Math 307 Abstract Algebra **Sample final examination questions with solutions**

1. Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and H contains $18, 30$ and 40, Determine H.

   Solution. Since $\gcd(18, 30, 40) = 2$, there exists an $x, y, z \in \mathbb{Z}$ such that $18x + 30y + 40z = 2$. In fact, one easily checks that $2 = 2 * 40 - 2 * 30 - 1 * 18 \in H$. So, H contains $2\mathbb{Z}$, which is the set of all even numbers. If H contains any additional element a, it will be of the form $2k + 1$. Then $1 = (2k + 1) - 2k \in H$ and $H = \mathbb{Z}$. Hence, H cannot contain other elements, and $H = 2\mathbb{Z}$.

2. Let H and K be subgroups of a group G. Show that $H \cup K \leq G$ if and only if $H \leq K$ or $K \leq H$.

   Solution. Let G be a group and let $H, K \leq G$. Assume without loss of generality that $H \leq K$, that is $H \subseteq K$, which implies that $H \cup K = K \leq G$.

   Conversely, assume that $H \not\leq K$ and $K \not\leq H$, that is $H \not\subseteq K$ and $K \not\subseteq H$, which implies that $H \cup K \neq K$ and $H \cup K \neq H$. Then, there exists an $h \in H \backslash K$ and a $k \in K \backslash H$ such that $h, k \in H \cup K$, Suppose, $H \cup K$ were a subgroup of G. Then $hk \in H \cup K$.

   Case 1. If $hk \in H$, then $h^{-1} \in H$ and hence $k = h^{-1}(hk) \in H$, which is a contradiction.

   Case 2. If $hk \in K$, then $k^{-1} \in K$ and hence $h = (hk)k^{-1} \in K$, which is a contradiction. Thus, $H \cup K$ cannot be a subgroup.

3. Suppose a and b are elements in a group such that $|a| = 4, |b| = 2$, and $a^3 b = ba$. Find $|ab|$.

   Solution. We prove that $|ab| = 2$. Note that $(ab)(ab) = a(ba)b = a(a^3 b)b = a^4 b^2 = e$. So, $|ab| = 1$ or 2. If $|ab| = 1$, then a is the inverse of b so that $4 = |a| = |b| = 2$, which is absurd. So, $|ab| = 2$.

4. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

   Solution. Suppose $H = \langle a \rangle = \{a, a^2, \ldots, a^m\}$ and $K = \langle b \rangle = \{b, b^2, \ldots, b^n\}$, where $a^m = b^n = e$, such that $\gcd(m, n) = 1$. Clearly, $e \in H \cap K$. Suppose $c \in H \cap K$ and $|c| = k$. Then k is factor of m and also a factor of n. Thus, $k = 1$ and $c = e$.

5. Suppose G is a set equipped with an associative binary operation $*$. Furthermore, assume that G has an left identity e, i.e., $eg = g$ for all $g \in G$, and that every $g \in G$ has an left inverse g', i.e., $g' * g = e$. Show that G is a group.

   Solution. Let $g \in G$. We first show that the left inverse g' of g is also the right inverse. To see this, let $\hat{g}$ be the left inverse of g'. Then $(\hat{g}) = (\hat{g})(g'g) = (\hat{g}g')g = eg = g$. So, $\hat{g} = g$ satisfies $e = \hat{g}g' = gg'$.

   Now, because $gg' = g'g = e$, we have $ge = g(g'g) = (gg')g = g$.

6. Suppose x is an element of a cyclic group of order 15 and exactly two of x^3, x^5, and x^9 are equal. Determine $|x^{13}|$.

   Solution. Let $x \in G = \langle a \rangle = \{a, \ldots, a^{15}\}$. Clearly, $|x| > 1$, else $e = x^3 = x^5 = x^9$. Note also that $|x|$ is a factor of $|G| = 15$. Thus, $|x| \in \{3, 5, 15\}$. Consider 3 cases.

1. $x^3 = x^5 \neq x^9$. Then $x^2 = x^{5-3} = e$. So, $|x| = 2$, a contradiction.
2. $x^3 \neq x_5 = x^9$. Then $x^4 = x^{9-5} = e$ so that $|x| \in \{2, 4\}$, a contradiction.
3. $x^3 = x^9 \neq x^5$. Then $x^6 = x^{9-3} = e$ so that $|x| \in \{2, 3, 6\}$. Thus, $|x| = 3$ and $|x^{13}| = |x| = 3$.

