)^T = B^T A^T = BA = AB \]

So, \( AB \) is symmetric.

Now assuming that \( AB \) is symmetric, \( A^T = A \) and \( B^T = B \).
\[ AB = (AB)^T = B^T A^T = BA \]

8. Suppose that \( \{ \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \} \) is a set of linearly independent vectors in \( \mathbb{R}^n \). Prove that
\[ \{ \mathbf{v}_1, \mathbf{v}_1 + \mathbf{v}_2, \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3, \ldots, \mathbf{v}_1 + \mathbf{v}_2 + \cdots + \mathbf{v}_k \} \]

is also linearly independent.

**Solution.** This is problem 1 in part B in the exam of Spring 2007.
Part A. Do five of the following eight problems.

1. Show that every subgroup of a cyclic group is cyclic.

2. Let $G$ be a group of symmetries of the square with vertices A, B, C, D (that is, the group of rigid motions of the plane which transform the square into itself). Let $H_1 \subset G$ be the subgroup of $G$ consisting of those symmetries which do not move the point A and $H_2 \subset G$ the subgroup of $G$ consisting of rotations. Is $H_1$ a normal subgroup of $G$? Is $H_2$ a normal subgroup of $G$? Justify your answer.

3. Prove that all groups of order 4 are abelian.

4. Let $R$ be the set of $2 \times 2$-matrices with real entries:

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

Then $R$ forms a ring under matrix addition and multiplication. Let

$$S = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in R \right\}$$

(a) Prove that $S$ is a subring of $R$.

(b) Is $S$ an ideal of $R$?

5. Consider the map $\theta : \mathbb{R}[x] \to \mathbb{R}$ given by $f(x) \mapsto f'(1)$, where $f'$ is the derivative of $f$.

(a) Is $\theta$ a group homomorphism from $(\mathbb{R}[x], +)$ to $(\mathbb{R}, +)$?

(b) Is $\theta$ a ring homomorphism from $(\mathbb{R}[x], +, \cdot)$ to $(\mathbb{R}, +, \cdot)$?

6. Give an example of a finite group $G$ and an integer $n$ such that $n$ divides the order of $G$ but $G$ has no subgroup of order $n$. Explain why $G$ has no such subgroup.

7. (a) Show that every field is an integral domain.

(b) Give an example of an integral domain that is not a field. Explain.

8. Let $\mathbb{Z}_5[x]$ be the ring of polynomials over the finite field $\mathbb{Z}_5$.

(a) Show that $f(x) = x^3 + 3x + 2$ is irreducible over $\mathbb{Z}_5$.

(b) Express $g(x) = x^4 + 4$ as a product of irreducible polynomials in $\mathbb{Z}_5[x]$. 
1. Suppose that $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k$ are vectors in $\mathbb{R}^n$.
   
   (a) If $\mathbf{y} = a_1 \mathbf{x}_1 + a_2 \mathbf{x}_2 + \cdots + a_k \mathbf{x}_k$ where $a_1 \neq 0$, show that $\text{span}\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\} = \text{span}\{\mathbf{y}, \mathbf{x}_2, \ldots, \mathbf{x}_k\}$.
   
   (b) If $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\}$ is independent, show that $\{\mathbf{x}_1, \mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3, \ldots, \mathbf{x}_1 + \mathbf{x}_2 + \cdots + \mathbf{x}_k\}$ is also independent.

2. Let $V$ be a vector space.
   
   (a) Show that if $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ is a linearly independent set of vectors in $V$, then so is every non-empty subset of $S$.
   
   (b) Show that if $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ is a linearly dependent set of vectors in $V$ and $\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n$ are any vectors in $V$, then $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$ is also linearly dependent.

3. Show that $A = \begin{bmatrix} 1 & 3 \\ -3 & -5 \end{bmatrix}$ is not diagonalizable.

4. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation given by $T(x, y) = (x + ky, -y)$. Show that $T$ is one-to-one for every real value of $k$ and that $T^{-1} = T$.

5. Let $\mathbf{v}_1 = \langle 0, 1, 0 \rangle$, $\mathbf{v}_2 = \langle -\frac{4}{5}, 0, \frac{3}{5} \rangle$, and $\mathbf{v}_3 = \langle \frac{3}{5}, 0, \frac{4}{5} \rangle$.
   
   (a) Check that $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is an orthonormal basis for $\mathbb{R}^3$ with the Euclidean inner product.
   
   (b) Express the vector $\mathbf{u} = \langle 1, 1, 1 \rangle$ as a linear combination of the vectors in $S$ and find the coordinates of $\mathbf{u}$ with respect to the basis $S$.

6. Find the characteristic polynomial, eigenvalues, and eigenvectors for $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 0 & -3 & 0 \end{bmatrix}$.

7. Suppose that $L : \mathbb{R}^3 \to \mathbb{R}^2$ is given by $L(x, y, z) = (x + 1, y - z)$. Is $L$ a linear transformation? Explain.

8. Compute the rank and nullity of $A = \begin{bmatrix} 1 & 2 & 3 \\ -1 & 2 & 1 \\ 3 & 1 & 2 \end{bmatrix}$. 
1. Show that every subgroup of a cyclic group is cyclic.

**Solution.** Let $G = \langle g \rangle$, and $H$ a subgroup of $G$. Let $i$ be the least positive integer such that $g^i \in H$.

Let $h \in H$, then $h = g^j$ for some $i \leq j$. Using the division algorithm we get that

$$j = iq + r$$

for some integers $q, r$ such that $0 \leq r < i$.

Note that $g^j = g^{iq+r} = g^iq^r$, thus $(g^iq)^{-1}g^r = g^r$, which forces $g^r \in H$ (as both $(g^iq)^{-1}$ and $g^j$ live in $H$). This yields a contradiction unless $r = 0$. It follows that $i$ divides $j$, and thus $H = \langle g^i \rangle$.

2. Let $G$ be a group of symmetries of the square with vertices A, B, C, D (that is, the group of rigid motions of the plane which transform the square into itself). Let $H_1 \subset G$ be the subgroup of $G$ consisting of those symmetries which do not move the point A and $H_2 \subset G$ the subgroup of $G$ consisting of rotations. Is $H_1$ a normal subgroup of $G$? Is $H_2$ a normal subgroup of $G$? Justify your answer.

**Solution.** The group of symmetries of the square is called $D_4$, its order is 8.

The group of all rotations, $H_2$, is cyclic of order 4. Since its index is two in $D_4$, then it is normal in $D_4$.

Note that $H_1$ can be considered as the group generated by a reflection (that fixes A), thus $H_1 \cap H_2 = \{e\}$ (otherwise a rotation would fix a vertex). It follows that $D_4 = H_1H_2$. So, if $H_1$ were normal, then $D_4$ would be Abelian. However, $D_4$ is not Abelian, as a clockwise rotation in 90 degrees followed by a reflection with diagonal axis $\ell$ is not the same as a reflection with axis $\ell$ followed by a clockwise rotation in 90 degrees.

3. Prove that all groups of order 4 are abelian.

**Solution.** Let $G = \{e, a, b, c\}$ be a group of order 4, and let $g \in G$.

If the order of some nonidentity element in $G$ is 4, then $G$ is cyclic of order four and thus Abelian.

If all nonidentity elements in $G$ have order two. Note that $ab$ cannot be $a$ or $b$ (that would force the existence of a second identity), thus $ab = c$, similarly $ba = c$. The same argument shows that $ac = ca = b$ and that $bc = cb = a$. Hence, $G$ is abelian.
4. Let $R$ be the set of $2\times 2$-matrices with real entries:

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

Then $R$ forms a ring under matrix addition and multiplication. Let

$$S = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in R \right\}$$

(a) Prove that $S$ is a subring of $R$.

(b) Is $S$ an ideal of $R$?

Solution.

(a) Let $M, N \in S$, then the difference $M - N$ is clearly in $S$. Also, since the zero matrix is in $S$, then the only thing left to prove is that $MN \in S$. But this follows from

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} x & 0 \\ y & z \end{bmatrix} = \begin{bmatrix} ax & 0 \\ cx + dy & dz \end{bmatrix} \in S$$

(b) $S$ is not an ideal of $R$ because, for example, using that the identity is in $S$ we get

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \notin S$$

5. Consider the map $\theta : \mathbb{R}[x] \to \mathbb{R}$ given by $f(x) \mapsto f'(1)$, where $f'$ is the derivative of $f$.

(a) Is $\theta$ a group homomorphism from $(\mathbb{R}[x], +)$ to $(\mathbb{R}, +)$?

(b) Is $\theta$ a ring homomorphism from $(\mathbb{R}[x], +, \cdot)$ to $(\mathbb{R}, +, \cdot)$?

Solution.

(a) We need to check if $\theta$ preserves the additive group operation of $\mathbb{R}[x]$.

$$\theta(p(x) + q(x)) = p'(1) + q'(1) = \theta(p(x)) + \theta(q(x))$$

So, $\theta$ is a group homomorphism from $(\mathbb{R}[x], +)$ to $(\mathbb{R}, +)$

(b) $\theta$ is not a ring homomorphism, as for $p(x) = x - 1$ and $q(x) = x^2$ we get

$$\theta(p(x)q(x)) = p'(1)q(1) + p(1)q'(1) = 1$$

and

$$\theta(p(x))\theta(q(x)) = p'(1)q'(1) = 2$$

6. Give an example of a finite group $G$ and an integer $n$ such that $n$ divides the order of $G$ but $G$ has no subgroup of order $n$. Explain why $G$ has no such subgroup.
Solution. We know that $A_5$ is simple, and that it has order 60. If $A_5$ had a subgroup of order 30, then that subgroup would have index two and, thus, it would be normal. It follows that $A_5$ has no subgroup of order 30.

7. (a) Show that every field is an integral domain.
   (b) Give an example of an integral domain that is not a field. Explain.

Solution.

(a) A field is clearly a commutative ring.
   Let $ab = 0$, with $a \neq 0$. Since in a field every nonzero element has an inverse, then $ab = 0$ implies $b = a^{-1}0 = 0$, so $b = 0$. It follows that every field has no zero divisors.

(b) $\mathbb{Z}$ has no zero divisors and, for example, 2 has no inverse in $\mathbb{Z}$

8. Let $\mathbb{Z}_5[x]$ be the ring of polynomials over the finite field $\mathbb{Z}_5$.
   (a) Show that $f(x) = x^3 + 3x + 2$ is irreducible over $\mathbb{Z}_5$.
   (b) Express $g(x) = x^4 + 4$ as a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

Solution.

(a) Since the degree of $f(x)$ is three, then for it to be irreducible over $\mathbb{Z}_5$ it is enough to check that it has no zeros (roots) in $\mathbb{Z}_5$. This is easy to check as (all computations in $\mathbb{Z}_5$!)

\[
\begin{align*}
  f(0) &= 2 \\
  f(1) &= 1 \\
  f(2) &= 1 \\
  f(3) &= 3 \\
  f(4) &= 3
\end{align*}
\]

(b) Since $4 \equiv -1 \pmod{5}$ then $g(x) = x^4 + 1 \in \mathbb{Z}_5[x]$. Factoring as usual we get

\[
g(x) = (x^2 - 1)(x^2 + 1) = (x^2 - 1)(x^2 - 4) = (x - 1)(x + 1)(x - 2)(x + 2)
\]

Since all the factors are linear we are done.
Part B.

1. Suppose that $x_1, x_2, \ldots, x_k$ are vectors in $\mathbb{R}^n$.

(a) If $y = a_1x_1 + a_2x_2 + \cdots + a_kx_k$ where $a_1 \neq 0$, show that $\text{span}\{x_1, x_2, \ldots, x_k\} = \text{span}\{y, x_2, \ldots, x_k\}$.

(b) Let $\{x_1, x_2, \ldots, x_k\}$ be a linear combination of the elements of the set $\{0 = x_1 + x_2 + \cdots + x_k\}$.

Solution.

(a) Note that $y \in \text{span}\{x_1, x_2, \ldots, x_k\}$, then we clearly have

$$\text{span}\{y, x_2, \ldots, x_k\} \subset \text{span}\{x_1, x_2, \ldots, x_k\}$$

Now let $v = \alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_kx_k \in \text{span}\{x_1, x_2, \ldots, x_k\}$

then

$$v = \frac{\alpha_1}{a_1}(a_1x_1) + \alpha_2x_2 + \cdots + \alpha_kx_k$$

$$= \alpha_1(\alpha_2x_2 + \cdots + \alpha_kx_k) + \alpha_2x_2 + \cdots + \alpha_kx_k - \frac{\alpha_1}{a_1}(a_2x_2 + \cdots + a_kx_k)$$

$$= \frac{\alpha_1}{a_1}y + \left(\alpha_2 - \frac{\alpha_1}{a_1}\right)x_2 + \cdots + \left(\alpha_k - \frac{\alpha_1}{a_1}\right)x_k$$

which is an element of $\text{span}\{y, x_2, \ldots, x_k\}$. So,

$$\text{span}\{x_1, x_2, \ldots, x_k\} \subset \text{span}\{y, x_2, \ldots, x_k\}$$

(b) Let

$$0 = \alpha_1x_1 + \alpha_2(x_1 + x_2) + \alpha_3(x_1 + x_2 + x_3) + \cdots + \alpha_k(x_1 + x_2 + \cdots + x_k)$$

be a linear combination of the elements of the set $\{x_1, x_1 + x_2, x_1 + x_2 + x_3, \ldots, x_1 + x_2 + \cdots + x_k\}$.

We re-write the previous equation as

$$0 = (\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_k)x_1 + (\alpha_2 + \alpha_3 + \cdots + \alpha_k)x_2 + \cdots + (\alpha_{k-1} + \alpha_k)x_{k-1} + \alpha_kx_k$$

which is a linear combination of the elements of the set $\{x_1, x_2, \ldots, x_k\}$. Since this set is linearly independent, then

$$0 = \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_k \quad 0 = \alpha_2 + \alpha_3 + \cdots + \alpha_k \quad 0 = \alpha_{k-1} + \alpha_k \quad 0 = \alpha_k$$

But, $0 = \alpha_k$ plugged into $0 = \alpha_{k-1} + \alpha_k$ yields $0 = \alpha_{k-1}$, and then we can repeat this process as many times as necessary to get that all the $\alpha_i$'s have to be zero! This implies that the set $\{x_1, x_1 + x_2, x_1 + x_2 + x_3, \ldots, x_1 + x_2 + \cdots + x_k\}$ is linearly independent.
2. Let \( V \) be a vector space.

(a) Show that if \( S = \{v_1, v_2, \ldots, v_r\} \) is a linearly independent set of vectors in \( V \), then so is every non-empty subset of \( S \).
(b) Show that if \( \{v_1, v_2, \ldots, v_r\} \) is a linearly dependent set of vectors in \( V \) and \( v_{r+1}, \ldots, v_n \) are any vectors in \( V \), then \( \{v_1, v_2, \ldots, v_r, v_{r+1}, \ldots, v_n\} \) is also linearly dependent.

Solution.

(a) If a non-empty subset \( T \) of \( S \) were linearly dependent, then there would be scalars (not all zero) that could be used to write a linear combination of the elements in \( T \) that is equal to zero. So, now we could extend this linear combination to a linear combination of the elements in \( S \) by just multiplying by zero the elements in \( S \setminus T \). This would yield a non-trivial linear combination of the elements of \( S \) that is equal to zero. A contradiction.

(b) Using the same idea used in part (a). If there is a non-trivial linear combination of the elements in \( \{v_1, v_2, \ldots, v_r\} \) that is equal to zero, then we extend it to the set \( \{v_1, v_2, \ldots, v_r, v_{r+1}, \ldots, v_n\} \) by just multiplying the elements \( v_{r+1}, \ldots, v_n \) by zero.

3. Show that \( A = \begin{bmatrix} 1 & 3 \\ -3 & -5 \end{bmatrix} \) is not diagonalizable.

Solution. The characteristic polynomial of \( A \) is

\[
\chi_A(\lambda) = \begin{vmatrix} 1 - \lambda & 3 \\ -3 & -5 - \lambda \end{vmatrix} = (1 - \lambda)(-5 - \lambda) + 9 = \lambda^2 + 4\lambda + 4 = (\lambda + 2)^2
\]

We now look at the eigenspace associated to \( \lambda = -2 \). We need to solve the equation \( Av = -2v \), which yields the system of equations

\[
\begin{align*}
x + 3y &= -2x \\
-3x - 5y &= -2y
\end{align*}
\]

which has solution space spanned by \((1, -1)\).

It follows that \( \lambda = -2 \) has geometric multiplicity one and algebraic multiplicity two. Hence, \( A \) is not diagonalizable.

4. Let \( T: \mathbb{R}^2 \to \mathbb{R}^2 \) be the linear transformation given by \( T(x, y) = (x + ky, -y) \). Show that \( T \) is one-to-one for every real value of \( k \) and that \( T^{-1} = T \).
Solution. Let us look at the kernel of $T$.

$$Ker(T) = \{(x, y) \in \mathbb{R}^2; T(x, y) = (0, 0)\}$$

$$= \{(x, y) \in \mathbb{R}^2; (x + ky, -y) = (0, 0)\}$$

$$= \{(x, y) \in \mathbb{R}^2; x + ky = 0 \text{ and } -y = 0\}$$

$$= \{(0, 0)\}$$

So, $T$ is one-to-one.

It is easy to see that $T \circ T(x, y) = (x, y)$ for all $(x, y) \in \mathbb{R}^2$.

5. Let $v_1 = (0, 1, 0)$, $v_2 = (-\frac{4}{5}, 0, \frac{3}{5})$, and $v_3 = (\frac{2}{5}, 0, \frac{4}{5})$.

(a) Check that $S = \{v_1, v_2, v_3\}$ is an orthonormal basis for $\mathbb{R}^3$ with the Euclidean inner product.

