

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 $\varphi: G \rightarrow H$ 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 $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$. 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) (\Rightarrow) 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.
- (\Leftarrow) Any subgroup of an abelian group is normal.

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.

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

$$x \pm y = (2m \pm 2p) + (n \pm q)\sqrt{2} = 2(m \pm p) + (n \pm q)\sqrt{2} \in I.$$

Now let x be as above and let $r = a + b\sqrt{2} \in R$. Then

$$rx = (2am + 2bn) + (an + bm)\sqrt{2} = 2(am + bn) + (an + bm)\sqrt{2} \in I.$$

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

$$\begin{array}{l} A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 1 & 3 & 2 \end{bmatrix} & \text{now we subtract } R_1 \text{ from } R_3 \\ \rightarrow \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 0 & 1 & 1 \end{bmatrix} & \text{now we subtract } 3R_3 \text{ from } R_2, \text{ and } R_3 \text{ from } R_1 \\ \rightarrow \begin{bmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix} & \text{now we subtract } 3R_3 \text{ from } R_2, \text{ and } R_3 \text{ from } R_1 \end{array}$$

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

$$x - y = 3x \qquad 2x + 4y = 3y$$

which has solution space spanned by $(1, -2)$.

For $\lambda = 2$ we need to solve the equation $Av = 2v$, which yields the system

$$x - y = 2x \qquad 2x + 4y = 2y$$

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

$$\begin{aligned} u_2 &= \langle 0, 3, 4 \rangle - \frac{\langle 1, 0, -1 \rangle \cdot \langle 0, 3, 4 \rangle}{|\langle 1, 0, -1 \rangle|^2} \langle 1, 0, -1 \rangle \\ &= \langle 0, 3, 4 \rangle + 2\langle 1, 0, -1 \rangle \\ &= \langle 2, 3, 2 \rangle \end{aligned}$$

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

$$\gamma = 0 \qquad \beta + \gamma = 0 \qquad \alpha + \gamma = 0$$

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 $\varphi : \mathbb{C} \rightarrow \mathbb{R}^2$ given by $\varphi(x + iy) = (x, y)$ is an isomorphism of vector spaces.

Solution. We first check that φ is a homomorphism.

$$\begin{aligned} \varphi((x + iy) + (a + bi)) &= \varphi(x + a + i(y + b)) \\ &= (x + a, y + b) \\ &= (x, y) + (a, b) \\ &= \varphi(x + iy) + \varphi(a + bi) \end{aligned}$$

and for $\alpha \in \mathbb{R}$

$$\begin{aligned} \varphi(\alpha(x + iy)) &= \varphi(\alpha x + \alpha iy) \\ &= (\alpha x, \alpha y) \\ &= \alpha(x, y) \\ &= \alpha\varphi(x + iy) \end{aligned}$$

Now, since φ 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.

$$\begin{aligned}
 \det(A) &= \begin{vmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{vmatrix} && \text{now we subtract row 3 from row 1 and row 2} \\
 &= \begin{vmatrix} 0 & x-z & x^2-z^2 \\ 0 & y-z & y^2-z^2 \\ 1 & z & z^2 \end{vmatrix} && \text{now we factor } x-z \text{ and } y-z \text{ in rows 1 and 2} \\
 &= (x-z)(y-z) \begin{vmatrix} 0 & 1 & x+z \\ 0 & 1 & y+z \\ 1 & z & z^2 \end{vmatrix} && \text{now we subtract row 2 from row 1} \\
 &= (x-z)(y-z) \begin{vmatrix} 0 & 0 & x-y \\ 0 & 1 & y+z \\ 1 & z & z^2 \end{vmatrix} \\
 &= (x-z)(y-z)(x-y) \begin{vmatrix} 0 & 1 \\ 1 & z \end{vmatrix} \\
 &= -(x-z)(y-z)(x-y) = (y-x)(z-x)(z-y)
 \end{aligned}$$

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 $A^{n+1} = 2^n A$

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