7. Consider $\sigma = (13256)(23)(46512)$.

   (a) Express σ as a product of disjoint cycles. Solution. $\sigma = (1, 2, 4)(3, 5)$.

   (b) Express σ as a product of transpositions. Solution. $\sigma = (1, 4)(1, 2)(3, 5)$.

   (c) Express σ as a product minimum number of transpositions.

   (Prove that the number is minimum!)

   Solution. σ moves more than 5 numbers in $\{1, \ldots, 6\}$. So, we need at least three transpositions.

8. (a) Let $\alpha = (1, 3, 5, 7, 9, 8, 6)(2, 4, 10)$. What is the smallest positive integer n such that $\alpha^n = \alpha^{-5}$?

   Solution. We need to find the smallest n such that $\alpha^{n+5} = \varepsilon$. Since $|\alpha| = \text{lcm}(5, 3) = 21$, we see that $n = 16$.

   (b) Let $\beta = (1, 3, 5, 7, 9)(2, 4, 6)(8, 10)$. If β^m is a 5-cycle, what can you say about m?

   Solution. Note that β^m is a 5-cycle if and only if $(2, 4, 6)^m = (8, 6)^m = \varepsilon$ and $(1, 3, 5, 7, 9)^m$ is a five cycle. This happen if and only if m is a multiple of $6 = \text{lcm}(3, 2)$ and m is not a multiple of 5. That is $m = 6k$ and k is not a multiple of 5.

9. In S_7 show that $x^2 = (1, 2, 3, 4)$ has no solutions, but $x^3 = (1, 2, 3, 4)$ has at least two.

   Solution. Note that $(x^2)^4 = \varepsilon$. So, $|x| = 1, 2, 4$. Clearly, $|x| \neq 1, 2$, else $x^2 \neq (1, 2, 3, 4)$. If $|x| = 4$, then x is a 4-cycle, or the product of a 4-cycle and a 2-cycle; in either case, $x^2 \neq (1, 2, 3, 4)$.

   A shorter proof is to observe that $x^2 = (1, 2, 3, 4) = (1, 4)(1, 3)(1, 2)$ is an odd permutation. But x^2 must be an even permutation for any $x \in S_n$.

   Let $x \in \{(1, 4, 3, 2), (1, 4, 3, 2)(5, 6, 7)\}$. Then $x^3 = (1, 2, 3, 4)$.

10. Let $H \leq S_n$.

   (a) Show that either $H \leq A_n$ or $|H \cap A_n| = |H|/2$.

   Solution. Suppose $H \leq S_n$. Let $S_1 = H \cap A_n$, and $S_2 = H - S_1$.

   Case 1. If $S_2 = \emptyset$, then $H \leq A_n$.

   Case 2. If $S_2 \neq \emptyset$ and $g \in S_2$ is an odd permutation. Then define $f : S_1 \to S_2$ by $f(x) = gx$.

   It is well defined because for every even permutation $x \in H$, $gx \in H$ is an odd permutation and will be in S_2.

   It is 1-1 because $f(x_1) = f(x_2)$ implies $gx_1 = gx_2$ so that $x_1 = x_2$ by cancellation.

   If is onto because for every $y \in S_2$, we can let $x = g^{-1}y \in H \cap A_n = S_1$ so that $f(x) = y$.

   Since there is a bijection from S_1 to S_2, we see that $|S_1| = |S_2|$, and $|H \cap A_n| = |H|/2$ as asserted.

(b) If $|H|$ is odd, show that $H \leq A_n$.

Solution. Since $|H|$ is odd, it cannot be the case that $|H \cap A_n| = |H|/2$. So, $H \leq A_n$.

11. Let G be a group. Show that $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is an isomorphism if and only if G is Abelian.

    Solution. Suppose G is Abelian. First, we show that ϕ is bijective. Clearly, if $\phi(a) = \phi(b)$, then $a^{-1} = b^{-1}$. Taking inverse on both sides, we see that $a = b$; so ϕ is 1-1. If $a \in G$, then $\phi(a^{-1}) = a$; so ϕ is onto. Now, by commutativity, for any $a, b \in G$. $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$. Thus, ϕ is a group isomorphism.