(b) Express the vector $u = (1, 1, 1)$ as a linear combination of the vectors in $S$ and find the coordinates of $u$ with respect to the basis $S$.

Solution.

(a) It is easy to check that the norm of $v_1, v_2$ and $v_3$ is one. Also,

$$\langle v_1, v_2 \rangle = 0 \quad \langle v_1, v_3 \rangle = 0 \quad \langle v_2, v_3 \rangle = -\frac{12}{25} + \frac{12}{25} = 0$$

Since a set of pairwise orthogonal vectors must be linearly independent, then $S$ is a set having three linearly independent vectors in a three-dimensional vector space, thus $S$ is a basis.

(b) We want to find $\alpha, \beta$ and $\gamma$ such that

$$u = \alpha v_1 + \beta v_2 + \gamma v_3$$

Since $v_2$ and $v_3$ have a zero in their second component, then $\alpha = 1$. So, we just need to solve the system

$$-\frac{4}{5} \beta + \frac{3}{5} \gamma = 1 \quad \frac{3}{5} \beta + \frac{4}{5} \gamma = 1$$

It follows that $\beta = -\frac{1}{5}$ and $\gamma = = \frac{7}{5}$. So,

$$u = \left(1, -\frac{1}{5}, \frac{7}{5}\right)$$

Express the vector $u = (1, 1, 1)$ as a linear combination of the vectors in $S$ and find the coordinates of $u$ with respect to the basis $S$.

6. Find the characteristic polynomial, eigenvalues, and eigenvectors for $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & -1 \\ 0 & -3 & 0 \end{bmatrix}$.
Solution. We first find the characteristic polynomial of $A$

$$
\chi_A(\lambda) = \begin{vmatrix}
1 - \lambda & 1 & 1 \\
0 & 2 - \lambda & -1 \\
0 & -3 & -\lambda
\end{vmatrix}
$$

$$
= (1 - \lambda) \begin{vmatrix}
2 - \lambda & -1 \\
-3 & -\lambda
\end{vmatrix}
$$

$$
= (1 - \lambda)(\lambda^2 - 2\lambda - 3)
$$

$$
= (1 - \lambda)(\lambda - 3)(\lambda + 1)
$$

Since all the eigenvalues of $A$ are distinct (they are $\lambda = -1, 1, \text{ and } 3$). Then $A$ is diagonalizable to

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

Now we look for eigenvectors. First of all, just by looking at $A$ we realize that $Ae_1 = e_1$, so that would be an eigenvector associated to the eigenvalue $\lambda = 1$.

For $\lambda = -1$ we need to solve the equation $Av = -v$, which yields the system of equations

$$
x + y + z = -x \\
2y - z = -y \\
-3y = -z
$$

which has solution subspace spanned by $(-2,1,3)$. Thus we can consider $(-2,1,3)$ as an eigenvector for $\lambda = -1$.

For $\lambda = 3$ we need to solve the equation $Av = 3v$, which yields the system of equations

$$
x + y + z = 3x \\
2y - z = 3y \\
-3y = 3z
$$

which has solution subspace spanned by $(0,1,-1)$. Thus we can consider $(0,1,-1)$ as an eigenvector for $\lambda = 3$.

7. Suppose that $L : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ is given by $L(x,y,z) = (x + 1, y - z)$. Is $L$ a linear transformation? Explain.

Solution. It is not. If this function were linear, then its kernel would be a subspace. However, since $L(0,0,0) = (1,0)$, then the zero vector is not in the ‘kernel’ of $L$. This is a contradiction.

8. Compute the rank and nullity of $A = \begin{bmatrix}
1 & 2 & 3 \\
-1 & 2 & 1 \\
3 & 1 & 2
\end{bmatrix}$.

Solution. Since the first two columns are linearly independent, then the rank is at least two. Now note that the sum of the first and second column yield the third column plus the vector $\begin{bmatrix}
0 \\
0 \\
2
\end{bmatrix}$. This implies that the third column is not in the span of the first two (the two zeros in the ‘extra vector’ do the work). It follows that the rank is three, and thus the nullity is zero.
Part A. Do five of the following eight problems.

1. Let $R$ be the ring of all continuous real valued functions on the closed interval $[0, 1]$. Prove that the map $\phi : R \to \mathbb{R}$ defined by $\phi(f) = \int_0^1 f(t) \, dt$ is a homomorphism of additive groups but not a ring homomorphism.

2. Show that the symmetric group $S_n$ ($n \geq 2$) is generated by the 2-cycles $(1\, 2), (2\, 3), \ldots, (n-1\, n)$.

3. Let $\mathbb{R}^\times$ denote the multiplicative group of nonzero real numbers and $\mathbb{R}$ denote the additive group of real numbers. Show that $\mathbb{R}^\times \cong \mathbb{R} \times \mathbb{Z}_2$.

4. An element $x$ in a ring $R$ is called nilpotent if $x^m = 0$ for some $m \in \mathbb{Z}^+$. Let $R$ be a commutative ring with $1 \neq 0$. Prove that if $a$ is a nilpotent element of $R$, then $1 - ab$ is a unit for all $b \in R$.

5. (a) Let $H = \{(1), (2\, 3)\}$. Is $H$ normal in $S_3$?
   (b) What is the order of the element $14 + \langle 8 \rangle$ in the quotient group $\mathbb{Z}_{24}/\langle 8 \rangle$?

6. Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

7. Prove that if $H$ and $K$ are finite subgroups of $G$ whose orders are relatively prime then $H \cap K = 1$.

8. Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.
   (a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.
   (b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.
Part B. Do five of the following eight problems.

1. Determine the dimension of the solution space (over the real numbers) to the system of equations

\[
\begin{align*}
    x_1 + x_2 &= 0 \\
    x_2 + x_3 &= 0 \\
    x_3 + x_4 &= 0 \\
    x_4 + x_5 &= 0 \\
    -x_1 + x_5 &= 0
\end{align*}
\]

2. Find a unit vector in \( \mathbb{R}^3 \) that is mutually perpendicular to \( v = (1, 2, 3) \) and \( w = (3, 2, 1) \).

3. Suppose

\[
A = \begin{pmatrix}
    1 & -1 & 0 & 2 \\
    -2 & 0 & 1 & 0 \\
    -1 & -1 & 0 & 3
\end{pmatrix}.
\]

Determine a basis over the reals for the image of the linear transformation \( L(v) = Av \).

4. Determine the inverse of the matrix

\[
\begin{pmatrix}
    0 & 0 & 0 & 1 \\
    0 & 0 & 2 & 0 \\
    0 & 3 & 0 & 0 \\
    4 & 0 & 0 & 0
\end{pmatrix}
\]

5. Suppose \( A \) is an invertible matrix. Prove \( (A^t)^{-1} = (A^{-1})^t \) where \( M^t \) and \( M^{-1} \) represent the transpose and inverse, respectively, of the matrix \( M \).

6. Determine an orthonormal basis for \( \text{span}\{(-1, 0, 0, 1), (0, 0, 1, -1), (1, -1, 0, 0)\} \).

7. State what it means (the definition) for a finite set of vectors to be linearly independent, and use this definition to prove the set of vectors \( \{(1, 1, 0), (0, 1, 1), (1, 0, 1)\} \) is linearly independent.

8. Determine the eigenvalues of the matrix

\[
\begin{pmatrix}
    2 & 2 & -5 \\
    3 & 7 & -15 \\
    1 & 2 & -4
\end{pmatrix}
\]
Part A.

1. Let $R$ be the ring of all continuous real valued functions on the closed interval $[0, 1]$. Prove that the map $\phi : R \rightarrow \mathbb{R}$ defined by $\phi(f) = \int_0^1 f(t) \, dt$ is a homomorphism of additive groups but not a ring homomorphism.

**Solution.** We know that
\[
\int (f + g) \, dt = \int f \, dt + \int g \, dt
\]
using this it is easy to show that $\phi$ is a homomorphism of additive groups. In fact
\[
\phi(f + g) = \int_0^1 [f(t) + g(t)] \, dt = \int_0^1 f(t) \, dt + \int_0^1 g(t) \, dt = \phi(f) + \phi(g)
\]
However, for the functions $f(t) = t$ and $g(t) = t$ we get
\[
\phi(fg) = \int_0^1 t^2 \, dt = \frac{1}{3} \neq \frac{1}{4} = \left( \int_0^1 t \, dt \right)^2 = \phi(f)\phi(g)
\]

2. Show that the symmetric group $S_n \ (n \geq 2)$ is generated by the 2-cycles $(1 \ 2), (2 \ 3), \ldots, (n-1 \ n)$.

**Solution.** First let us show that using these 2-cycles we can construct any 2-cycle. Call the set of elements above $T$.

Let $(a \ b)$ be a 2-cycle in $S_n$. WLOG assume $b = a + k + 1$ for some positive integer $k$.

Note that $(a \ a+1)$ is one of the cycles we can use, and that
\[
(a+1 \ b) = (a \ a+1)(a \ b)(a \ a+1)
\]
We now repeat this with $(a \ a+2)$ to get
\[
(a+2 \ b) = (a+1 \ a+2)(a+1 \ b)(a+1 \ a+2) = (a+1 \ a+2)(a \ a+1)(a \ b)(a \ a+1)(a+1 \ a+2)
\]
... etcetera, until we get
\[
(a+k \ b) = (a+k-1 \ a+k) \cdots (a \ a+2)(a \ a+1)(a \ b)(a \ a+1)(a+1 \ a+2) \cdots (a+k-1 \ a+k)
\]
Since $b = a + k + 1$, then the left hand side is in $T$, and the right hand side is a product of elements in $T$ and $(ab)$. If we move most of the things to the left hand side (multiplying by inverses) we get
\[
(a \ a+1)(a+1 \ a+2) \cdots (a+k-1 \ a+k)(a+k \ b)(a+k-1 \ a+k) \cdots (a+1 \ a+2)(a \ a+1) = (a \ b)
\]
which means that $(a \ b)$ is generated by elements in $T$.

Since every element in $S_n$ can be written as a product of 2-cycles, then $T$ generates all $S_n$. 
3. Let $\mathbb{R}^\times$ denote the multiplicative group of nonzero real numbers and $\mathbb{R}$ denote the additive group of real numbers. Show that $\mathbb{R}^\times \cong \mathbb{R} \times \mathbb{Z}_2$.

**Solution.** Think $\mathbb{Z}_2$ as the multiplicative group $\{1, -1\}$. Define a function $\text{sign}(x) : \mathbb{R}^\times \to \mathbb{Z}_2$ by $\text{sign}(x) = 1$ if $x$ is positive, and $\text{sign}(x) = -1$ if $x$ is negative.

Note that $\text{sign}(xy) = \text{sign}(x)\text{sign}(y)$ for all non-zero real numbers $x$ and $y$.

Consider the map $\phi : \mathbb{R} \times \to \mathbb{R} \times \mathbb{Z}_2$ defined by $\phi(x) = (\ln |x|, \text{sign}(x))$ (I know it is ugly—defined as I am using additive notation for the first component and multiplicative for the second).

Now note that

$$\phi(xy) = (\ln |xy|, \text{sign}(xy)) = (\ln |x| + \ln |y|, \text{sign}(x)\text{sign}(y)) = (\ln |x|, \text{sign}(x))(\ln |y|, \text{sign}(y))$$

So, $\phi$ is a homomorphism. It is easy to see that $\phi$ is onto using that $\ln |x|$ is onto $\mathbb{R}$. Moreover,

$$\text{Ker}(\phi) = \{x \in \mathbb{R}^\times; \ln |x| = 0 \text{ and } \text{sign}(x) = 1\} = \{1\}$$

Hence, $\phi$ defines an isomorphism.

4. An element $x$ in a ring $R$ is called nilpotent if $x^m = 0$ for some $m \in \mathbb{Z}^+$. Let $R$ be a commutative ring with $1 \neq 0$. Prove that if $a$ is a nilpotent element of $R$, then $1 - ab$ is a unit for all $b \in R$.

**Solution.** First notice that if $a^m = 0$ for some $m$, then $(ab)^m = 0$ for the same $m$ (here using the ring is commutative). So, let’s call $ab = x$, we know $x$ is nilpotent and that the $m^{th}$ power kills it.

Now consider the product

$$(1 - x)(1 + x + x^2 + \cdots + x^{m-1}) = 1 - x^m = 1$$

It follows that the inverse of $1 - x$ is $1 + x + x^2 + \cdots + x^{m-1}$ (whatever that is, anyway it will be an element of the ring).

5. (a) Let $H = \{(1), (2 3)\}$. Is $H$ normal in $S_3$?

(b) What is the order of the element $14 + \langle 8 \rangle$ in the quotient group $\mathbb{Z}_{24}/\langle 8 \rangle$?

**Solution.**

(a) No, as $(123)(23)(123)^{-1} = (13) \notin H$

(b) The group $H = \langle 8 \rangle$ has the elements $H = \{0, 8, 16\}$.

Now I will compute the ‘powers’ of 14 all modulo 24

14 $\notin H$

14 + 14 = 28 $\equiv 4 \notin H$

14 + 14 + 14 $\equiv 4 + 14 \equiv 18 \notin H$

14 + 14 + 14 + 14 $\equiv 4 + 4 \equiv 8 \in H$

Hence, the order of $14 + \langle 8 \rangle$ is 4
6. Prove that any subfield of \( \mathbb{R} \) must contain \( \mathbb{Q} \).

**Solution.** A field always \( F \) has a one. By closure of the addition of \( F \) we can see that all the integers must be in \( F \) (here we are using that \( \mathbb{Z} \subset \mathbb{R} \)). Since we need inverses for all non-zero elements in \( F \), then all the elements of the form \( \frac{1}{x} \), for \( x \in \mathbb{Z} \) must be in \( F \) as well. Finally, using closure of the multiplication we can construct any rational as the product of two elements in \( F \),
\[
\frac{a}{b} = a \cdot \frac{1}{b}
\]
and thus \( \mathbb{Q} \subset F \).

7. Prove that if \( H \) and \( K \) are finite subgroups of \( G \) whose orders are relatively prime then \( H \cap K = 1 \).

**Solution.** This is problem 4 part A in the exam of Fall 2007.

8. Consider the additive quotient group \( \mathbb{Q}/\mathbb{Z} \).

(a) Show that every coset of \( \mathbb{Z} \) in \( \mathbb{Q} \) contains exactly one representative \( q \in \mathbb{Q} \) in the range \( 0 \leq q < 1 \).

(b) Show that every element of \( \mathbb{Q}/\mathbb{Z} \) has finite order but that there are elements of arbitrarily large order.

**Solution.**

(a) Let \( x \in \mathbb{Q} \), we denote the greatest integer that is less or equal to \( x \) as \( [x] \), then \( x - [x] \in [0, 1) \). Since \( [x] \) is an integer, then \( x + \mathbb{Z} = x - [x] + \mathbb{Z} \). So, every coset of \( \mathbb{Z} \) in \( \mathbb{Q} \) contains at least one representative in \([0, 1)\). Moreover, having two representatives in \([0, 1)\) will force a number \( x \) to have two decimal parts, that is not possible.

(b) Let \( x = \frac{a}{b} \in \mathbb{Q} \). WLOG we take \( b > 0 \). Then, the order of \( x + \mathbb{Z} \) is at most \( b \), as
\[
\frac{a}{b} + \cdots + \frac{a}{b} \quad (b \text{ times})
\]
is equal to \( a \in \mathbb{Z} \)

So, every element in \( \mathbb{Q}/\mathbb{Z} \) has finite order.

Now consider a number \( N \) (as large as you wish), we know there are infinitely many primes, thus there must be a prime number \( p \) that is larger than \( N \). It is easy to see that \( x = \frac{1}{p} \) has order \( p > N \).
Part B.

1. Determine the dimension of the solution space (over the real numbers) to the system of equations
\[
\begin{align*}
    x_1 + x_2 &= 0 \\
    x_2 + x_3 &= 0 \\
    x_3 + x_4 &= 0 \\
    x_4 + x_5 &= 0 \\
    -x_1 + x_5 &= 0
\end{align*}
\]

**Solution.** The last equation in the system says \(x_5 = x_1\), the previous to the last says \(x_4 = -x_5\), which together with the last one imply \(x_1 = -x_4\). Since \(x_3 = -x_4\) we get that \(x_1 = x_3\).

The solution space of this system is spanned by \((1, -1, 1, -1, 1)\). So, the dimension is one.

2. Find a *unit* vector in \(\mathbb{R}^3\) that is mutually perpendicular to \(v = (1, 2, 3)\) and \(w = (3, 2, 1)\).

**Solution.** We will first find a vector that is perpendicular to \(v\) and \(w\), then we will normalize it.

The vector we are looking for is \(u = (x, y, z)\), it follows that
\[
0 = (x, y, z) \cdot (1, 2, 3) = x + 2y + 3z \quad \text{and} \quad 0 = (x, y, z) \cdot (3, 2, 1) = 3x + 2y + z
\]

So, subtracting these two equations we get \(2x - 2z = 0\), which implies \(x = z\). Plugging this into one of the equations we get \(4x + 2y = 0\), which implies \(y = -2x\). Hence, the solution space for the system of equations above is spanned by \((1, -2, 1)\).

So, any vector that is a multiple of \((1, -2, 1)\) is orthogonal to both \(v\) and \(w\). In particular, we take
\[
\frac{1}{||(1, -2, 1)||} (1, -2, 1) = \frac{1}{\sqrt{6}} (1, -2, 1)
\]
which has norm one.

3. Suppose
\[
A = \begin{pmatrix}
1 & -1 & 0 & 2 \\
-2 & 0 & 0 & 1 \\
-1 & -1 & 0 & 3
\end{pmatrix}
\]

Determine a basis over the reals for the image of the linear transformation \(L(v) = Av\).