    Conversely, suppose ϕ is an isomorphism. Then for any $a, b \in G$, $a^{-1}b^{-1} = \phi(a)\phi(b) = \phi(ab) = (ab)^{-1} = b^{-1}a^{-1}$. Taking inverse on both sides, we see that $ba = ab$.

12. Let G be a group with $|G| = pq$, where p, q are primes. Prove that every proper subgroup of G is cyclic. But the whole group may not be cyclic.

    Solution. Let H be a proper subgroup of G. Then $|H| \in \{1, p, q\}$. By Homework 2, or a corollary of Lagrange theorem, H has prime order or order 1 is cyclic.

    Consider S_3 of order 6. Every proper subgroup is cyclic, but S_3 is not.

13. (a) Let $H = \langle (1, 2) \rangle \in S_3$. Write down all the left cosets of H in S_3, and also the right cosets of H in S_3.

    Solution. $(1, 3)H = (1, 2, 3)H = \{(1, 3), (1, 2, 3)\}$, $(2, 3)H = (1, 3, 2)H = \{(2, 3), (1, 3, 2)\}$.

    $H(1, 3) = H(1, 3, 2) = \{(1, 3), (1, 3, 2)\}$, $H(3, 2) = H(1, 2, 3) = \{(3, 2), (1, 2, 3)\}$.

    (b) Let $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} \leq \mathbb{Z}$ under addition. Determine the number of left cosets $a + n\mathbb{Z} = \{a + x : x \in n\mathbb{Z}\}$ of $n\mathbb{Z}$ in $\mathbb{Z}$.

    Solution. The left cosets are the same as right cosets are the n sets:

    $$[k] = \overline{k} = \{nx + k : x \in \mathbb{Z}\}, \qquad k = 0, \ldots, n - 1.$$

    Note that for any $a \in \mathbb{Z}$, $a + n\mathbb{Z} = k \in \{0, 1, \ldots, n - 1\}$ if and only if $a - k$ is a multiple of n. (Division algorithm creates a complete residue system for $n\mathbb{Z}$.)

14. Let G be a group with $|G| = pq$, where p, q are primes. Prove that every proper subgroup of G is cyclic. But the whole group may not be cyclic.

    Solution. Let H be a proper subgroup of G. Then $|H| \in \{1, p, q\}$. By Homework 2, or a corollary of Lagrange theorem, H has prime order or order 1 is cyclic.

    Consider S_3 of order 6. Every proper subgroup is cyclic, but S_3 is not.

15. Let G be a group of order p^2 for a prime p. Show that G is cyclic or $g^p = e$ for all $g \in G$.

    Solution. Note that elements of G have orders in the set $\{1, p, p^2\}$.

    Case 1. There is an element $a \in G$ of order p^2. Then $G = \langle a \rangle$ is cyclic.

    Case 2. No elements in G has order p^2, then each element x in G has order 1 or p; so, $x^p = e$.

16. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.

Solution. No. If $G = \langle a \rangle$ is cyclic, then a^{5k} for $k = 1, \ldots, 10$ are the only elements of order 11. If G is not cyclic then each elements in G not equal to e have order 5 or 11. If x has order 11, then $x, x^2, \ldots, x^{10}$ have order 11 and generate the same subgroup. If y has order 5, then y, y^2, y^3, y^4 have order 5 and generate the same subgroup. So, G can be partitioned into disjoint subsets of the form

$$(1)\ \{e\}, \quad (2)\ \{x, \ldots, x^{10}\}, \quad (3)\ \{y, y^2, y^3, y^4\}.$$

In particular, $55 = 1 + 5r + 4s$ if there are r type (2) subsets and s type (3) subsets in G. Since there are exactly 20 elements of order 11, so $r = 2$. But then there is no $s \in \mathbb{N}$ such that $55 - 1 - 20 = 4s$.

17. Let G be a (**finite**) group, and $H \leq K \leq G$. Prove that

$$|G : H| = |G : K|\,|K : H|.$$

Prove the same result for infinite group G as long as $|G : H|$ is finite.

Solution. Clearly, $|G : H| = |G|/|H| = (|G|/|K|)(|K : H|) = |G : K|\,|K : H|$.

Suppose G is an infinite group. Assume $|G : H| = t$. Then G is a disjoint union of t cosets of H, namely, $g_1H, \ldots, g_kH$. Since $G = g_1H \cup \cdots g_tH \subseteq g_1K \cup \cdots \cup g_tK$, there are at most t left cosets of K in G. Hence $|G : K|$ is finite, say, equal to r. Also, $|K : H|$ is finite. Otherwise, we there is an infinite sequence of elements $k_1, k_2, \cdots \in K$ such that $k_1H, k_2H, \ldots$ are disjoint cosets in $K \leq G$, contradicting there are finitely many disjoint cosets in G. So, assume that $k_1H, \ldots, k_sH$ are the disjoint cosets of H in K. We **claim** that g_ik_jH are all the distinct cosets of H in G. Thus, $|G : H| = rs = |G : K|\,|K : H|$ as asserted.

To prove our claim, first observe that every $g \in G$ lies in a g_iK for some $i = \{1, \ldots, r\}$, so that $g = g_ik$ for some $k \in K$. But then $k \in k_jH$ for some $j \in \{1, \ldots, s\}$. So, $g \in g_ik_jH$. It remains to show that the cosets g_ik_jH are disjoint for $1 \leq i \leq r, 1 \leq j \leq s$. Suppose by contradiction that $g_ik_jH = g_pk_qH$ for $(i,j) \neq (p,q)$. If $i \neq p$, then $g_ik_jH \cap g_pk_qH \subseteq g_iK \cap g_pK = \emptyset$; if $i = p$ but $j \neq q$, then $k_jH \cap k_qH$ is empty and so is $g_ik_jH \cap g_ik_qH$. The result follows.

18. Prove that A_5 has no subgroup of order 30.

Solution. Note that A_5 has elements of the form in disjoint cycle decomposition:

(1) ε, (2) $(i_1, i_2)(j_1, j_2)$ (15 of them), (3) (i_1, i_2, i_3) (20 of them), (4) $(i_1, \ldots, i_5)$ (24 of them).

Suppose $H \leq A_5$ has order 30 and contains n_i element of type (i) for $i = 1, 2, 3, 4$, then $30 = 1 + n_2 + 2n_3 + 4n_4$ is even. So, $n_2 > 0$. Let $\sigma = (i_1, i_2)(j_1, j_2) \in H$. Consider $\tau = (i_1, i_2, j_1) \in A_4$. Then $\tau\sigma \in \tau H = G - H = H\tau$. Thus $\tau\sigma\tau^{-1} = (j_1, i_2)(i_1, j_2) \in H$. Similarly, $\tau^{-1}\sigma\tau = (j_2, i_2)(j_1, i_1) \in H$. But then $K = \{\varepsilon, \sigma, \tau^{-1}\sigma\tau, \tau\sigma\tau^{-1}\}$ is a 4 element subgroup of H, which is impossible by Lagrange Theorem.

19. Suppose G is a group of order n, and $k \in \mathbb{N}$ is relatively prime to n. Show that $g : G \to G$ defined by $g(x) = x^k$ is one-one. If G is Abelian, show that g is an automorphism.

Solution. Note that there are $x, y \in \mathbb{Z}$ such that $nx + ky = 1$. If $x^k = y^k$, then by the fact that $x^n = y^n = e$, we have

$$x = x^{nx+ky} = (x^k)^y = (y^k)^y = y^{nx+ky} = y.$$

Since G is finite, the function $x \mapsto x^k$ is 1-1 if and only if it is bijective. If G is Abelian, then $(xy)^k = x^k y^k$ so that the map $x \mapsto x^k$ is an isomorphism.

20. Show that every $\sigma \in S_n$ is a product of the n-cycle $\alpha = (1, 2, \ldots, n)$ and the 2-cycle $\tau = (1, 2)$.

    Determine the minimum number of α and τ needed for a given σ.

    Solution. Note that $\alpha^k \tau \alpha^{-k} = (k+1, k+2)$ for $k = 1, \ldots, n-2$. Thus, we can generate transpositions of the form $(1, 2), (2, 3), \ldots, (n-1, n)$.