**Solution.** We know the image of \(L\) is spanned by the column vectors of the matrix \(A\). Since one of the column vectors is the zero vector, then we just have to play with
\[
B = \begin{pmatrix}
1 & -1 & 2 \\
-2 & 0 & 1 \\
-1 & -1 & 3
\end{pmatrix}
\]
(which has determinant zero, thus we need to get rid of columns)

We will do some column operations on this matrix to find a basis for $Im(L)$

\[
B = \begin{pmatrix}
1 & -1 & 2 \\
-2 & 0 & 1 \\
-1 & -1 & 3 \\
\end{pmatrix}
\]

now we add column 2 to column 1

\[
= \begin{pmatrix}
0 & -1 & 2 \\
-2 & 0 & 1 \\
-2 & -1 & 3 \\
\end{pmatrix}
\]

now we add column 2 twice to column 3

\[
= \begin{pmatrix}
0 & -1 & 0 \\
-2 & 0 & 1 \\
-2 & -1 & 1 \\
\end{pmatrix}
\]

Now we can see clearly that column 1 and column 3 are linearly dependent. So, a basis for $Im(L)$ is given by

\[\{(-1, 0, -1), (0, 1, 1)\}\]

4. Determine the inverse of the matrix

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 2 & 0 \\
0 & 3 & 0 & 0 \\
4 & 0 & 0 & 0 \\
\end{pmatrix}
\]

**Solution.** Since this is an anti-diagonal matrix then its inverse is also anti-diagonal and given by

\[
\begin{pmatrix}
0 & 0 & 0 & \frac{1}{4} \\
0 & 0 & \frac{1}{3} & 0 \\
0 & \frac{1}{2} & 0 & 0 \\
1 & 0 & 0 & 0 \\
\end{pmatrix}
\]

5. Suppose $A$ is an invertible matrix. Prove $(A^t)^{-1} = (A^{-1})^t$ where $M^t$ and $M^{-1}$ represent the transpose and inverse, respectively, of the matrix $M$.

**Solution.** We know that $(AB)^t = B^tA^t$, then

\[
I = (A^{-1}A)^t = A^t(A^{-1})^t
\]

and

\[
I = (AA^{-1})^t = (A^{-1})^tA^t
\]

6. Determine an orthonormal basis for $\text{span}\{(-1, 0, 0, 1), (0, 0, 1, -1), (1, -1, 0, 0)\}$. 
Solution. We will use the Gram-Schmidt process.

Note that the vectors \( v_1 = (0, 0, 1, -1) \) and \( v_2 = (1, -1, 0, 0) \) are already orthogonal. So, we just need to find the third vector

Then

\[
\begin{align*}
v_3 &= (-1, 0, 0, 1) - \frac{(0, 0, 1, -1) \cdot (-1, 0, 0, 1)}{|(0, 0, 1, -1)|^2} (0, 0, 1, -1) - \frac{(1, 1, 0, 0) \cdot (-1, 0, 0, 1)}{|(1, 1, 0, 0)|^2} (1, 1, 0, 0) \\
&= (-1, 0, 0, 1) + \frac{1}{2} (0, 0, 1, -1) + \frac{1}{2} (1, -1, 0, 0) \\
&= \left( -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \right)
\end{align*}
\]

So, \( v_1, v_2 \) and \( v_3 \) are orthogonal and span the same subspace the original three vectors spanned. Now we normalize these vectors by dividing them by their norm. The final answer is

\[
\left\{ \frac{1}{\sqrt{2}} (0, 0, 1, -1), \frac{1}{\sqrt{2}} (1, -1, 0, 0), \left( -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \right) \right\}
\]

7. State what it means (the definition) for a finite set of vectors to be linearly independent, and use this definition to prove the set of vectors \( \{(1, 1, 0), (0, 1, 1), (1, 0, 1)\} \) is linearly independent.

Solution. A set of vectors is linearly independent if the only linear combination of these vectors that yields the zero vector is the trivial one (i.e. all scalars must be zero).

Assume that

\[
(0, 0, 0) = \alpha (1, 1, 0) + \beta (0, 1, 1) + \gamma (1, 0, 1) = (\alpha + \gamma, \alpha + \beta, \beta + \gamma)
\]

then we get the system

\[
\begin{align*}
\alpha + \gamma &= 0 \\
\alpha + \beta &= 0 \\
\beta + \gamma &= 0
\end{align*}
\]

which has only one solution \( \alpha = \beta = \gamma = 0 \).

8. Determine the eigenvalues of the matrix

\[
\begin{pmatrix}
2 & 2 & -5 \\
3 & 7 & -15 \\
1 & 2 & -4
\end{pmatrix}
\]
Solution. Let's play with this determinant

\[
\chi_A(\lambda) = \begin{vmatrix}
2 - \lambda & 2 & -5 \\
3 & 7 - \lambda & -15 \\
1 & 2 & -4 - \lambda \\
\end{vmatrix}
\]

now we multiply row 1 by 3

\[
= \frac{1}{3} \begin{vmatrix}
6 - 3\lambda & 6 & -15 \\
3 & 7 - \lambda & -15 \\
1 & 2 & -4 - \lambda \\
\end{vmatrix}
\]

now we subtract row 2 from row 1

\[
= \frac{1}{3} \begin{vmatrix}
3 - 3\lambda & -1 + \lambda & 0 \\
3 & 7 - \lambda & -15 \\
1 & 2 & -4 - \lambda \\
\end{vmatrix}
\]

now we multiply column 2 by 3

\[
= \frac{1}{3^2} \begin{vmatrix}
3 - 3\lambda & -3 + 3\lambda & 0 \\
3 & 21 - 3\lambda & -15 \\
1 & 6 & -4 - \lambda \\
\end{vmatrix}
\]

now we add column 1 to column 2

\[
= \frac{1}{3^2} \begin{vmatrix}
3 - 3\lambda & 0 & 0 \\
3 & 24 - 3\lambda & -15 \\
1 & 7 & -4 - \lambda \\
\end{vmatrix}
\]

\[
= \frac{1}{3^2}(3 - 3\lambda) \begin{vmatrix}
24 - 3\lambda & -15 \\
7 & -4 - \lambda \\
\end{vmatrix}
\]

\[
= (1 - \lambda) \begin{vmatrix}
8 - \lambda & -5 \\
7 & -4 - \lambda \\
\end{vmatrix}
\]

\[
= (1 - \lambda)((8 - \lambda)(-4 - \lambda) + 35)
\]

\[
= (1 - \lambda)(\lambda^2 - 4\lambda + 3)
\]

\[
= (1 - \lambda)(\lambda - 3)(\lambda - 1)
\]

So, the eigenvalues are \(\lambda = 1\) (with multiplicity 2) and \(\lambda = 3\) (with multiplicity one).
Part A. Do five of the following 8 problems.

1. Show that a nonzero finite commutative ring $R$ with no zero-divisors has a multiplicative identity.

2. Let $G = \{ x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1 \}$. Define the operation $*$ on $G$ by $a * b = a^{\ln b}$, for all $a, b \in G$. Prove that $G$ is an Abelian group under the operation $*$.

3. Let $\mathbb{R}[x]$ denote the ring of all polynomials with real coefficients. Also, let $a \in \mathbb{R}$, and let $f(x) \in \mathbb{R}[x]$, with derivative $f'(x)$. Show that the remainder when $f(x)$ is divided by $(x - a)^2$ is $f'(a)(x - a) + f(a)$.

4. Let $\phi : G_1 \rightarrow G_2$ and $\theta : G_2 \rightarrow G_3$ be group homomorphisms. Prove that $\theta\phi : G_1 \rightarrow G_3$ is a homomorphism. prove that $\ker(\phi) \subseteq \ker(\theta\phi)$.

5. Let $N$ be a subgroup of the center of $G$. Show that if $G/N$ is a cyclic group, then $G$ must be Abelian.

6. Show that a relation on $\mathbb{R}^+$ defined by $x \sim y$ iff $x^y = y^x$ is an equivalence relation.

7. Let $F$ be a field and let $\phi : F \rightarrow R$ be a ring homomorphism. Show that $\phi$ is either zero or one-to-one.

8. Let $S_n$ denote the symmetric group of degree $n$ and let $A_n$ denote the alternating group of degree $n$. For any elements $\sigma, \tau \in S_n$ show that $\sigma\tau\sigma^{-1}\tau^{-1} \in A_n$. 
1. Consider the linear transformation with matrix \( A = \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \). Find a basis for the kernel and a basis for the image of the transformation.

2. Let \( A \) be an \( m \times n \) matrix. Consider the set
\[
W = \{ v \in \mathbb{R}^n \mid Av = 0 \}
\]
Prove that \( W \) a subspace of \( \mathbb{R}^n \).

3. Let \( A = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \). Prove that the linear transformation \( T(x) = Ax \) represents a rotation of the vector \( x \) by an angle of \( \theta \).

4. Find an orthonormal basis for the subspace of \( \mathbb{R}^4 \) spanned by the vectors \( u_1 = \langle 0, -1, 0, 0 \rangle \), \( u_2 = \langle 3, 0, 1, 0 \rangle \), and \( u_3 = \langle 1, 1, 0, 1 \rangle \).

5. Let \( A \) be an invertible \( n \times n \) matrix, and let \( c \) be a nonzero real number. Prove or disprove:
\[
(cA)^{-1} = \frac{1}{c}A^{-1}.
\]

6. Let \( A_{m \times n} \) and \( B_{n \times p} \) be matrices. Prove that \( (AB)^T = B^T A^T \), where \( A^T \) denotes the transpose of the matrix \( A \).

7. Let \( A = \begin{bmatrix} 0 & 0 & -2 \\ 0 & -1 & 2 \\ -1 & 0 & 1 \end{bmatrix} \). Find the eigenvalues and corresponding eigenvector(s) of \( A \).

8. Let \( A \) be an invertible \( n \times n \) matrix. Prove that \( \det(A^{-1}) = \frac{1}{\det(A)} \).
1. Show that a nonzero finite commutative ring \( R \) with no zero-divisors has a multiplicative identity.

**Solution.** Fix an element \( r \in R^* \). Consider the map \( \phi : R \to R \) defined by \( \phi(x) = xr \).

Note that \( \phi(x) = \phi(y) \) implies \( r(x - y) = 0 \).

Since \( R \) has no zero divisors, then \( \phi \) is one-to-one. But, as \( R \) is finite then \( \phi \) is bijective. It follows there is an element \( x_r \in R \) such that \( rx_r = r \).

Using that \( \phi \) is onto we represent an element \( y \in R \) as \( y = rx \) for some \( x \in R \), then

\[ x_r y = x_r(rx) = (x_r)x = rx = y \]

So, \( x_r \) works as the identity for ALL elements in \( R \).

2. Let \( G = \{ x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1 \} \). Define the operation \( * \) on \( G \) by \( a * b = a^{\ln b} \), for all \( a, b \in G \). Prove that \( G \) is an Abelian group under the operation \( * \).

**Solution.** Let \( a, b \in G \), then \( a^{\ln b} \) is also a positive real number (\( a \) is positive). Moreover, since \( \ln b \neq 0 \) (as \( b \neq 1 \)) then \( a^{\ln b} \neq 1 \). So, closure for the product works out.

What is the identity? It is \( e \)!! (meaning \( e \sim 2.71 \))... confusing as the standard notation for the identity in a group is also \( e \). To check this just notice that

\[ e^{\ln b} = b \quad \text{and} \quad a^{\ln e} = a^{1} = a \]

What is the inverse of \( a \in G \)? We look for an element \( b \) such that \( a * b = e \), or in other words

\[ a^{\ln b} = e \]

Applying natural log both sides we get

\[ \ln (a^{\ln b}) = \ln e \]

which is

\[ \ln a \ln b = 1 \]

So, \( b \) is given by the unique positive number such that \( \ln b \) is the multiplicative inverse of \( \ln a \).

Finally, we check that the group is Abelian

\[ a * b = a^{\ln b} = (e^{\ln a})^{\ln b} = (e^{\ln b})^{\ln a} = b^{\ln a} \]

3. Let \( \mathbb{R}[x] \) denote the ring of all polynomials with real coefficients. Also, let \( a \in \mathbb{R} \), and let \( f(x) \in \mathbb{R}[x] \), with derivative \( f'(x) \). Show that the remainder when \( f(x) \) is divided by \( (x - a)^2 \) is \( f'(a)(x - a) + f(a) \).
Solution. Since the degree of $f'(a)(x-a) + f(a)$ is one, then we just need to show that

$$f(x) = q(x)(x-a)^2 + f'(a)(x-a) + f(a)$$

for some $q(x) \in \mathbb{R}[x]$. The remainder theorem says that

$$f(x) = p(x)(x-a) + f(a)$$

for some $p(x) \in \mathbb{R}[x]$. We now derive the previous equation both sides to get

$$f'(x) = p'(x)(x-a) + p(x)$$

So, $f'(a) = p(a)$

We use the remainder theorem again with $p(x)$ divided by $(x-a)$ to get

$$p(x) = q(x)(x-a) + f(a)$$

for some $q(x) \in \mathbb{R}[x]$.

It follows that

$$f(x) = p(x)(x-a) + f(a)$$

$$= [q(x)(x-a) + p(a)](x-a) + f(a)$$

$$= q(x)(x-a)^2 + p(a)(x-a) + f(a)$$

$$= q(x)(x-a)^2 + f'(a)(x-a) + f(a)$$

4. Let $\phi : G_1 \to G_2$ and $\theta : G_2 \to G_3$ be group homomorphisms. Prove that $\theta \phi : G_1 \to G_3$ is a homomorphism. prove that $\ker(\phi) \subset \ker(\theta \phi)$.

Solution. Let $g, h \in G_1$

$$\theta \phi (gh) = \theta (\phi (gh)) = \theta (\phi (g) \phi (h)) = \theta (\phi (g)) \theta (\phi (h)) = \theta \phi (g) \theta \phi (h)$$

Hence, $\theta \phi$ is a group homomorphism

Now let $g \in \ker(\phi)$, then

$$\theta \phi (g) = \theta (\phi (g)) = \theta (e_{G_2}) = e_{G_3}$$

So, $g \in \ker(\theta \phi)$.

5. Let $N$ be a subgroup of the center of $G$. Show that if $G/N$ is a cyclic group, then $G$ must be Abelian.
Solution. Let $G/N = \langle gN \rangle$. Take two elements in $G$, $x = g^i n$ and $y = g^j m$, where $i,j \in \mathbb{Z}$ and $n,m \in N$, then (don’t forget that both $n$ and $m$ live in the center of $G$)

$$xy = (g^i n)(g^j m)$$
$$= g^i (ng^j)m$$
$$= g^i (g^j n)m$$
$$= (g^i g^j)(nm)$$
$$= (g^i g^j)(mn)$$
$$= g^j (g^i m)n$$
$$= g^j (mg^i)n$$
$$= (g^j m)(g^i n) = yx$$

6. Show that a relation on $\mathbb{R}^+$ defined by $x \sim y$ iff $x^y = y^x$ is an equivalence relation.

Solution. Since $x^y = y^x$ implies $y^x = x^y$ and $x^x = x^x$ then $\sim$ is both reflexive and symmetric. Now assume that $x^y = y^x$ and $y^z = z^y$ (note that none of these elements is zero), then

$$x^z = (x^y)^{z/y} = (y^x)^{z/y} = (y^z)^{x/y} = (z^y)^{x/y} = z^x$$

Hence, transitivity also holds.

7. Let $F$ be a field and let $\phi : F \to R$ be a ring homomorphism. Show that $\phi$ is either zero or one-to-one.

Solution. Since $F$ is a field, then it has no proper ideals. However, the kernel of $\phi$ is an ideal of $F$, thus $\ker(\phi) = \{0\}$ (in which case $\phi$ is one-to-one) or $\ker(\phi) = F$, in the latter case $\phi$ is the zero function.

8. Let $S_n$ denote the symmetric group of degree $n$ and let $A_n$ denote the alternating group of degree $n$. For any elements $\sigma, \tau \in S_n$ show that $\sigma \tau \sigma^{-1} \tau^{-1} \in A_n$.

Solution. Note that $\sigma \tau$ is even if and only if $\sigma^{-1} \tau^{-1}$ is even. The result follows by noting that the product of two permutations having the same parity is always even.
Part B.

1. Consider the linear transformation with matrix \( A = \begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \). Find a basis for the kernel and a basis for the image of the transformation.

**Solution.** Set \( Ax = 0 \). Then the solution space is \( \left\{ \begin{bmatrix} 2z \\ -3z \\ z \\ 0 \end{bmatrix} \mid z \in \mathbb{R} \right\} \). Therefore it is of dimension 1, and a basis is \( \begin{bmatrix} 2 \\ -3 \\ 1 \\ 0 \end{bmatrix} \).

Since \( A \) is \( 3 \times 4 \), the image is a subspace of \( \mathbb{R}^3 \). Moreover, the dimension of the image is 3 since the dimension of the kernel is 1. A 3-dimensional subspace of \( \mathbb{R}^3 \) must be \( \mathbb{R}^3 \) itself, so we may use the standard basis \( \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \).

2. Let \( A \) be an \( m \times n \) matrix. Consider the set 

\[ W = \{ v \in \mathbb{R}^n \mid Av = 0 \} \]

Prove that \( W \) a subspace of \( \mathbb{R}^n \).

**Solution.** Let \( u, v \in W \) and let \( c \in \mathbb{R} \). Then

(i) \( A(u + v) = Au + Av = 0 + 0 = 0 \). Therefore \( u + v \in W \).

(ii) \( A(cu) = cAu = c \cdot 0 = 0 \). Therefore \( cu \in W \).

Since \( W \) is closed under addition and scalar multiplication, \( W \) is a subspace of \( \mathbb{R}^n \).

3. Let \( A = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \). Prove that the linear transformation \( T(x) = Ax \) represents a rotation of the vector \( x \) by an angle of \( \theta \).