    Now, $(i, i+1)(i+1, i+2)(i, i+1) = (i, i+2)$; so, we get $(i, i+2)$ for all $i = 1, \ldots, n-2$.

    Next, $(i, i+1)(i+1, i+3)(i, i+1) = (i, i+3)$; so, we get $(i, i+3)$ for all $i = 1, \ldots, n-3$. Repeating these arguments, we get (i, j) for all transpositions. So, we can get any $\sigma \in S_n$.

21. If r is a divisor of m and s is a divisor of n, find a subgroup of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ that is isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$.

    Solution. Let $a = m/r, b = n/s$, $H = \{(pa, qb) : p, q \in \mathbb{Z}\}$, and $\phi : \mathbb{Z}_r \oplus \mathbb{Z}_s \to H$ defined by $\phi(p, q) = (pa, qb)$ is an isomorphism.

    1) ϕ is well-defined: If $(p_1, q_1) = (p_2, q_2)$, then $p_1 - p_2 = ru, q_1 - q_2 = sv$ with $r, s \in \mathbb{Z}$. So, $p_1 a - p_2 a = ura = um$ and $q_1 b - q_2 b = svb = sn$. Thus, $\phi(p_1, q_1) = (p_1 a, q_1 b) = (p_2 a, q_2 b) = \phi(p_2, q_2)$.

    2) ϕ is one-one: If $\phi(p_1, q_1) = (p_1 a, q_1 b) = (p_2 a, q_2 b) = \phi(p_2, q_2)$, then $p_1 a - p_2 a = um = ura$ and $q_1 b - q_2 b = svb = sn$ with $r, s \in \mathbb{Z}$ so that $p_1 - p_2 = ru, q_1 - q_2 = sv$.

    3) ϕ is onto: Suppose $(pa, qb) \in H$. Then clearly, $\phi(p, q) = (pa, qb)$.

22. (a) Prove that $\mathbb{R} \oplus \mathbb{R}$ under addition in each component is isomorphic to $\mathbb{C}$.

    Solution. Define $\phi : \mathbb{R} \oplus \mathbb{R} \to \mathbb{C}$ by $\phi(a, b) = a + ib$. One checks that ϕ is an isomorphism.

    (b) Prove that $\mathbb{R}^* \oplus \mathbb{R}^*$ under multiplication in each component is not isomorphic to $\mathbb{C}^*$.

    Solution. Suppose $\phi : \mathbb{C}^* \to \mathbb{R}^* \oplus \mathbb{R}^*$ is an isomorphism. Then ϕ send identity to identity, i.e., $\phi(1) = (1, 1)$. Then $-i \in \mathbb{C}$ has order 4, and $\phi(i) = (a, b)$ must also have order 4. However, $(1, 1) = (a, b)^4 = (a^4, b^4)$ implies that $a, b \in \{1, -1\}$, and $(a, b)^2 = (1, 1)$, which is a contradiction.

23. Let $a = (a_1, \ldots, a_n) \in G_1 \oplus \cdots \oplus G_n$. Determine the order of a in terms of those of $a_1, \ldots, a_n$. (Infinite order is possible.)

    Solution. If a_j with infinite order, then the jth entries of $a^m = (a_1^m, \ldots, a_n^m)$ is not e_j for all $m \in \mathbb{N}$. Thus, a has infinite order. If $|a_j| = m_j$ is finite for each j, and if $a^m = (a_1^m, \ldots, a_n^m) = (e_1, \ldots, e_n)$. Thus, m is a common multiple of $m_1, \ldots, m_n$. Evidently, $m = \text{lcm}(m_1, \ldots, m_n)$ is the smallest positive integer such that $a_j^m = e_j$ for all $j = 1, \ldots, n$.

24. (a) What is the order of the element $14 + \langle 8 \rangle$ in $\mathbb{Z}_{24}/\langle 8 \rangle$?

Solution. Note that $H = \langle 8 \rangle = \{8, 16, 0\}$. Then $14+H \neq H$, $2(14+H) = 28+H = 12+H \neq H$, $3(14+H) = 42+H = 10+H \neq H$, $4(14+H) = 56+H = 0+H = H$. Thus, $14+H$ has order 4.