**Solution.** Let \( a = \begin{bmatrix} x \\ y \end{bmatrix} \) and let \( b = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos \theta x - \sin \theta y \\ \sin \theta x + \cos \theta y \end{bmatrix} \). We must show that \( a \cdot b = |a||b| \cos \theta \).
We have $|a| = \sqrt{x^2 + y^2}$ and
\[
|b| = \sqrt{(x \cos \theta - y \sin \theta)^2 + (x \sin \theta + y \cos \theta)^2} \\
= \sqrt{x^2 \cos^2 \theta - 2xy \cos \theta \sin \theta + y^2 \sin^2 \theta + x^2 \sin^2 \theta + 2xy \sin \theta \cos \theta + y^2 \cos^2 \theta} \\
= \sqrt{x^2 + y^2}.
\]
Therefore
\[
a \cdot b = x^2 \cos \theta - xy \sin \theta + xy \sin \theta + y^2 \cos \theta \\
= (x^2 + y^2) \cos \theta \\
= |a||b| \cos \theta.
\]

4. Find an orthonormal basis for the subspace of $\mathbb{R}^4$ spanned by the vectors $u_1 = \langle 0, -1, 0, 0 \rangle$, $u_2 = \langle 3, 0, 1, 0 \rangle$, and $u_3 = \langle 1, 1, 0, 1 \rangle$.

**Solution.** Using the Gram-Schmidt process, we have that $v_1, v_2, v_3$ is an orthogonal basis, where $v_1 = u_1 = \langle 0, -1, 0, 0 \rangle$, $v_2 = u_2 = \langle 3, 0, 1, 0 \rangle$ (since $u_1 \cdot u_2 = 0$), and $v_3 = \langle 1, 1, 0, 1 \rangle - \frac{3}{10} \langle 0, -1, 0, 0 \rangle - \frac{3}{10} \langle 3, 0, 1, 0 \rangle = \langle 1, 1, 0, 1 \rangle - \frac{3}{10} \langle 3, 0, 1, 0 \rangle = \langle \frac{7}{10}, 0, -\frac{3}{10}, 1 \rangle$.

We have $|v_1| = 1$, $|v_2| = \sqrt{10}$, and $|v_3| = \sqrt{110}$. Therefore an orthonormal basis is \{\langle 0, -1, 0, 0 \rangle, \frac{1}{\sqrt{10}} \langle 3, 0, 1, 0 \rangle, \frac{1}{\sqrt{110}} \langle 1, 1, 0, 1 \rangle - \frac{3}{10} \langle 3, 0, 1, 0 \rangle \}.

5. Let $A$ be an invertible $n \times n$ matrix, and let $c$ be a nonzero real number. Prove or disprove: $(cA)^{-1} = \frac{1}{c} A^{-1}$.

**Solution.** $(cA) \left(\frac{1}{c} A^{-1}\right) = c \cdot \frac{1}{c} AA^{-1} = I_n$. Therefore $(cA)^{-1} = \frac{1}{c} A^{-1}$.

6. Let $A_{m \times n}$ and $B_{n \times p}$ be matrices. Prove that $(AB)^T = B^T A^T$, where $A^T$ denotes the transpose of the matrix $A$.

**Solution.** Let $A = [a_{ij}]$ and $B = [b_{ij}]$. The $(i, j)$-entry of $(AB)^T$ is the $(j, i)$-entry of $AB$, which is $[j$th row of $A] \cdot [i$th column of $B] = a_{j1}b_{1i} + \ldots + a_{jn}b_{ni} = \sum_{k=1}^{n} a_{jk}b_{ki}$.

On the other hand, the $(i, j)$-entry of $B^T A^T$ is $[i$th row of $B^T] \cdot [j$th column of $A^T] = b_{1i}a_{i1} + \ldots + b_{ni}a_{in} = \sum_{k=1}^{n} a_{jk}b_{ki}$.

Since the corresponding entries are equal, we have that $(AB)^T = B^T A^T$.

7. Let $A = \begin{bmatrix} 0 & 0 & -2 \\ 0 & -1 & 2 \\ -1 & 0 & 1 \end{bmatrix}$. Find the eigenvalues and corresponding eigenvector(s) of $A$. 

Solution. The characteristic polynomial is
\[ p(\lambda) = \lambda ((\lambda + 1)(\lambda - 1)) - 2(\lambda + 1) \]
\[ = (\lambda + 1) (\lambda(\lambda - 1) - 2) \]
\[ = (\lambda + 1)(\lambda^2 - \lambda - 2) \]
\[ = (\lambda + 1)^2(\lambda - 2); \]
therefore the eigenvalues are \( \lambda_1 = -1, \lambda_2 = 2. \)

For \( \lambda_1 \) we have the system \((-I - A)x = 0\), which gives
\[
\begin{bmatrix}
-1 & 0 & 2 & 0 \\
0 & 0 & -2 & 0 \\
1 & 0 & -2 & 0
\end{bmatrix}
\]
which reduces to
\[
\begin{bmatrix}
1 & 0 & -2 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\].

A basis for the solution space is \( \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\} \). So an eigenvector for \( \lambda_1 \) is \( v_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \).

Similarly for \( \lambda_2 \) we have the system \((2I - A)x = 0\), which gives
\[
\begin{bmatrix}
2 & 0 & 2 & 0 \\
0 & 3 & -2 & 0 \\
1 & 0 & 1 & 0
\end{bmatrix}
\]
which reduces to
\[
\begin{bmatrix}
1 & 0 & 1 & 0 \\
0 & 3 & -2 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\].

A basis for the solution space is \( \left\{ \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix} \right\} \). So an eigenvector for \( \lambda_2 \) is \( v_2 = \begin{bmatrix} -1 \\ \frac{3}{2} \\ 1 \end{bmatrix} \).

8. Let \( A \) be an invertible \( n \times n \) matrix. Prove that \( \det(A^{-1}) = \frac{1}{\det(A)}. \)

Solution. We have \( 1 = \det(I_n) = \det(AA^{-1}) = \det(A) \det(A^{-1}) \). Therefore \( \det(A^{-1}) = \frac{1}{\det(A)}. \)
Part A. Do five of the following 8 problems.

1. Prove that if $G$ is any cyclic group, then $G$ is abelian. (*Your proof must include the case where $G$ is infinite.*)

2. Let $S_n$ denote the group of permutations on the set $\{1, 2, \ldots, n\}$, and let $\sigma \in S_n$ be an odd permutation. Prove that $\sigma^{-1}$ is an odd permutation.

3. Let $N$ be a normal subgroup of an abelian group $G$. Prove that the factor group $G/N$ is abelian.

4. Let $G = \mathbb{Q} - \{-1\}$ be the set of rational numbers except $-1$. For $a, b \in G$, let $a * b$ be defined by $a * b = a + b + ab$. Prove that $(G, *)$ is a group.

5. Let $H$ be a subgroup of a group $G$. For $a, b \in G$, define a relation on $G$ by letting $a \sim b$ if and only if $ab^{-1} \in H$. Prove that $\sim$ is an equivalence relation.

6. Prove that the polynomial $f(x) = x^7 - 10x^4 + 15x - 5$ is irreducible over the field of rational numbers.

7. An element $a$ of a ring $R$ is called a zero divisor if there exists a nonzero element $b \in R$ such that $ab = 0$. If $a$ is a zero divisor of a commutative ring $R$ and $r \in R$, prove that $ar$ is a zero divisor.

8. Let $R$ and $S$ be commutative rings, and let $\varphi: R \rightarrow S$ be a non-trivial ring homomorphism.
   (a) Prove that the kernel of $\varphi$ is an ideal of $R$.
   (b) If $R$ is a field, prove that $\varphi$ is one-to-one.
Part B. Do five of the following 8 problems.

1. Let $L_A : \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation given by $L_A(v) = A v$ where $A$ is a real $n \times n$ matrix. Show that if $n$ is odd then $L$ has a real eigenvalue.

2. If $v_1, v_2, \ldots, v_n$ are distinct eigenvectors corresponding to distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of a matrix $A$, prove that $\{v_1, v_2, \ldots, v_n\}$ is a linearly independent set.

3. Let $V$ be a real vector space of dimension $n$, and suppose that $S = \{v_1, v_2, \ldots, v_t\}$ is a linearly independent subset of $V$. Prove that there is a basis $B$ of $V$ such that $S \subseteq B$.

4. Let $S$ be the set of all functions $f : \mathbb{R} \to \mathbb{R}$ that satisfy the differential equation
   \[ y'' - y' + 2y = 0. \]
   Is $S$ a real vector space? (Assume the usual operations $(f + g)(t) = f(t) + g(t)$ and $(c \cdot f)(t) = cf(t)$ where $c \in \mathbb{R}$.) Explain why or why not.

5. Let $A$ and $B$ be $n \times n$ matrices. Show that $AB$ is invertible if and only if $A$ and $B$ are invertible.

6. Prove that a linear transformation of vector spaces $L : V \to W$ is one to one if and only if $L$ maps linearly independent subsets of $V$ to linearly independent subsets of $W$.

7. Let $V$ be a finite dimensional vector space and $L : V \to W$ be a linear transformation to vector space $W$. Prove that $\dim(\ker L) + \dim(\text{image } L) = \dim V$.

8. Let $A$ be an $n \times n$ matrix. Prove that $A$ is invertible if and only if the determinant of $A$ is non-zero.
1. Prove that if $G$ is any cyclic group, then $G$ is abelian. (*Your proof must include the case where $G$ is infinite.*)

**Solution.** Let $G = \langle a \rangle$, and let $x, y \in G$. Then $x = a^k$ and $y = a^l$ for some $k, l \in \mathbb{Z}$. Thus $xy = a^k a^l = a^{k+l} = a^l a^k = yx$.

2. Let $S_n$ denote the group of permutations on the set $\{1, 2, \ldots, n\}$, and let $\sigma \in S_n$ be an odd permutation. Prove that $\sigma^{-1}$ is an odd permutation.

**Solution.** $\sigma$ can be written as a product of an odd number of transpositions. Suppose $\sigma = (a_1 b_1)(a_2 b_2) \cdots (a_{2k+1} b_{2k+1})$.

Then $\sigma^{-1} = (a_{2k+1} b_{2k+1}) \cdots (a_1 b_1)$, again a product of an odd number of transpositions. Therefore $\sigma^{-1}$ is odd.

3. Let $N$ be a normal subgroup of an abelian group $G$. Prove that the factor group $G/N$ is abelian.

**Solution.** Let $aN, bN \in G/N$. Then $aNbN = abN = baN = bNaN$.

4. Let $G = \mathbb{Q} - \{-1\}$ be the set of rational numbers except $-1$. For $a, b \in G$, let $a \star b$ be defined by $a \star b = a + b + ab$. Prove that $(G, \star)$ is a group.

**Solution.**

**Closure.** If $a, b \in G$, then clearly $a + b + ab \in \mathbb{Q}$. If $a+b+ab = -1$ then $a(1+b) = -(b+1)$, and hence $a = -\frac{b+1}{1+b} = -1$, a contradiction. Therefore $G$ is closed under $\star$.

**Associativity.** We have

\[
(a \star b) \star c = (a + b + ab) \star c = (a + b + ab) + c + (a + b + ab)c
\]

\[
= a + b + c + ab + ac + bc + abc
\]

\[
= a + (b + c + bc) + a(b + c + bc) = a \star (b + c + bc) = a \star (b \star c).
\]

**Identity.** We claim that $e = 0$ is the identity element. For all $a \in G$ we have

\[
a + 0 + a \cdot 0 = a = 0 + a + 0 \cdot a.
\]

**Inverse.** Let $a \in G$. We claim that $a^{-1} = -\frac{a}{1+a}$, which is an element of $G$ since $a \neq 1$.

We have

\[
a + \left(-\frac{a}{1+a}\right) + a \cdot \left(-\frac{a}{1+a}\right) = \frac{a(1+a) - a - a^2}{1+a} = 0.
\]

Thus $(G, \star)$ is a group.
5. Let $H$ be a subgroup of a group $G$. For $a, b \in G$, define a relation on $G$ by letting $a \sim b$ if and only if $ab^{-1} \in H$. Prove that $\sim$ is an equivalence relation.

Solution.

Reflexivity. Let $a \in G$. Then $aa^{-1} = e \in H$. Thus $a \sim a$.

Symmetry. If $ab^{-1} \in H$, then $(ab^{-1})^{-1} = ba^{-1} \in H$. Thus $a \sim b \Rightarrow b \sim a$.

Transitivity. If $ab^{-1}, bc^{-1} \in H$, then $ab^{-1}bc^{-1} = ac^{-1} \in H$. Thus $a \sim b, b \sim c \Rightarrow a \sim c$.

Thus $\sim$ is an equivalence relation.

6. Prove that the polynomial $f(x) = x^7 - 10x^4 + 15x - 5$ is irreducible over the field of rational numbers.

Solution. Using Eisenstein’s Criterion with $p = 5$, we see that $5 \mid a_i$ for $0 \leq i \leq 6$ where $a_i$ is the coefficient of $x^i$; also $5$ does not divide the leading coefficient, and $25$ does not divide the constant term. Therefore $f(x)$ is irreducible over $\mathbb{Q}$.

7. An element $a$ of a ring $R$ is called a zero divisor if there exists a nonzero element $b \in R$ such that $ab = 0$. If $a$ is a zero divisor of a commutative ring $R$ and $r \in R$, prove that $ar$ is a zero divisor.

Solution. If $a$ is a zero divisor, then there is a nonzero element $b \in R$ such that $ab = 0$. Therefore $arb = rab = 0$. Thus $ar$ is a zero divisor.

8. Let $R$ and $S$ be commutative rings, and let $\varphi: R \to S$ be a non-trivial ring homomorphism.

(a) Prove that the kernel of $\varphi$ is an ideal of $R$.

(b) If $R$ is a field, prove that $\varphi$ is one-to-one.

Solution.

(a) Let $k_1, k_2 \in \ker(\varphi)$ and $r \in R$. Then $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2) = 0 + 0 = 0$. Thus $k_1 + k_2 \in \ker(\varphi)$. Also $\varphi(rk_1) = \varphi(r)\varphi(k_1) = \varphi(0) \cdot 0 = 0$; therefore $rk_1 \in \ker(\varphi)$. Thus $\ker(\varphi) \triangleleft R$.

(b) The only ideals of a field are $\{0\}$ and the field itself. Thus $\ker(\varphi) = \{0\}$ or $\ker(\varphi) = F$. But $\varphi$ is given to be nontrivial; therefore $\ker(\varphi) \neq F$. Hence $\ker(\varphi) = \{0\}$, and $\varphi$ is one-to-one.
1. Let $L_A: \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation given by $L_A(v) = Av$ where $A$ is a real $n \times n$ matrix. Show that if $n$ is odd then $L$ has a real eigenvalue.

**Solution.** Since the dimension of $\mathbb{R}^n$ is odd the characteristic polynomial of $A$ will be of odd degree. Since every polynomial in $\mathbb{R}[x]$ of odd degree has a real root, we conclude that $L_A$ has a real eigenvalue.

2. If $v_1, v_2, \ldots, v_n$ are distinct eigenvectors corresponding to distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of a matrix $A$, prove that $\{v_1, v_2, \ldots, v_n\}$ is a linearly independent set.

**Solution.** Assume that $v_1, v_2, \ldots, v_n$ form a linearly dependent set. Let $k$ be the smallest positive integer such that $v_k \in \text{span}\{v_1, v_2, \ldots, v_{k-1}\}$. Thus there are real numbers $c_1, \ldots, c_{k-1}$ such that

$$v_k = c_1 v_1 + c_2 v_2 + \cdots + c_{k-1} v_{k-1} \quad (1)$$

Hence,

$$Av_k = c_1 Av_1 + c_2 Av_2 + \cdots + c_{k-1} Av_{k-1} \quad \text{thus} \quad (2)$$

$$\lambda_k v_k = c_1 \lambda_1 v_1 + c_2 \lambda_2 v_2 + \cdots + c_{k-1} \lambda_{k-1} v_{k-1} \quad (3)$$

Now subtract equation (3) from $\lambda_k$ times equation (1) to get

$$0 = c_1 (\lambda_k - \lambda_1) v_1 + c_2 (\lambda_k - \lambda_2) v_2 + \cdots + c_{k-1} (\lambda_k - \lambda_{k-1}) v_{k-1}$$

Since the $\lambda_i$ are all distinct and the set $\{v_1, v_2, \ldots, v_{k-1}\}$ is independent, we must have that all of the $c_i$ are zero. It follows that $v_k$ is zero, contradicting the hypothesis that $v_k$ is an eigenvector of $A$.

3. Let $V$ be a real vector space of dimension $n$, and suppose that $S = \{v_1, v_2, \ldots, v_t\}$ is a linearly independent subset of $V$. Prove that there is a basis $B$ of $V$ such that $S \subseteq B$.

**Solution.** If $t = n$ then $S$ is a basis. So assume that $t < n$. Let $B = \{w_1, \ldots, w_n\}$ be a basis of $V$. Consider the set $B^*\{v_1, v_2, \ldots, v_t, w_1, w_2, \ldots, w_n\}$. Clearly this spans $V$. Thus we can form a basis from $B^*$ by deleting every vector $x$ that is a linear combination of the vectors preceding $x$. Since the $v_i$’s are independent of one another, none of the $v_i$’s will be deleted during this procedure. Thus $S$ is a subset of the resulting basis.

4. Let $S$ be the set of all functions $f: \mathbb{R} \to \mathbb{R}$ that satisfy the differential equation

$$y'' - y' + 2y = 0.$$ 

Is $S$ a real vector space? (Assume the usual operations $(f + g)(t) = f(t) + g(t)$ and $(c \cdot f)(t) = cf(t)$ where $c \in \mathbb{R}$.) Explain why or why not.
Solution. $S$ is a vector space. Since the derivative is a linear transformation it is easily verified that $S$ is closed under addition and scalar multiplication. The other vector space properties are easily seen as well.

5. Let $A$ and $B$ be $n \times n$ matrices. Show that $AB$ is invertible if and only if $A$ and $B$ are invertible.

Solution. ($\implies$) Assume that $AB$ is invertible. Suppose that $B$ is not invertible. Thus there is a non-trivial solution to the homogenous system $Bx = 0$. This non-trivial solution will also solve the system $ABx = 0$ contradicting the hypothesis that $AB$ is invertible. So $B$ must be invertible.

Now given that $AB$ and $B$ are invertible, we have that $A = (AB)B^{-1}$ is the product of invertible matrices, whence $A$ is invertible.

($\impliedby$) If $A$ and $B$ are invertible, then $AB$ is the product of invertible matrices and has inverse $B^{-1}A^{-1}$.

6. Prove that a linear transformation of vector spaces $L: V \rightarrow W$ is one to one if and only if $L$ maps linearly independent subsets of $V$ to linearly independent subsets of $W$.

Solution. If $V$ is the zero vector space the result is vacuously true. So assume that $V \neq \{0\}$.

($\implies$) Assume that $L$ is one to one. Let $\{v_1, \ldots, v_n\}$ be a linearly independent set in $V$. Suppose that there are constants $\{c_1, \ldots, c_n\}$ such that

$$c_1Lv_1 + c_2Lv_2 + \cdots + c_nLv_n = 0$$

Since $L$ is linear we would then have

$$L(c_1v_1 + c_2v_2 + \cdots + c_nv_n) = 0$$

Since $L$ is one to one, this implies that $c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$ whence all the $c_i$’s must be zero because of the linear independence of $\{v_1, \ldots, v_n\}$.

($\impliedby$) Assume that $L$ preserves linear independence. Let $v \in V$ be a non-zero vector. Then the set $\{v\}$ is linearly independent, whence $\{Lv\}$ is linearly independent. Thus $Lv \neq 0$, so $L$ is one to one.

7. Let $V$ be a finite dimensional vector space and $L: V \rightarrow W$ be a linear transformation to vector space $W$. Prove that $\dim(\text{kernel } L) + \dim(\text{image } L) = \dim V$. 


Solution. Let $n = \dim V$ and $k = \dim \ker L$. Note that $k \leq n$. If $k = n$ then $\ker L = V$ and $\im L = \{0\}$ so the result is true.

So suppose that $0 \leq k < n$. Let $\{v_1, v_2, \ldots, v_k\} \subseteq V$ be a basis for $\ker L$. Since $\{v_1, v_2, \ldots, v_k\}$ is linearly independent, it can be extended to a basis

$$B_V = \{v_1, v_2, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

of $V$. We will show that $T = \{Lv_{k+1}, \ldots, Lv_n\}$ is a basis of the image of $L$.

To see that $T$ spans let $w \in \im L$. Thus $w = Lv$ for some $v$ in $V$. Write so there are constants $c_i (1 \leq i \leq n)$ such that $v = c_1 v_1 + c_2 v_2 + \cdots c_k v_k + c_{k+1} v_{k+1} + \cdots + c_n v_n$. Thus

$$w = Lv = 0 + c_{k+1} Lv_{k+1} + \cdots + c_n Lv_n$$

whence $T$ spans image $L$.

To see that $T$ is linearly independent, suppose that there are constants $c_i (k+1 \leq i \leq n)$ such that $c_{k+1} Lv_{k+1} + \cdots + c_n Lv_n = 0$. Thus $c_{k+1} v_{k+1} + \cdots + c_n v_n$ is in the kernel of $L$ whence there are constants $t_i (1 \leq i \leq k)$ such that $c_{k+1} v_{k+1} + \cdots + c_n v_n = t_1 v_1 + \cdots + t_k v_k$.

The fact that all the $v_i$'s are independent then implies that all the $c_i$'s (and all the $t_i$'s) are zero.

Thus we’ve shown that $\dim(\im L) = n - k$ and the result follows.

8. Let $A$ be an $n \times n$ matrix. Prove that $A$ is invertible if and only if the determinant of $A$ is non-zero.

Solution. (⇒) If $A$ is invertible then $A$ is the product of elementary matrices. Since the determinant respect matrix multiplication and no elementary matrix has zero determinant, it follows that $A$ has non-zero determinant.

(⇐) If $A$ is not invertible then $A$ is row equivalent to a matrix $\hat{A}$ that contains a row of zeros. Hence $A = E_1 E_2 \cdots E_n \hat{A}$ where $E_1, E_2, \ldots, E_n$ is a sequence of elementary matrices. Thus

$$\det A = \det [E_1 E_2 \cdots E_n \hat{A}] = \det (E_1) \det (E_2) \cdots \det (E_n) \det (\hat{A}) = 0$$

since $\det \hat{A} = 0$. 
Part A. Do five of the following 8 problems.

1. Let $a$ and $p$ be integers. If $p$ is prime and $a$ is not divisible by $p$, prove that the additive order of $a$ modulo $p$ is equal to $p$.

2. Let $G$ and $H$ be groups, and let $\varphi : G \to H$ be a group homomorphism with kernel $\ker(\varphi)$. Prove that $\ker(\varphi)$ is a normal subgroup of $G$.

3. Let $N$ be a normal subgroup of a group $G$. Prove that the factor group $G/N$ is abelian if and only if $aba^{-1}b^{-1} \in N$ for all elements $a, b \in G$.

4. Let $G$ be any group with no proper nontrivial subgroups, and assume the order of $G$ is greater than 1. Prove that $G$ is finite cyclic of order $p$ for some prime $p$.

5. Let $G$ be a group and let $D = \{(a, a, a) \mid a \in G\}$.
   (a) Prove that $D$ is a subgroup of the direct product $G \times G \times G$.
   (b) Prove that $D$ is normal in $G \times G \times G$ if and only if $G$ is abelian.
   
   *Hint. If $D$ is normal, then $(a, a, b)(b, b, b)(a, a, b)^{-1} \in D$ for all $a, b \in G$.*

6. Let $\mathbb{Q}[x]$ be the set of all polynomials in $x$ with rational coefficients. Define a relation $\sim$ on $\mathbb{Q}[x]$ by $f(x) \sim g(x)$ if and only if $f(x) - g(x)$ is divisible by $x^2 + 1$. Prove that $\sim$ is an equivalence relation.

7. Let $R$ be the ring $\{m+n\sqrt{2} \mid m, n \in \mathbb{Z}\}$, and let $I$ be the subset $\{m+n\sqrt{2} \in R \mid m \text{ is even}\}$. Prove that $I$ is an ideal of $R$.

8. Assume that the set $S = \{a + b\sqrt{3} \mid a, b \text{ are rational numbers}\}$ is a commutative ring. Prove that $S$ is a field.
Part B. Do five of the following 8 problems.

1. For which values of the parameters $a$, $b$, and $c$ is the matrix $A = \begin{bmatrix} a & 1 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ invertible? Find the inverse when it exists.

2. Consider the linear transformation with matrix $A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Find a basis for the kernel and a basis for the image of the transformation.

3. Let $A = \begin{bmatrix} 1 & -1 \\ 2 & 4 \end{bmatrix}$. Find all eigenvalues of $A$ and all their corresponding eigenvectors.

4. Find an orthonormal basis for the subspace of $\mathbb{R}^3$ spanned by the vectors $v_1 = \langle 1, 0, -1 \rangle$ and $v_2 = \langle 0, 3, 4 \rangle$.

5. (a) Show that two non-zero vectors are linearly dependent if and only if one is a scalar multiple of the other.
   
   (b) Let $v_1$, $v_2$, and $v_3$ be linearly independent vectors in $\mathbb{R}^n$. Are the vectors $v_1$, $v_2$, and $v_1 + v_2 + v_3$ necessarily linearly independent?

6. Let $\mathbb{C}$ denote the field of complex numbers and $\mathbb{R}$ the field of real numbers. With the usual operations, $\mathbb{C}$ is a vector space over $\mathbb{R}$. Prove that the map $\varphi: \mathbb{C} \rightarrow \mathbb{R}^2$ given by $\varphi(x + iy) = (x, y)$ is an isomorphism of vector spaces.

7. Prove or disprove: The matrix $A = \begin{bmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{bmatrix}$ over $\mathbb{R}$ has determinant equal to $(y - x)(z - x)(z - y)$.

8. Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. Prove that $A^n = 2^{n-1}A$ for all positive integers $n$. 
Part A.

1. Let $a$ and $p$ be integers. If $p$ is prime and $a$ is not divisible by $p$, prove that the additive order of $a$ modulo $p$ is equal to $p$.

**Solution.** The additive order of $[a]_p$ is at most $p$ since $ap \equiv 0 \pmod{p}$.

If $ax \equiv 0 \pmod{p}$, then $p \mid ax$. Since $p$ is prime this implies $p \mid a$ or $p \mid x$. But $p \nmid a$; thus $p \mid x$. Since $x \neq 0$ we have that $p \leq x$. Thus $x$ cannot be less than $p$.

2. Let $G$ and $H$ be groups, and let $\varphi: G \to H$ be a group homomorphism with kernel $\ker(\varphi)$.

Prove that $\ker(\varphi)$ is a normal subgroup of $G$.

**Solution.** Let $n \in \ker(\varphi)$ and $g \in G$. Then $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)^{-1} = 1$. Therefore $gng^{-1} \in \ker(\varphi)$.

3. Let $N$ be a normal subgroup of a group $G$. Prove that the factor group $G/N$ is abelian if and only if $aba^{-1}b^{-1} \in N$ for all elements $a, b \in G$.

**Solution.** $aba^{-1}b^{-1} \in N$ if and only if $Naba^{-1}b^{-1} = N$ if and only if $Nab = Nba$ if and only if $NaNb = NbNa$.

4. Let $G$ be any group with no proper nontrivial subgroups, and assume the order of $G$ is greater than 1. Prove that $G$ is finite cyclic of order $p$ for some prime $p$.

**Solution.** Let $a \in G$, $a \neq 1$. Then $\langle a \rangle$ is a nontrivial subgroup of $G$ and thus is all of $G$. So $G$ is cyclic. If $G$ is infinite then $G \cong \mathbb{Z}$, a contradiction to the hypothesis that $G$ has no proper nontrivial subgroups since $2\mathbb{Z} \leq \mathbb{Z}$. Thus $G$ is finite, and is isomorphic to $\mathbb{Z}_n$ for some $n$. Let $q$ be a prime factor of $n$. If $n$ is not prime then $q < n$ and we have $\langle a^q \rangle$ a proper, nontrivial subgroup of $G$ of order $n/q$, a contradiction. Thus $n = p$ is prime.

5. Let $G$ be a group and let $D = \{(a,a,a) \mid a \in G\}$.

(a) Prove that $D$ is a subgroup of the direct product $G \times G \times G$.

(b) Prove that $D$ is normal in $G \times G \times G$ if and only if $G$ is abelian.

**Hint.** If $D$ is normal, then $(a,a,b)(b,b,b)(a,a,b)^{-1} \in D$ for all $a, b \in G$. 

Solution.

(a) First, $D$ is nonempty since $(e, e, e) \in D$. Now let $(a, a, a), (b, b, b) \in D$. Then $(a, a, a)(b, b, b)^{-1} = (ab^{-1}, ab^{-1}ab^{-1}) \in D$.

(b) (⇒) Let $a, b \in G$. Using the hint, if $D$ is normal, then $(a, a, b)(b, b, b)(a, a, b)^{-1} \in D$ for all $a, b \in G$ by definition of normal subgroup. Now $(a, a, b)(b, b, b)(a, a, b)^{-1} = (aba^{-1}, aba^{-1}, bbb^{-1}) = (aba^{-1}, aba^{-1}, b) \in D$ implies $aba^{-1} = b$, or $ab = ba$. Thus $G$ is abelian.

(⇐) Any subgroup of an abelian group is normal.

6. Let $Q[x]$ be the set of all polynomials in $x$ with rational coefficients. Define a relation $\sim$ on $Q[x]$ by $f(x) \sim g(x)$ if and only if $f(x) - g(x)$ is divisible by $x^2 + 1$. Prove that $\sim$ is an equivalence relation.

Solution. Reflexive. $f(x) - f(x) = 0 = 0 \cdot (x^2 + 1)$, so $f(x) \sim f(x)$.

Symmetric. Suppose $f(x) - g(x) = k(x)(x^2 + 1)$. Then $g(x) - f(x) = -k(x)(x^2 + 1)$.

Transitive. Suppose $f(x) - g(x) = k(x)(x^2 + 1)$ and $g(x) - h(x) = m(x)(x^2 + 1)$. Then $f(x) - h(x) = f(x) - g(x) + g(x) - h(x) = k(x)(x^2 + 1) + m(x)(x^2 + 1) = (k(x) + m(x))(x^2 + 1)$.

7. Let $R$ be the ring $\{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$, and let $I$ be the subset $\{m + n\sqrt{2} \in R \mid m \text{ is even}\}$. Prove that $I$ is an ideal of $R$.

Solution. Let $x = 2m + n\sqrt{2}$, $y = 2p + q\sqrt{2} \in I$. Then

$$x \pm y = (2m \pm 2p) + (n \pm q)\sqrt{2} = 2(m + p) + (n + q)\sqrt{2} \in I.$$ 

Now let $x$ be as above and let $r = a + b\sqrt{2} \in R$. Then

$$rx = (2am + 2bm) + (an + bm)\sqrt{2} = 2(am + bn) + (an + bm)\sqrt{2} \in I.$$ 

Therefore $I$ is an ideal of $R$.

8. Assume that the set $S = \{a + b\sqrt{3} \mid a, b \text{ are rational numbers}\}$ is a commutative ring. Prove that $S$ is a field.

Solution. Let $x = a + b\sqrt{3} \neq 0$. We must show that there are rational numbers $c, d$ for which $(a + b\sqrt{3})(c + d\sqrt{3}) = 1$. In other words, $ac + 3bd = 1$ and $ad + bc = 0$. At least one of $a$ or $b$ must be nonzero. If $a \neq 0$ then $d = \frac{b}{a} \cdot c$, and $ac - \frac{3b^2c}{a} = 1$. Note that $a^2 - 3b^2$ cannot be 0 since if so then $a = \pm b\sqrt{3}$ and $a$ and $b$ are not both rational, a contradiction. Therefore $c = \frac{a}{a^2 - 3b^2}$, $d = -\frac{b}{a} \cdot \frac{a}{a^2 - 3b^2} = -\frac{b}{a^2 - 3b^2}$, and $x^{-1} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}$. Thus every nonzero element of $S$ has a multiplicative inverse. If $a = 0$ then $c = -\frac{ad}{b} = 0$, and $3bd = 1$, or $d = \frac{1}{3b}$. Thus $x^{-1} = \frac{1}{3b}\sqrt{3}$.  

Part B.

1. For which values of the parameters $a$, $b$, and $c$ is the matrix $A = \begin{bmatrix} a & 1 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ invertible? Find the inverse when it exists.

Solution. Since $A$ is upper triangular then its determinant is just the product of the elements in the diagonal. Thus, in this case $\det(A) = a$. So, $A$ is invertible whenever $a \neq 0$.

When $a \neq 0$ the inverse of $A$ is

$$A^{-1} = \begin{bmatrix} a^{-1} & -a^{-1} & a^{-1}(c - b) \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$

2. Consider the linear transformation with matrix $A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Find a basis for the kernel and a basis for the image of the transformation.

Solution. Performing row operations on $A$ we get

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \text{now we subtract } R_1 \text{ from } R_3$$

$$\rightarrow \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{now we subtract } 3R_3 \text{ from } R_2, \text{ and } R_3 \text{ from } R_1$$

$$\rightarrow \begin{bmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{now we subtract } 3R_3 \text{ from } R_2, \text{ and } R_3 \text{ from } R_1$$

It follows that the kernel of $A$ is spanned by $(1, -1, 1)$.

Since $A$ is symmetric, we use the matrix obtained by row operations to see that the range is spanned by $(1, 1, 0)$ and $(0, 1, 1)$.

3. Let $A = \begin{bmatrix} 1 & -1 \\ 2 & 4 \end{bmatrix}$. Find all eigenvalues of $A$ and all their corresponding eigenvectors.
Solution. The characteristic polynomial of $A$ is

$$
\chi_A(\lambda) = \begin{vmatrix}
1 - \lambda & -1 \\
2 & 4 - \lambda
\end{vmatrix} = \lambda^2 - 5\lambda + 6 = (\lambda - 3)(\lambda - 2)
$$

So, the eigenvalues of $A$ are $\lambda = 3$ and $\lambda = 2$.

For $\lambda = 3$ we need to solve the equation $Av = 3v$, which yields the system

$$
\begin{align*}
x - y &= 3x \\
2x + 4y &= 3y
\end{align*}
$$

which has solution space spanned by $(1, -2)$.

For $\lambda = 2$ we need to solve the equation $Av = 2v$, which yields the system

$$
\begin{align*}
x - y &= 2x \\
2x + 4y &= 2y
\end{align*}
$$

which has solution space spanned by $(1, -1)$.

4. Find an orthonormal basis for the subspace of $\mathbb{R}^3$ spanned by the vectors $v_1 = \langle 1, 0, -1 \rangle$ and $v_2 = \langle 0, 3, 4 \rangle$

Solution. The first step on the Gram-Schmidt process says that we fix $v_1$ and define

$$
u_2 = \langle 0, 3, 4 \rangle - \frac{\langle 1, 0, -1 \rangle \cdot \langle 0, 3, 4 \rangle}{\langle 1, 0, -1 \rangle^2} \langle 1, 0, -1 \rangle
= \langle 0, 3, 4 \rangle + 2\langle 1, 0, -1 \rangle
= \langle 2, 3, 2 \rangle
$$

So, right now we have an orthogonal basis. We obtain an orthonormal basis by dividing $v_1$ and $u_2$ by their norm. The final answer is

$$
\left\{ \frac{1}{\sqrt{2}} \langle 1, 0, -1 \rangle, \frac{1}{\sqrt{17}} \langle 2, 3, 2 \rangle \right\}
$$

5. (a) Show that two non-zero vectors are linearly dependent if and only if one is a scalar multiple of the other.