(b) What is the order of $4U_5(105)$ in the factor group $U(105)/U_5(105)$.

Solution. Note that $U_5(105) = \{1, 11, 16, 26, 31, 41, 46, 61, 71, 76, 86, 101\}$. Then $[4U_5(105)]^2 = 16U_5(105) = U_5(105)$. Thus, $4U_5(106)$ has order 2.

25. (a) Prove that if $H \leq G$ and $|G : H| = 2$, then H is normal.

Solution. If $|G : H| = 2$, then there are two left cosets H, aH with $a \notin H$, and G has two right cosets H, Ha such that $aH = G - H = Ha$. So, H is normal.

(b) Show that A_n is normal in S_n.

Solution. Since $|S_n : A_n| = 2$, A_n is normal in S_n.

26. Let $G = \mathbb{Z}_4 \oplus U(4)$, $H = \langle (2,3) \rangle$ and $K = \langle (2,1) \rangle$. Show that G/H is not isomorphic to G/K.

Note that $H = \{(2,3), (0,1)\}$ and $K = \{(2,1) = (0,1)\}$.

Then $G/H = \{(0,1)+H, (1,1)+H, (2,1)+H, (3,1)+H\}$ isomorphic to $\mathbb{Z}_4$,

and $G/K = \{(0,1)+K, (0,3)+K, (1,1)+K, (1,3)+K\}$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

27. Let G be a finite group, and H be a normal subgroup of G.

(a) Show that the order of aH in G/H must divide the order of a in G.

Solution. Suppose $|a| = m$. Then $(aH)^m = eH = H$. So, $|aH|$ is a factor of m.

(b) Show that it is possible that $aH = bH$, but $|a| \neq |b|$.

Solution. Suppose $G = \mathbb{Z}_6$, $H = \{0, 3\}$. Then $0 + H = 3 + H$ where $|0| = 1$ and $|3| = 2$.

28. If G is a group and $|G : Z(G)| = 4$, prove that $G/Z(G)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Solution. If $|G/Z(G)| = 4$, it is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \otimes \mathbb{Z}_2$. If $G/Z(G)$ is cyclic, then G is Abelian so that $G = Z(G)$ and $|G/Z(G)| = 1$, a contradiction.

29. Suppose that $N \lhd G$ and $|G/N| = m$, show that $x^m \in N$ for all $x \in G$.

Solution. By Lagrange theorem, $(xN)^m = eN = N$ in G/N. Thus, $x^m \in N$.

30. (a) Explain why $x \mapsto 3x$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{10}$ is not a homomorphism.

(b) Prove that there is no isomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Solution. (a) In $\mathbb{Z}_{12}$, $[0] = [12]$. But then $\phi([0]) = [0] \neq [6] = [36] = \phi([12])$ in $\mathbb{Z}_{10}$.

(b) Note that $(1,0)$ has order 8 in $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, but $\phi(1,0) \in \mathbb{Z}_4 \oplus \mathbb{Z}_4$ has order at most 4.

31. How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$. How many are there to $\mathbb{Z}_8$?

Solution. Note that a homomorphism $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ is completely determined by $\phi([1]_m) = [k]_n$ with $k = 0, 1, \ldots, n-1$. In order that ϕ is well-defined, $[x]_m = [y]_m$ should ensure $[kx]_n = [ky]_n$. The condition reduces to: $m|(x-y)$ implies $n|k(x-y)$, equivalently, $n|km$. It will be an isomorphism if $\phi([i]) = [1]$ for some i because we can get $\phi([xi]) = [x]$ for every $x \in \mathbb{Z}_n$.

Thus, $\phi([1])$ is a homomorphism with $\phi([1]) = [k]$ if and only if $k = 0, 2, 4, 6$. Of course, none of these homomorphisms is onto.

32. Prove that $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ by $\phi(a, b) = a - b$ is a homomorphism. Determine the kernel, and $\phi^{-1}(\{3\}) = \{(x, y) \in \mathbb{Z} \oplus \mathbb{Z} : \phi(x, y) = 3\}$.

    Solution. $\phi((a, b)+(c, d)) = \phi(a+c, b+d) = (a+c)-(b+d) = (a-b)+(c-d) = \phi(a, b)+\phi(c, d)$ for any $(a, b), (c, d) \in \mathbb{Z} \oplus \mathbb{Z}$. So, ϕ is an homomorphism.