(b) Let $v_1, v_2,$ and $v_3$ be linearly independent vectors in $\mathbb{R}^n$. Are the vectors $v_1, v_2,$ and $v_1 + v_2 + v_3$ necessarily linearly independent?

Solution.

(a) If one vector is a multiple of the other, let us say $v = \alpha w$, then

$$
v - \alpha w = 0
$$

Hence, the vectors are dependent.

If the vectors are linearly dependent, then

$$
\alpha v + \beta w = 0
$$

with WLOG $\alpha \neq 0$. Then we can ‘solve’ for $v$ to get $v = -\frac{\beta}{\alpha} w$. 
(b) Yes, because if
\[ \alpha v_1 + \beta v_2 + \gamma (v_1 + v_2 + v_3) = 0 \]
then
\[ (\alpha + \gamma) v_1 + (\beta + \gamma) v_2 + \gamma v_3 = 0 \]
which forces a system
\[ \gamma = 0 \quad \beta + \gamma = 0 \quad \alpha + \gamma = 0 \]
with a unique (trivial) solution.

6. Let \( \mathbb{C} \) denote the field of complex numbers and \( \mathbb{R} \) the field of real numbers. With the usual operations, \( \mathbb{C} \) is a vector space over \( \mathbb{R} \). Prove that the map \( \varphi : \mathbb{C} \to \mathbb{R}^2 \) given by \( \varphi(x + iy) = (x, y) \) is an isomorphism of vector spaces.

**Solution.** We first check that \( \varphi \) is a homomorphism.
\[
\varphi((x + iy) + (a + bi)) = \varphi(x + a + i(y + b)) \\
= (x + a, y + b) \\
= (x, y) + (a, b) \\
= \varphi(x + iy) + \varphi(a + bi)
\]
and for \( \alpha \in \mathbb{R} \)
\[
\varphi(\alpha(x + iy)) = \varphi(\alpha x + \alpha iy) \\
= (\alpha x, \alpha y) \\
= \alpha(x, y) \\
= \alpha \varphi(x + iy)
\]
Now, since \( \varphi \) is clearly bijective, we are done.

7. Prove or disprove: The matrix
\[
A = \begin{bmatrix}
1 & x & x^2 \\
1 & y & y^2 \\
1 & z & z^2
\end{bmatrix}
\]
over \( \mathbb{R} \) has determinant equal to \( (y - x)(z - x)(z - y) \).
Solution. It is true.

\[
\begin{vmatrix}
1 & x & x^2 \\
1 & y & y^2 \\
1 & z & z^2 \\
\end{vmatrix} = \begin{vmatrix}
0 & x - z & x^2 - z^2 \\
0 & y - z & y^2 - z^2 \\
1 & z & z^2 \\
\end{vmatrix}
\]

now we subtract row 3 from row 1 and row 2

\[
\begin{vmatrix}
0 & x - z & x^2 - z^2 \\
0 & y - z & y^2 - z^2 \\
0 & y - z & y^2 - z^2 \\
\end{vmatrix}
\]

now we factor \(x - z\) and \(y - z\) in rows 1 and 2

\[
= (x - z)(y - z) \begin{vmatrix}
0 & 0 & x + z \\
0 & 1 & y + z \\
0 & 1 & y + z \\
\end{vmatrix}
\]

now we subtract row 2 from row 1

\[
= (x - z)(y - z) \begin{vmatrix}
0 & 0 & x - y \\
0 & 1 & y - z \\
1 & z & z^2 \\
\end{vmatrix}
\]

\[
= (x - z)(y - z)(x - y) \begin{vmatrix}
0 & 0 & 1 \\
1 & z & z \\
1 & z & z \\
\end{vmatrix}
\]

\[
= -(x - z)(y - z)(x - y) = (y - x)(z - x)(z - y)
\]

8. Let \(A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\). Prove that \(A^n = 2^{n-1}A\) for all positive integers \(n\).

Solution. By induction. For \(n = 1\) the result is trivially true.

Assume \(A^k = 2^{k-1}A\), for all \(k \leq n\). Now we want to check that \(A^{n+1} = 2^nA\)

\[
A^{n+1} = A^n A
= (2^{n-1}A) A
= 2^{n-1} A^2
= 2^{n-1}(2A)
= 2^n A
\]
Part A. Do five of the following 8 problems.

1. Let $a$, $b$, $m$, and $n$ be integers, and suppose $am + bn = 1$. Prove that $a$ and $b$ are relatively prime.

2. Let $T = \mathbb{R}^3 - \{(0, 0, 0)\}$. Define a relation $\sim$ on $T$ by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if and only if there exists a nonzero real number $\lambda$ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$. Prove that $\sim$ is an equivalence relation.

3. Let $G$ and $H$ be groups, and let $\varphi: G \rightarrow H$ be an onto group homomorphism. Suppose $G$ is abelian. Prove that $H$ is abelian.

4. Let $G$ be a group, and let $N$ be the subset $\{g \in G \mid gx = xg \text{ for all } x \in G\}$ ($N$ is called the center of $G$). Prove that $N$ is a normal subgroup of $G$.

5. Let $S_n$ denote the group of permutations on the set $\{1, 2, \ldots, n\}$, and let $A_n$ denote the subset consisting of even permutations.
   (a) Prove that $A_n$ is a normal subgroup of $S_n$. You may assume $A_n$ is a subgroup of $S_n$.
   (b) Prove that $S_n/A_n$ is isomorphic to the group $\mathbb{Z}_2 = \{0, 1\}$.

6. Let $R$ be a ring with identity element $1_R$, and let $I$ be an ideal of $R$. Prove that if $1_R$ is in $I$, then $I = R$.

7. Let $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ be defined by $\varphi(a + bi) = a - bi$ for all $a + bi \in \mathbb{C}$. Prove that $\varphi$ is a ring isomorphism.

8. Prove that the only ideals of a field $F$ are $\{0_F\}$ and $F$, where $0_F$ denotes the additive identity element of $F$. 
Part B. Do **five** of the following 8 problems.

1. Let \( A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 3 \end{bmatrix} \), and let \( R \) be the reduced row echelon form for \( A \).

   (a) Find \( R \), determine the (row) rank of \( A \), and find a basis for the row space of \( A \).

   (b) Find a matrix \( P \) such that \( PA = R \).

2. Find an orthonormal basis for the subspace of the Euclidean space \( \mathbb{R}^3 \) spanned by the vectors \( v_1 = (1, 0, 1) \) and \( v_2 = (0, 3, 4) \).

3. Prove: If \( S \) is a finite linearly independent subset of the vector space \( V \) and \( w \in V \) is not in the subspace spanned by \( S \), then the set \( S \cup \{w\} \) is linearly independent.

4. Let \( V \) and \( W \) be vector spaces over the field \( F \) and let \( T \) be a linear transformation from \( V \) into \( W \). Suppose \( V \) is finite dimensional. Prove: \( \text{rank} (T) + \text{nullity} (T) = \dim (V) \).

5. For each natural number \( n \), determine the value of the determinant of the following matrix:

\[
A = \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 0 & 3 & 4 & \cdots & n \\ 1 & 2 & 0 & 4 & \cdots & n \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 1 & 2 & 3 & 4 & \cdots & 0 \end{bmatrix}
\]

6. Let \( A \) be the symmetric matrix \( \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \). Find an orthogonal matrix \( T \) such that \( T^{-1}AT \) is a diagonal matrix.

7. Let \( A = (a_{ij}) \) be an \( n \times n \) matrix over the reals. Show that \( A \) can be expressed in a unique way as \( A = S + K \) where \( S \) is symmetric and \( K \) is skew-symmetric. (*Hint: Consider the matrices \( \frac{1}{2}(A + A^t) \) and \( \frac{1}{2}(A - A^t) \).*)

8. Let \( A \) and \( B \) be \( n \times n \) matrices and suppose \( A \) and \( B \) are similar. Show:

   (a) \( \det(A) = \det(B) \).

   (b) If \( A \) is nonsingular, so is \( B \), and \( A^{-1} \) is similar to \( B^{-1} \).
1. Let $a$, $b$, $m$, and $n$ be integers, and suppose $am + bn = 1$. Prove that $a$ and $b$ are relatively prime.

**Solution.** Suppose $d = (a, b)$. Let $a = ds$, $b = dt$. Then $1 = am + bn = d(sm + tn)$. Therefore $d = 1$.

2. Let $T = \mathbb{R}^3 - \{(0, 0, 0)\}$. Define a relation $\sim$ on $T$ by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if and only if there exists a nonzero real number $\lambda$ such that $x_1 = \lambda x_2$, $y_1 = \lambda y_2$, and $z_1 = \lambda z_2$. Prove that $\sim$ is an equivalence relation.

**Solution.** An equivalence relation must be reflexive, symmetric and transitive.

- **Reflexive.** Let $\lambda = 1$. Then $(x, y, z) = 1 \cdot (x, y, z)$, so $(x, y, z) \sim (x, y, z)$.

- **Symmetric.** Suppose $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$. Then $(x_2, y_2, z_2) = \frac{1}{\lambda}(x_1, y_1, z_1)$.

- **Transitive.** Suppose $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$ and $(x_2, y_2, z_2) = \mu(x_3, y_3, z_3)$. Then $(x_1, y_1, z_1) = \lambda\mu(x_3, y_3, z_3)$.

3. Let $G$ and $H$ be groups, and let $\varphi : G \rightarrow H$ be an onto group homomorphism. Suppose $G$ is abelian. Prove that $H$ is abelian.

**Solution.** Let $h$, $k \in H$. Since $\varphi$ is onto there exist $a$, $b \in G$ such that $\varphi(a) = h$ and $\varphi(b) = k$. Thus $hk = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = kh$.

4. Let $G$ be a group, and let $N$ be the subset $\{g \in G \mid gx = xg \text{ for all } x \in G\}$ ($N$ is called the center of $G$). Prove that $N$ is a normal subgroup of $G$.

**Solution 1.** First note that $1 \in N$ since $1 \cdot x = x \cdot 1$ for all $x \in G$. Thus $N$ is nonempty. Let $m$ and $n$ be elements of $N$, and let $x \in G$. Since $xn = nx$, we have $x = nxn^{-1}$ and thus $n^{-1}x = xn^{-1}$. Therefore $xmn^{-1} = mnx^{-1} = mn^{-1}x$, and $mn^{-1} \in N$. Thus $N \leq G$.

To show that $N$ is normal, let $m$ and $x$ be as above. Then $xm = mx$ and thus $xmx^{-1} = m \in N$.

**Solution 2.** First note that $1 \in N$ since $1 \cdot x = x \cdot 1$ for all $x \in G$. Now let $m$ and $n$ be elements of $N$, and let $x \in G$. Then $xmn = mnx = mnx$; therefore $mn \in N$. Since $xn = nx$, we have $x = nxn^{-1}$ and thus $n^{-1}x = xn^{-1}$. Therefore $n^{-1} \in N$. Thus $N \leq G$.

To show that $N$ is normal, let $m$ and $x$ be as above. Then $xm = mx$ and thus $xmx^{-1} = m \in N$.
5. Let \( S_n \) denote the group of permutations on the set \( \{1, 2, \ldots, n\} \), and let \( A_n \) denote the subset consisting of even permutations.

(a) Prove that \( A_n \) is a normal subgroup of \( S_n \). You may assume \( A_n \) is a subgroup of \( S_n \).
(b) Prove that \( S_n/A_n \) is isomorphic to the group \( \mathbb{Z}_2 = \{0, 1\} \).

Solution.

(a) Let \( \tau \in A_n \) and let \( \sigma \in S_n \). If \( \sigma \) is even, then so is \( \sigma^{-1} \). Similarly, if \( \sigma \) is odd, then so is \( \sigma^{-1} \). Therefore \( \sigma \tau \sigma^{-1} \) can be written as an even number of transpositions.

(b) Solution 1. Let \( \varphi: S_n \rightarrow \mathbb{Z}_2 \) be defined by \( \varphi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases} \).

Clearly \( \varphi \) is an onto homomorphism since even \( \circ \) even = even, odd \( \circ \) odd = even, etc. Moreover, \( \ker(\varphi) = A_n \). Therefore by the First Isomorphism Theorem, \( S_n/A_n \cong \mathbb{Z}_2 \).

Solution 2. Let \( \varphi: S_n/A_n \rightarrow \mathbb{Z}_2 \) be defined by \( \varphi(\sigma A_n) = \begin{cases} 0 & \text{if } \sigma A_n \text{ is even} \\ 1 & \text{if } \sigma A_n \text{ is odd} \end{cases} \).

Clearly \( \varphi \) is an onto homomorphism since even \( \circ \) even = even, odd \( \circ \) odd = even, etc. Moreover, \( |S_n/A_n| = 2 = |\mathbb{Z}_2| \). Therefore \( \varphi \) is an isomorphism.

6. Let \( R \) be a ring with identity element \( 1_R \), and let \( I \) be an ideal of \( R \). Prove that if \( 1_R \) is in \( I \), then \( I = R \).

Solution. Let \( r \in R \). Then since \( 1_R \in I \) we have \( r \cdot 1_R = r \in I \) since \( I \) is an ideal of \( R \).

7. Let \( \varphi: \mathbb{C} \rightarrow \mathbb{C} \) be defined by \( \varphi(a + bi) = a - bi \) for all \( a + bi \in \mathbb{C} \). Prove that \( \varphi \) is a ring isomorphism.

Solution. Clearly \( \varphi \) is onto. \( \varphi \) is also one-to-one since if \( \varphi(a + bi) = a - bi = 0 \), then \( a = 0 \) and \( b = 0 \), and thus \( a + bi = 0 \). \( \varphi \) is a ring homomorphism since

\[
\varphi((a + bi) + (c + di)) = \varphi(a + c + (b + d)i) = a + c - (b + d)i = \varphi(a + bi) + \varphi(c + di)
\]

\[
\varphi((a + bi)(c + di)) = \varphi(ac - bd + (ad + bc)i) = ac - bd - (ad + bc)i = (a - bi)(c - di) = \varphi(a + bi)\varphi(c + di).
\]

Therefore \( \varphi \) is a ring isomorphism.

8. Prove that the only ideals of a field \( F \) are \( \{0_F\} \) and \( F \), where \( 0_F \) denotes the additive identity element of \( F \).

Solution. Suppose \( I \) is an ideal of \( F \). If \( I = \{0_F\} \) then we are done, so suppose \( a \in I \), \( a \neq 0 \). Then there is an element \( a^{-1} \in F \) since \( F \) is a field. Therefore \( a^{-1}a = 1 \in I \) since \( I \) is an ideal. But by \#6, this implies \( I = F \).
Part B.

1. Let \( A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 3 \end{bmatrix} \), and let \( R \) be the reduced row echelon form for \( A \).

   (a) Find \( R \), determine the (row) rank of \( A \), and find a basis for the row space of \( A \).

   (b) Find a matrix \( P \) such that \( PA = R \).

Solution. We need to perform row reduction on \( A \) to get to \( R \). The matrices of the elementary operations we will use will yield \( P \).

\[
A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 3 \end{bmatrix}
\]

now we do \( R_1 \mapsto R_1 - \frac{1}{3} R_3 \)

\[
\rightarrow \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 3 \end{bmatrix}
\]

now we do \( R_2 \mapsto R_2 - \frac{4}{3} R_3 \)

\[
\rightarrow \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} = R
\]

It follows that

\[ P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & - \frac{4}{3} & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & - \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & - \frac{1}{3} \\ 0 & 1 & - \frac{3}{3} \\ 0 & 0 & 1 \end{bmatrix} \]

2. Find an orthonormal basis for the subspace of the Euclidean space \( \mathbb{R}^3 \) spanned by the vectors \( v_1 = (1, 0, 1) \) and \( v_2 = (0, 3, 4) \).

Solution. The first step on the Gram-Schmidt process says that we fix \( v_1 \) and define

\[
u_2 = \begin{bmatrix} 0 & 3 & 4 \end{bmatrix} - \frac{(1, 0, 1) \cdot (0, 3, 4)}{||(1, 0, 1)||^2} (1, 0, 1)
\]

\[ = (0, 3, 4) - 2(1, 0, 1) 
\]

\[ = (-2, 3, 2)
\]

So, right now we have an orthogonal basis. We obtain an orthonormal basis by dividing \( v_1 \) and \( u_2 \) by their norm. The final answer is

\[ \left\{ \frac{1}{\sqrt{2}} (1, 0, 1), \frac{1}{\sqrt{17}} (-2, 3, 2) \right\}
\]

3. Prove: If \( S \) is a finite linearly independent subset of the vector space \( V \) and \( w \in V \) is not in the subspace spanned by \( S \), then the set \( S \cup \{ w \} \) is linearly independent.
Solution. Consider a linear combination of the elements of $S$ and $w$ that is equal to zero. If the scalar with $w$ is zero, then we have a linear combination of the elements of $S$ that is equal to zero, thus all the scalars are equal to zero. If the scalar with $w$ is different from zero, then we can ‘solve’ for $w$ and leave $w$ as a linear combination of the elements of $S$, which would imply that $w \in \text{Span}(S)$. A contradiction.

4. Let $V$ and $W$ be vector spaces over the field $F$ and let $T$ be a linear transformation from $V$ into $W$. Suppose $V$ is finite dimensional. Prove: $\text{rank}(T) + \text{nullity}(T) = \text{dim}(V)$.

Solution. We know that $V/\ker(T) \cong \text{Im}(T)$. So, $\text{dim}(V/\ker(T)) = \text{dim}(\text{Im}(T)) = \text{rank}(T)$.

Since
\[
\text{dim}(V/\ker(T)) = \text{dim}(V) - \text{dim}(\ker(T)) = \text{dim}(V) - \text{nullity}(T)
\]
then
\[
\text{dim}(V) - \text{nullity}(T) = \text{rank}(T)
\]

5. For each natural number $n$, determine the value of the determinant of the following matrix:

\[
A = \begin{bmatrix}
1 & 2 & 3 & 4 & \cdots & n \\
1 & 0 & 3 & 4 & \cdots & n \\
1 & 2 & 0 & 4 & \cdots & n \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
1 & 2 & 3 & 4 & \cdots & 0
\end{bmatrix}
\]

Solution.

\[
\det(A) = \begin{vmatrix}
1 & 2 & 3 & 4 & \cdots & n \\
1 & 0 & 3 & 4 & \cdots & n \\
1 & 2 & 0 & 4 & \cdots & n \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
1 & 2 & 3 & 4 & \cdots & 0
\end{vmatrix}
\]

Now we subtract row 1 to all rows
\[
= (-1)^{n-1}n!
\]
because the matrix above is upper triangular

6. Let $A$ be the symmetric matrix $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$. Find an orthogonal matrix $T$ such that $T^{-1}AT$ is a diagonal matrix.
**Solution.** Since $A$ is symmetric, then its eigenvectors associated to distinct eigenvalues must be orthogonal. So, the only thing we have to do is to get the standard diagonalization of $A$.

The characteristic polynomial of $A$ is

$$\chi_A(\lambda) = (1 - \lambda)^2 - 1 = \lambda^2 - 2\lambda = \lambda(\lambda - 2)$$

For $\lambda = 0$ we get the system

$$\begin{align*}
x - y &= 0 \\
-x + y &= 0
\end{align*}$$

which has solution space spanned by $(1, 1)$. 

For $\lambda = 2$ we get the system

$$\begin{align*}
x - y &= 2x \\
-x + y &= 2y
\end{align*}$$

which has solution space spanned by $(1, -1)$. 

It follows that $T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

7. Let $A = (a_{ij})$ be an $n \times n$ matrix over the reals. Show that $A$ can be expressed in a unique way as $A = S + K$ where $S$ is symmetric and $K$ is skew-symmetric. (Hint: Consider the matrices $\frac{1}{2}(A + A^t)$ and $\frac{1}{2}(A - A^t)$).

**Solution.** Note that the matrix $\frac{1}{2}(A + A^t)$ is symmetric and that the matrix $\frac{1}{2}(A - A^t)$ is skew-symmetric. Also, note that

$$\frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t) = A$$

Now we just have to check the uniqueness of the representation. So, we assume there are matrices $M$ (symmetric) and $N$ (skew-symmetric) such that $A = M + N$. So,

$$M + N = \frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t)$$

which implies

$$M - \frac{1}{2}(A + A^t) = \frac{1}{2}(A - A^t) - N$$

In the previous equation the right hand side is skew-symmetric and the left hand side is symmetric. It follows that

$$M - \frac{1}{2}(A + A^t) = \frac{1}{2}(A - A^t) - N = 0$$

Hence, the representation is unique.
8. Let $A$ and $B$ be $n \times n$ matrices and suppose $A$ and $B$ are similar. Show:

(a) $\det(A) = \det(B)$.
(b) If $A$ is nonsingular, so is $B$, and $A^{-1}$ is similar to $B^{-1}$.

**Solution.** Assume $B = PAP^{-1}$

(a) Since the determinant is multiplicative, then

$$\det(B) = \det(PAP^{-1}) = \det(P) \det(A) \det(P^{-1}) = \det(P) \det(A) \det(P)^{-1} = \det(A)$$

(b) If $A$ is nonsingular, then $\det(A) \neq 0$, which implies $\det(B) \neq 0$, and thus $B$ is non-singular. In this case

$$B^{-1} = (PAP^{-1})^{-1} = (P^{-1})^{-1} A^{-1} P^{-1} = PA^{-1}P^{-1}$$

So, $A^{-1}$ is similar to $B^{-1}$. 
Part A. Solve five of the following eight problems:

1. Prove that if $N \trianglelefteq G$ and $H$ is any subgroup of $G$, then $N \cap H \trianglelefteq H$.

2. Prove that if $H$ and $K$ are finite subgroups of $G$ whose orders are relatively prime, then $H \cap K = \{e\}$.

3. Show that the relation on $\mathbb{Z}$ defined by $a \sim b$ iff $a^2 \equiv b^2 \mod 6$ is an equivalence relation.

4. Suppose that $\phi$ is a homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{30}$ and $\ker(\phi) = \{0, 10, 20\}$. If $\phi(23) = 9$, determine all elements that map to 9. That is, find all $k \in \mathbb{Z}_{30}$ such that $\phi(k) = 9$.

5. (a) Show that $a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ has order 3 in $GL(2, \mathbb{R})$ and $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4.

   (b) Show that $ab$ has infinite order.

6. Prove that $\sigma^2$ is an even permutation for every permutation $\sigma$.

7. Define a new addition and multiplication on $\mathbb{Z}$ by

   $a \oplus b = a + b - 1$ \quad and \quad $a \otimes b = ab - (a + b) + 2$

   Prove that with these operations $\mathbb{Z}$ is an integral domain.

8. Show that a finite commutative ring with no zero-divisors has a multiplicative identity.
Part B. Solve five of the following eight problems:

1. Suppose that $A$ is an $n \times n$ matrix such that $A^3 = 0$ but $A^2 \neq 0$. Show that \{I, A, A^2\} is independent in the space of all $n \times n$ matrices with real entries.

2. Let $A$ be diagonalizable $2 \times 2$ matrix. If $\lambda^4 = 5\lambda$ for each eigenvalue $\lambda$ of $A$, show that $A^4 = 5A$.

3. If $T : V \rightarrow V$ is linear, show that $T^2 = IV$ iff $T$ is an isomorphism and $T^{-1} = T$.

4. (a) Find $A$ if $(A^{-1} - 3I)^T = 2 \begin{pmatrix} -1 & 2 \\ 5 & 4 \end{pmatrix}$

   (b) If $\det(A) = 2$ and $\det(B) = -3$, compute $\det(A^3B^{-1}A^T B^2)$.

5. Invertible $2 \times 2$ matrices with determinant one have the form

   $\begin{pmatrix} a & b \\ c & \frac{1+bc}{a} \end{pmatrix}$, where $a \neq 0$ and $bc \neq 1$, or

   $\begin{pmatrix} 0 & b \\ -\frac{1}{b} & d \end{pmatrix}$, where $b \neq 0$ and $d \neq 0$, or

   $\begin{pmatrix} a & b \\ -\frac{1}{b} & 0 \end{pmatrix}$, where $b \neq 0$

Determine the form(s) of all $2 \times 2$ matrices that are their own inverses.

6. Let $V = \{v \in \mathbb{R} | v > 0\}$. Show that $V$ is a vector space over $\mathbb{R}$ if the vector addition is ordinary multiplication and scalar multiplication is defined by $a \cdot v = v^a$.

7. If $\mathbb{R}^n = \text{span}\{v_1, v_2, \cdots, v_n\}$ and if $x$ and $y$ in $\mathbb{R}^n$ satisfy $x \cdot v_i = y \cdot v_i$ for all $i$, show that $x = y$.

8. Let $P_n$ denote the space of all polynomials with real coefficients that have degree at most $n$ (union the zero polynomial). Find a linear transformation $T : P_2 \rightarrow P_4$ such that

   $T(1) = x^4$, \quad $T(1 + x) = 1 + x^3$ \quad $T(1 + x^2) = 1 - x^2$
Part A.

1. Prove that if $N \trianglelefteq G$ and $H$ is any subgroup of $G$, then $N \cap H \trianglelefteq H$.

**Solution.** We know the intersection of two subgroups of $G$ is a subgroup of $G$. It follows that $N \cap H < H$.

Let $x \in N \cap H$, and $h \in H$. Since $N$ is normal in $G$ and $H \subset G$, then $hxh^{-1} \in N$. Moreover, by closure in $H$ $hxh^{-1} \in H$. So, $hxh^{-1} \in N \cap H$.

2. Prove that if $H$ and $K$ are finite subgroups of $G$ whose orders are relatively prime, then $H \cap K = \{e\}$

**Solution.** This is problem 7 in part A in the exam of Fall 2006.

3. Show that the relation on $\mathbb{Z}$ defined by $a \sim b$ iff $a^2 \equiv b^2 \mod 6$ is an equivalence relation.

**Solution.** Since $a^2 \equiv a^2 \mod 6$, and 6 dividing $a^2 - b^2$ implies that 6 divides $b^2 - a^2$ then the only thing left to check is transitivity. So, assume $a^2 \equiv b^2 \mod 6$ and $b^2 \equiv c^2 \mod 6$, that is $a^2 - b^2 = 6x$ and $b^2 - c^2 = 6y$ for some integers $x, y$. Then,

$$a^2 - c^2 = (a^2 - b^2) + (b^2 - c^2) = 6x + 6y = 6(x + y)$$

Since $x + y \in \mathbb{Z}$ then we are done.

4. Suppose that $\phi$ is a homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{30}$ and $\ker(\phi) = \{0, 10, 20\}$.

If $\phi(23) = 9$, determine all elements that map to 9. That is, find all $k \in \mathbb{Z}_{30}$ such that $\phi(k) = 9$. 

Solution. We know that the pre-image of any element in the range of a homomorphism is a coset of the kernel of the homomorphism. So, in this case,

\[ \phi^{-1}(9) = 23 + \ker(\phi) = \{23, 23 + 10, 23 + 20\} = \{23, 33, 43\} \]

5. (a) Show that \( a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \) has order 3 in \( GL(2, \mathbb{R}) \) and \( b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) has order 4.

(b) Show that \( ab \) has infinite order.

Solution.

(a) Easy computations show

\[ a^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad a^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \]

and

\[ b^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad b^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \]

(b) This follows from

\[ ab = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \quad \text{and thus} \quad (ab)^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \]

for all \( k \in \mathbb{Z}_+ \).

6. Prove that \( \sigma^2 \) is an even permutation for every permutation \( \sigma \).

Solution. This follows from the fact that in the integers

\[ \text{even} + \text{even} = \text{odd} + \text{odd} = \text{even} \]

In this case the number of 2-cycles in the representation of \( \sigma^2 \) is the sum of the number of 2-cycles in \( \sigma \), so it is the sum of two even or two odd numbers.

7. Define a new addition and multiplication on \( \mathbb{Z} \) by

\[ a \oplus b = a + b - 1 \quad \text{and} \quad a \otimes b = ab - (a + b) + 2 \]

Prove that with these operations \( \mathbb{Z} \) is an integral domain.
**Solution.** We first check that \((\mathbb{Z}, \oplus, \otimes)\) is a ring.

Closure is clear, it is also clear that the additive identity is the number 1, and the additive inverse of an element \(a\) is \(2 - a\). Note that this ring (to be) has no multiplicative identity.

Just checking at the formulas for \(\oplus\) and \(\otimes\) we see that both operations are ‘commutative’. So, we have ourselves a commutative ring.

Now assume that for \(a, b \in \mathbb{Z}\) we have

\[
0 = a \otimes b
\]

which means

\[
1 = ab - (a + b) + 2
\]

and this implies

\[
(a - 1)(b - 1) = 0
\]

Hence, either \(a = 1\) or \(b = 1\). Since 1 is the additive identity in our ring, then we are done.

8. Show that a finite commutative ring with no zero-divisors has a multiplicative identity.

**Solution.** This is problem 1 in part A of the exam of Spring 2006.
Part B.

1. Suppose that $A$ is an $n \times n$ matrix such that $A^3 = 0$ but $A^2 \neq 0$. Show that \{I, A, A^2\} is independent in the space of all $n \times n$ matrices with real entries.

**Solution.** If \{I, A, A^2\} is linearly dependent, then there is a non-trivial linear combination of them that equals zero, that is

$$aA^2 + bA + cI = 0$$

for some $a, b, c \in \mathbb{R}$.

But this implies that the minimal polynomial of $A$, $\mu_A(x)$, divides $p(x) = ax^2 + bx + c$. However, $A^3 = 0$ implies that $\mu_A(x) = x, x^2$ or $x^3$ and, since the degree of $p(x)$ is two, then $\mu_A(x) = x, x^2$, which contradicts the assumption $A^2 \neq 0$.

2. Let $A$ be diagonalizable $2 \times 2$ matrix. If $\lambda^4 = 5\lambda$ for each eigenvalue $\lambda$ of $A$, show that $A^4 = 5A$.

**Solution.** Since $A$ is diagonalizable, then there is a matrix $P$ such that $PAP^{-1} = D$, where $D$ is a diagonal matrix with diagonal entries the eigenvalues of $A$.

Since $\lambda^4 = 5\lambda$ for each eigenvalue $\lambda$ of $A$, it is easy to see that $D^4 = 5D$. But this implies that so does $A = P^{-1}DP$, in fact

$$A^4 = (P^{-1}DP)^4 = P^{-1}D^4P = P^{-1}(5D)P = 5(P^{-1}DP) = 5A$$

3. If $T : V \rightarrow V$ is linear, show that $T^2 = I_V$ iff $T$ is an isomorphism and $T^{-1} = T$.

**Solution.** $T^2 = I$ means that the composition of $T$ with itself is the identity. Hence $T$ is its own inverse, and thus it is an isomorphism.

The other direction is immediate.

4. (a) Find $A$ if $(A^{-1} - 3I)^T = 2 \begin{pmatrix} -1 & 2 \\ 5 & 4 \end{pmatrix}$

(b) If $\det(A) = 2$ and $\det(B) = -3$, compute $\det(A^2B^{-1}A^T B^2)$. 
Solution.

(a) Transposing we get

\[(A^{-1} - 3I) = \begin{pmatrix} -2 & 10 \\ 4 & 8 \end{pmatrix} \]

then, adding 3I both sides we get

\[A^{-1} = \begin{pmatrix} 1 & 10 \\ 4 & 11 \end{pmatrix} \]

It follows that

\[A^{-1} = \frac{1}{11 - 40} \begin{pmatrix} 11 & 10 \\ 4 & 1 \end{pmatrix} = \frac{1}{29} \begin{pmatrix} -11 & 10 \\ 4 & -1 \end{pmatrix} \]

(b)

\[
\det(A^3B^{-1}A^T B^2) = \det(A^3) \det(B^{-1}) \det(A^T) \det(B^2) \\
= \det(A)^3 \det(B)^{-1} \det(A) \det(B)^2 \\
= \det(A)^4 \det(B) \\
= 2^4(-3) = -48
\]

5. Invertible \(2 \times 2\) matrices with determinant one have the form

\[
\begin{pmatrix} a & b \\ c & \frac{1+bc}{a} \end{pmatrix}, \text{ where } a \neq 0 \text{ and } bc \neq 1, \text{ or}
\]

\[
\begin{pmatrix} 0 & b \\ -\frac{1}{b} & d \end{pmatrix}, \text{ where } b \neq 0 \text{ and } d \neq 0, \text{ or}
\]

\[
\begin{pmatrix} a & b \\ -\frac{1}{b} & 0 \end{pmatrix}, \text{ where } b \neq 0
\]

Determine the form(s) of all \(2 \times 2\) matrices that are their own inverses.

Solution. The short way to solve this would be to realize that \(A^2 = I\) means that the minimal polynomial of \(A\) divides \(x^2 - 1\). It follows that

\[
\mu_A(x) = x + 1 \quad \text{or} \quad \mu_A(x) = x - 1 \quad \text{or} \quad \mu_A(x) = (x - 1)(x + 1)
\]
In any case, the minimal polynomial of $A$ has distinct roots, thus $A$ is diagonalizable. It follows that $A$ diagonalizes to

$$B = \left( \begin{array}{cc} \pm 1 & 0 \\ 0 & \pm 1 \end{array} \right)$$

So, the answer would be any conjugation of the four matrices $B$ in the previous equation. Of course $\pm Id$ do not yield anything interesting, the others, though, give a big family of matrices.

6. Let $V = \{ v \in \mathbb{R} \mid v > 0 \}$. Show that $V$ is a vector space over $\mathbb{R}$ if the vector addition is ordinary multiplication and scalar multiplication is defined by $a \cdot v = v^a$.

**Solution.** Fix $v, w \in \mathbb{R}_{>0}$ and $a, b \in \mathbb{R}$.

Since both $vw$ and $v^a$ are positive reals, then closure works out. Also,

$$a(v + w) = (vw)^a = v^aw^a = av + aw$$

and

$$(a + b)v = v^{a+b} = v^av^b = av + aw$$

Finally, 0 in this vector space is the number 1, as $v + 1 = v \cdot 1 = v$. It follows that the additive inverse of $v$ in $V$ is $v^{-1}$, which is also a positive real number.

7. If $\mathbb{R}^n = \text{span}\{v_1, v_2, \cdots, v_n\}$ and if $x$ and $y$ in $\mathbb{R}^n$ satisfy $x \cdot v_i = y \cdot v_i$ for all $i$, show that $x = y$.