    $Ker(\phi) = \{(a, b) : 0 = \phi(a, b) = a - b\} = \{(a, a) : a \in \mathbb{Z}\}$.

33. For each pair of positive integer m and n, show that the map from $\mathbb{Z}$ to $\mathbb{Z}_m \oplus \mathbb{Z}_n$ defined by $x \mapsto ([x]_m, [x]_n)$ is a homorphism.

    (a) Determine the kernel when $(m, n) = (3, 4)$.

    (b) Determine the kernel when $(m, n) = (6, 4)$.

    (c) (Extra 4 points.) Generalize the result.

    Solution. The map is an homomorphism because for any $a, b \in \mathbb{Z}$,

    $$\phi(a + b) = ([a + b]_m, [a + b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n) = \phi(a) + \phi(b).$$

    (a) $\phi(x) = ([x]_3, [x]_4) = ([0], [0])$ if and only if $3|x$ and $4|x$. So, $Ker(\phi) = \{12k : k \in \mathbb{Z}\}$.

    (b) $\phi(x) = ([x]_6, [x]_4) = ([0], [0])$ if and only if $6|x$ and $4|x$. So, $Ker(\phi) = \{12k : k \in \mathbb{Z}\}$.

    (c) $\phi(x) = ([x]_m, [x]_n) = ([0], [0])$ if and only if $m|x$ and $n|x$. So, $Ker(\phi) = \{\ell k : k \in \mathbb{Z}\}$, where $\ell = \text{lcm}(m, n)$.

34. (Optional.) Suppose $K \leq G$ and $N \triangleleft G$. Show that KN/N is isomorphic to $K/(K \cap N)$.

    Solution. First, note that KN is a subgroup. Reason: $e \in KN$ is non-empty; if $k_1n_1, k_2n_2 \in KN$ then by the normality of N $(k_1n_1)(k_2n_2)^{-1} = k_1n_1n_2^{-2}k_2^{-1} = k_1n_3k_2^{-1} = k_1k_2^{-1}n_4 = k_3n_4 \in KN$ for some $n_3, n_4 \in N$ and $k_3 \in K$.

    Second, note that $K \cap N$ is normal in K because $k(K \cap N)k^{-1} = kKk^{-1} \cap kNk^{-1} = K \cap N$ for any $k \in K$.

    Third, note that N is normal in KN because $(kn)N(kn)^{-1} = knNn^{-1}k^{-1} = N$ for any $kn \in KN$.

    Define $\phi : KN/N \to K/(K \cap N)$ by $\phi(knN) = \phi(kN) = k(K \cap N)$ for any $kn \in KN$.

    It is well-defined: If $k_1n_1 = k_2n_2$, then $k_2^{-1}k_1 = n_2n_1^{-1} \in K \cap N$ so that $k_1(K \cap N) = k_2(K \cap N)$.

    It is 1-1: Note that all elements in KN/N has the form $(kn)N = kN$. If $\phi(k_1N) = \phi(k_2N)$ then $k_1(K \cap N) = k_2(K \cap N)$. Thus, $k_2^{-1}k_1 \in K \cap N \subseteq N$. Thus, $k_1N = k_2N$.

    It is onto because for any $k(K \cap N)$ in $K/(K \cap N)$, we have $\phi(kN) = k(K \cap N)$.

    Now, $\Phi((k_1N)(k_2N)) = \phi(k_1k_2N) = k_1k_2(K \cap N) = k_1(K \cap N)k_2(K \cap N) = \phi(k_1N)\phi(k_2N)$.

35. (a) Let G be the group of nonzero real numbers under multiplication. Suppose r is a positive integer. Show that $x \mapsto x^r$ is a homomoprhism. Determine the kernel, and determine r so that the map is an isomorphism.

    (b) Let G be the group of polynomial in x with real coefficients. Define the map $p(x) \mapsto P(x) = \int p(x)$ such that $P(0) = 0$. Show that f is an homomorphism, and determine its kernel.