**Solution.** First note that since the spanning set has the same number as the dimension of the space, then the set is a basis. Now let

$$x = x_1v_1 + x_2v_2 + \cdots + x_nv_n \quad \text{and} \quad x = y_1v_1 + y_2v_2 + \cdots + y_nv_n$$

Then

$$x \cdot v_i = x_1(v_1 \cdot v_i) + x_2(v_2 \cdot v_i) + \cdots + x_n(v_n \cdot v_i)$$

and

$$y \cdot v_i = y_1(v_1 \cdot v_i) + y_2(v_2 \cdot v_i) + \cdots + y_n(v_n \cdot v_i)$$
So,
\[ y_1(v_1 \cdot v_i) + y_2(v_2 \cdot v_i) + \cdots + y_m(v_m \cdot v_i) = x_1(v_1 \cdot v_i) + x_2(v_2 \cdot v_i) + \cdots + x_n(v_n \cdot v_i) \]
or
\[(x_1 - y_1)(v_1 \cdot v_i) + (x_2 - y_2)(v_2 \cdot v_i) + \cdots + (x_n - y_n)(v_n \cdot v_i) = 0\]
for all \(i\).
But this implies
\[ [(x_1 - y_1)v_1 + (x_2 - y_2)v_2 + \cdots + (x_n - y_n)v_n] \cdot v_i = 0 \]
for all \(i\).
So, the vector \(w = (x_1 - y_1)v_1 + (x_2 - y_2)v_2 + \cdots + (x_n - y_n)v_n\) is orthogonal to all vectors in the spanning set of \(\mathbb{R}^n\). It follows that \(w = 0\). Since \(w\) is a linear combination of linearly independent vectors, then \(x_i = y_i\) for all \(i\), and thus \(x = y\).

8. Let \(P_n\) denote the space of all polynomials with real coefficients that have degree at most \(n\) (union the zero polynomial). Find a linear transformation \(T : P_2 \rightarrow P_4\) such that
\[ T(1) = x^4, \quad T(1 + x) = 1 + x^3 \quad T(1 + x^2) = 1 - x^2 \]

**Solution.** Since \(T\) is linear, then
\[ T(x) = T(1 + x - 1) = T(1 + x) - T(1) = 1 + x^3 - x^4 \]
and
\[ T(x^2) = T(1 + x^2 - 1) = T(1 + x^2) - T(1) = 1 - x^2 - x^4 \]
It follows that
\[ T(a + bx + cx^2) = T(a) + T(bx) + T(cx^2) \]
\[ = aT(1) + bT(x) + cT(x^2) \]
\[ = a(x^4) + b(1 + x^3 - x^4) + c(1 - x^2 - x^4) \]
\[ = (b + c) - cx^2 + bx^3 + (a - b - c)x^4 \]
Part A. Do five of the following eight problems:

1. Let $S$ be a set, and let $\mathcal{P}(S) = \{A | A \subset S\}$ be the collection of all subsets of $S$. Define a relation $\sim$ on $\mathcal{P}(S)$ by letting $A \sim B$ if and only if there is a one-to-one correspondence from $A$ to $B$. Prove that $\sim$ is an equivalence relation.

2. Let $G$ be a group and let $f : G \rightarrow G$ be defined by $f(g) = g^{-1}$ for all $g \in G$. Under what conditions is $f$ a group homomorphism? Justify your answer.

3. Let $f : G \rightarrow H$ be a group homomorphism. Prove that $\ker(f)$ is a normal subgroup of $G$.

4. Show that in a finite cyclic group of order $n$ with identity element $e$, the equation $x^m = e$ has exactly $m$ solutions, for each positive integer $m$ that is a divisor of $n$.

5. Let $G$ be any group with no proper nontrivial subgroups, and assume the order of $G$ is greater than 1. Prove that $G$ is cyclic of order $p$ for some prime $p$.

6. (a) Let $R$ be a commutative ring such that $a^2 = a$ for each $a \in R$. Prove that $a + a = 0$ for each $a \in R$.
   
   (b) Prove that $(a + b)(a - b) = a^2 - b^2$ for all $a, b$ in a ring $R$ if and only if $R$ is commutative.

7. Let $R$ be the set of all continuous functions from the set of real numbers to itself. Define addition and multiplication of $f, g \in R$ by
   
   $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$
   
   for all numbers $x$.

   Prove that $R$ is a commutative ring under these operations.

8. Elements $a$ and $b$ of a ring $R$ are called zero divisors if $a$ and $b$ are nonzero and $ab = 0$. Prove that every finite commutative ring with no zero divisors is a field.
Part B. Solve five of the following eight problems:

1. (a) Show that $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ is not invertible for any choice of $a$ and $b$.

(b) If $A$ is any matrix, show that $AA^T$ and $A^TA$ are both symmetric matrices.

2. Find all $3 \times 3$ diagonal matrices $A$ that satisfy $A^2 - 3A - 4I = 0$.

3. If $A$ is an $n \times n$ diagonalizable matrix with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, show that $\det(A) = \lambda_1\lambda_2 \cdots \lambda_n$.

4. Show that
   \[ \langle (u_1, u_2), (v_1, v_2) \rangle = \frac{1}{4}u_1v_1 + \frac{1}{16}u_2v_2 \]
   defines an inner product on $\mathbb{R}^2$.

5. Let $P_n$ be the vector space of polynomials in $x$ of degree at most $n$ with real coefficients union the zero polynomial. Determine the dimension of the subspace of $P_n$ consisting of all polynomials
   \[ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \]
   for which $a_0 = 0$.

6. Show that $\begin{bmatrix} 2 & 1 \\ 1 & -5 \end{bmatrix}$ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ commute if $a - d = 7b$.

7. Suppose $A$ is a square matrix. Suppose $x$ is an eigenvector of $A$ with corresponding eigenvalue $\lambda$, and $y$ is an eigenvector of $A^T$ with corresponding eigenvalue $\mu$. Show that if $\lambda \neq \mu$, then $x \cdot y = 0$.

8. Let $B = \{v_1, v_2, v_3, v_4\}$ be a basis for a vector space $V$. Find the matrix with respect to $B$ of the linear operator $T : V \to V$ defined by $T(v_1) = v_2$, $T(v_2) = v_3$, $T(v_3) = v_4$, and $T(v_4) = v_1$. 
Part A.

1. Let $S$ be a set, and let $\mathcal{P}(S) = \{ A \mid A \subset S \}$ be the collection of all subsets of $S$. Define a relation $\sim$ on $\mathcal{P}(S)$ by letting $A \sim B$ if and only if there is a one-to-one correspondence from $A$ to $B$. Prove that $\sim$ is an equivalence relation.

Solution. Since the identity defines a one-to-one correspondence from a set to itself and if $f : S \to T$ defines a one-to-one correspondence then $f^{-1} : T \to S$ is also a one-to-one correspondence, then we just need to check transitivity. So, assume $f : S \to T$ is a one-to-one correspondence and $g : T \to U$ is also a one-to-one correspondence. Consider the map

$$g \circ f : S \to U$$

Since both $f$ and $g$ are bijective, then so is $fg$.

2. Let $G$ be a group and let $f : G \to G$ be defined by $f(g) = g^{-1}$ for all $g \in G$. Under what conditions is $f$ a group homomorphism? Justify your answer.

Solution. If $f$ is a group homomorphism, then for any $g, h \in G$ we get

$$h^{-1}g^{-1} = (gh)^{-1} = f(gh) = f(g)f(h) = g^{-1}h^{-1}$$

So, $h^{-1}g^{-1} = g^{-1}h^{-1}$ for all $g, h \in G$. Since every element in $G$ is the inverse of an element in $G$, then $G$ is Abelian.

Clearly, if $G$ is Abelian, then $f$ is a homomorphism. Hence,

$$f \text{ is a homomorphism } \iff G \text{ is an Abelian group}$$

3. Let $f : G \to H$ be a group homomorphism. Prove that $\ker(f)$ is a normal subgroup of $G$. 


Solution. Let us first check it is a subgroup. We know the identity of the group is there, so it is not empty. Also, for \( g, h \in ker(f) \)

\[
f(gh) = f(g)f(h) = e \cdot e = e
\]

and

\[
e = f(gg^{-1}) = f(g)f(g^{-1}) = e \cdot f(g^{-1}) = f(g^{-1})
\]

So, \( ker(f) \) is a subgroup of \( G \)

Finally, let \( x \in G \), then

\[
f(xgx^{-1}) = f(x)f(g)f(x^{-1}) = f(x) \cdot e \cdot f(x)^{-1} = f(x)f(x)^{-1} = e
\]

4. Show that in a finite cyclic group of order \( n \) with identity element \( e \), the equation \( x^m = e \) has exactly \( m \) solutions, for each positive integer \( m \) that is a divisor of \( n \).

Solution. Let \( G = \langle g \rangle \) and let \( m \) be a divisor of \( n \). Then the element \( h = g^{n/m} \in G \) has order \( m \) (otherwise the order of \( g \) wouldn’t be \( n \)). The subgroup \( \langle h \rangle \) has \( m \) elements, and all of them (by Lagrange’s theorem) satisfy \( x^m = e \). So, we have at least \( m \) solutions for the equation \( x^m = e \).

Now consider \( x = g^i \in G \) be such that \( x^m = e \). Then

\[
e = (g^i)^m = g^{im}
\]

So, \( n \) divides \( im \), and thus \( i \) is a multiple of \( \frac{n}{m} \). Hence \( g^i \in \langle h \rangle \).

5. Let \( G \) be any group with no proper nontrivial subgroups, and assume the order of \( G \) is greater than 1. Prove that \( G \) is cyclic of order \( p \) for some prime \( p \).

Solution. If \( G \) contains an element \( g \) of infinite order, then \( \mathbb{Z} \cong \langle g \rangle \triangleleft G \), and thus \( G \) contains infinitely many subgroups. So, all elements of \( G \) have finite order.

Let \( g \in G \), if there is an element \( h \in G \) that does not belong to \( \langle g \rangle \), then \( \langle g \rangle \) is a proper subgroup of \( G \), a contradiction. It follows that \( G \) is a (finite) cyclic group. Hence \( G \cong \mathbb{Z}_m \) for some \( m \). We know that \( \mathbb{Z}_m \) contains subgroups of order any divisor of \( m \). It follows that \( G \) must be isomorphic to \( \mathbb{Z}_p \) for some prime number \( p \)
6. (a) Let $R$ be a commutative ring such that $a^2 = a$ for each $a \in R$. Prove that $a + a = 0$ for each $a \in R$.

(b) Prove that $(a + b)(a - b) = a^2 - b^2$ for all $a, b$ in a ring $R$ if and only if $R$ is commutative.

Solution.

(a) 

\[ a + a = (a + a)^2 = a^2 + 2a^2 + a^2 = a + 2a + a = 2(a + a) \]

So, $a + a = 0$.

(b) Assume the ring is commutative, then

\[ (a + b)(a - b) = a^2 - ab + ba - b^2 = a^2 - ab + ab - b^2 = a^2 - b^2 \]

Assume $(a + b)(a - b) = a^2 - b^2$ for all $a, b$ in $R$. Since

\[ (a + b)(a - b) = a^2 - ab + ba - b^2 \quad \text{and} \quad a^2 - b^2 = a^2 - ab + ab - b^2 \]

then $a^2 - ab + ba - b^2 = a^2 - ab + ab - b^2$, which implies $ba = ab$.

7. Let $R$ be the set of all continuous functions from the set of real numbers to itself. Define addition and multiplication of $f, g \in R$ by

\[ (f + g)(x) = f(x) + g(x) \quad \text{and} \quad (f \cdot g)(x) = f(x)g(x) \]

for all numbers $x$.

Prove that $R$ is a commutative ring under these operations.

Solution. Clearly closure holds for both operations (Calculus!!). Also, the zero function is the additive identity and the identity map is the multiplicative identity of $R$.

All the other things needed to check for $R$ to be a commutative ring follow trivially from the fact that $\mathbb{R}$ is a commutative ring.

8. Elements $a$ and $b$ of a ring $R$ are called zero divisors if $a$ and $b$ are nonzero and $ab = 0$. Prove that every finite commutative ring with no zero divisors is a field.
Solution. In problem 8 of part A in the exam of Spring 2003 it is shown that a ring $R$ as the one we are considering must have a one (multiplicative identity). That proof uses that, for a fixed $r \in R^*$, the function $\phi_r : R \to R$ defined by $\phi_r(x) = rx$ is bijective.

Since we know that $R$ has a one, then there must be an $s \in R$ such that $\phi_r(s) = 1$ ($\phi$ is onto!). It follows that $rs = 1$, and thus $r$ has an inverse.
Part B.

1. (a) Show that \( A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \) is not invertible for any choice of \( a \) and \( b \).

(b) If \( A \) is any matrix, show that \( AA^T \) and \( A^T A \) are both symmetric matrices.

Solution.

(a) The determinant of \( A \) is zero no matter what \( a \) and \( b \) are.

(b) \((AA^T)^T = (A^T)^T A^T = AA^T\).

To show \( A^T A \) is symmetric we proceed in the same way.

2. Find all \( 3 \times 3 \) diagonal matrices \( A \) that satisfy \( A^2 - 3A - 4I = 0 \)

Solution. Since \( A \) satisfies \( A^2 - 3A - 4I = 0 \), then the minimal polynomial of \( A \) divides \( x^2 - 3x - 4 = (x - 4)(x + 1) \). It follows that the non-zero entries of \( A \) can only be \(-1\) and/or \(4\) (using that \( A \) is diagonal). So, there are 8 possibilities for \( A \) (too much to type, so I will write that down in an odd way)

\[
A = \begin{bmatrix}
1.5 \pm 2.5 & 0 & 0 \\
0 & 1.5 \pm 2.5 & 0 \\
0 & 0 & 1.5 \pm 2.5 \\
\end{bmatrix}
\]

3. If \( A \) is an \( n \times n \) diagonalizable matrix with eigenvalues \( \lambda_1, \lambda_2, \ldots, \lambda_n \), show that \( \det(A) = \lambda_1 \lambda_2 \cdots \lambda_n \)

Solution. We know \( \det(AB) = \det(A) \det(B) \).

Since \( A \) is diagonalizable, then there is a matrix \( P \) such that \( A = PDP^{-1} \), where \( D \) is diagonal with and diagonal entries given by the \( n \) eigenvalues of \( A \). Hence,

\[
\det(A) = \det(PDP^{-1}) = \det(P) \det(D) \det(P^{-1}) = \det(D) = \lambda_1 \lambda_2 \cdots \lambda_n
\]

4. Show that

\[
< (u_1, u_2), (v_1, v_2) > = \frac{1}{4} u_1 v_1 + \frac{1}{16} u_2 v_2
\]

defines an inner product on \( \mathbb{R}^2 \).
Solution. Let \( u = (u_1, u_2), v = (v_1, v_2) \in \mathbb{R}^2 \).

\[
<u, u> = \frac{1}{4}(u_1)^2 + \frac{1}{16}(u_2)^2
\]

which is greater or equal to zero, and zero only when both \( u_1 \) and \( u_2 \) are zero. Also,

\[
<u, v> = \frac{1}{4}u_1v_1 + \frac{1}{16}u_2v_2 = \frac{1}{4}v_1u_1 + \frac{1}{16}v_2u_2 = v, u>
\]

And finally, for \( \alpha, \beta \in \mathbb{R} \) and \( w = (w_1, w_2) \in \mathbb{R}^2 \)

\[
<\alpha u + \beta v, w> = \langle (\alpha u_1 + v_1, \alpha u_2 + v_2), (w_1, w_2) \rangle = \frac{1}{4}(\alpha u_1 + \beta v_1)w_1 + \frac{1}{16}(\alpha u_2 + \beta v_2)w_2 = \alpha \langle u, w \rangle + \beta \langle v, w \rangle
\]

5. Let \( P_n \) be the vector space of polynomials in \( x \) of degree at most \( n \) with real coefficients union the zero polynomial. Determine the dimension of the subspace of \( P_n \) consisting of all polynomials

\[
a_0 + a_1x + a_2x^2 + \cdots + a_nx^n
\]

for which \( a_0 = 0 \).

Solution. We are assuming that

\[
S = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in P_n; \ a_0 = 0\}
\]

is a subspace (if you want to show it, consider the homomorphism \( \phi: P_n \to \mathbb{R} \) defined by \( \phi(p(x)) = p(0) \))

It is clear that \( S \) is spanned by

\[
B = \{x, x^2, \cdots, x^n\}
\]

Since \( B \) is a subset of the standard basis of \( \mathbb{R}[x] \), then it must be linearly independent. It follows that the dimension of \( S \) is \( n - 1 \).
6. Show that \[
\begin{bmatrix}
2 & 1 \\
1 & -5
\end{bmatrix}
\quad \text{and} \quad 
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\] commute if \(a - d = 7b\).

**Solution.** We want the following two products to be the same:

\[
\begin{bmatrix}
2 & 1 \\
1 & -5
\end{bmatrix}
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
= 
\begin{bmatrix}
2a + c & 2b + d \\
a - 5c & b - 5d
\end{bmatrix}
\]

\[
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\begin{bmatrix}
2 & 1 \\
1 & -5
\end{bmatrix}
= 
\begin{bmatrix}
2a + b & a - 5b \\
2c + d & c - 5d
\end{bmatrix}
\]

Then, the two 1,1 entries being the same implies \(c = b\) (also implies by the two 2,2 entries being the same). So, now we have just one equation:

\[2b + d = a - 5b \quad \text{or} \quad a - d = 7b\]

7. Suppose \(A\) is a square matrix. Suppose \(x\) is an eigenvector of \(A\) with corresponding eigenvalue \(\lambda\), and \(y\) is an eigenvector of \(A^T\) with corresponding eigenvalue \(\mu\). Show that if \(\lambda \neq \mu\), then \(x \cdot y = 0\).

**Solution.** This is problem 7 in part B in the exam of Spring 2008.

8. Let \(B = \{v_1, v_2, v_3, v_4\}\) be a basis for a vector space \(V\). Find the matrix with respect to \(B\) of the linear operator \(T : V \to V\) defined by \(T(v_1) = v_2\), \(T(v_2) = v_3\), \(T(v_3) = v_4\), and \(T(v_4) = v_1\).

**Solution.** Since we are looking for the matrix of \(T\) with respect to the base \(B\), then we have to consider the \(v_1\)'s as if they were the canonical basis of, in this case, \(\mathbb{R}^4\). So,

\[
[T]_B = \begin{bmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]