    Solution. (a) Evidently, ϕ is well-defined and $\phi(xy) = x^r y^r = \phi(x)\phi(y)$ for all $x, y \in \mathbb{R}^*$. So, ϕ is an homomorphism. Now, $\phi(x) = x^r = 1$ if and only if (i) $x = 1$ or (ii) r is even and $x = -1$. So, $Ker(\phi) = \{1\}$ if r is odd, and $Ker(\phi) = \{1, -1\}$ if r is even.

    If r is even, then $Ker(\phi)| > 1$ so that ϕ is not injective and therefore not bijective.

    If r is odd, then ϕ is one-one and every $x \neq 0$ has a unique real root $x^{1/r}$. So, ϕ is an isomorphism.

    (b) Let $p(x) = a_0 + \cdots + a_n x^n$. Because we assume that $\phi(p(x)) = P(x)$ such that $P(0) = 0$, we have $\phi(p(x)) = a_0 x + a_1 x^2/2 + \cdots + a_n x^{n+1}/(n+1)$. Suppose $p(x)$ and $q(x)$ are two real polynomial. Then $\phi(p(x) + q(x)) = \int(p(x) + q(x)) = \int p(x) + \int q(x) = \phi(p(x)) + \phi(q(x))$. Here the integration constant is always 0 by assumption.

    If $p(x)$ is not the zero polynomial of degree $n \geq 0$, then $\int p(x)$ has degree $n + 1$ is nonzero. Thus, $Ker(\phi)$ contains only the zero polynomial.

36. Show that if $\phi : G_1 \to G_2$ is an homomorphism, and K is a normal subgroup of G_2, then $\phi^{-1}(K)$ is a normal subgroup of G_1.

    Proof. It follows from the classnote, or the proof in the book. Let K be normal in G_2 and $H = \phi^{-1}(K)$ in G_1. Then for any $a \in G_1$, consider aHa^{-1}. Since

    $$\phi(aHa^{-1}) = \{\phi(a)\phi(h)\phi(a)^{-1} : h \in H\} = \phi(a)K\phi(a)^{-1} = K$$

    by the normality of K in G_2, we see that $H = \phi^{-1}(K) = aHa^{-1}$. So, H is normal in G_1.

37. (a) Determine all homomorphisms from $\mathbb{Z}_n$ to itself.

    (b) Find a homomorphism from $U(30)$ to $U(30)$ with kernel $\{1, 11\}$ and $\phi(7) = 7$.

    Solution. (a) Suppose $\phi(1) = k \in \mathbb{Z}_n$. For ϕ to be well-defined, we need $a = b$ in $\mathbb{Z}_n$, i.e., $n|(a - b)$ implies that $ka = kb$ in $\mathbb{Z}_n$, which is always true. So, there are n homomorphisms.

    (b) Note that $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\} = \langle 7 \rangle \times \langle 11 \rangle$. Given $\phi(7) = 7$ and $\phi(11) = 1$, the homomorphism is completely determined. It is a 2 to 1 map such that $\phi(1) = \phi(11) = 1$, $\phi(7) = \phi(17) = 7$, $\phi(13) = \phi(23) = 13$, $\phi(19) = \phi(29) = 19$.

38. Let p be a prime. Determine the number of homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ to $\mathbb{Z}_p$.

    Solution. If ϕ is a homomorphism such that $\phi(1, 0) = x$ and $\phi(0, 1) = y$, then $\phi(a, b) = a\phi(1, 0) + b\phi(0, 1) = ax + by$. For each choice of $(x, y) \in \mathbb{Z}_p, \mathbb{Z}_p$, $(a_1, b_1) = (a_2, b_2)$ implies that $p|(a_1 - a_2)$ and $p|(b_1 - b_2)$. So, $p|(a_1 x + b_1 y - a_2 x - b_2 y)$. Thus, ϕ is well-defined, and satisfies $\phi((a, b) + (c, d)) = (a + c)x + (b + d)y = \phi(a, b) + \phi(c, d)$. So, ϕ is a homomorphism. Hence, there are p^2 choices.

39. Show that if M and N are normal subgroup of G and $N \leq M$, then $(G/N)/(M/N)$ is isomorphic to G/M.

Solution. Consider $\phi : G/N \to G/M$ defined by $\phi(gN) = gM$.

To show that g is well-defined, let $g_1N = g_2N$ in G/N. Then $g_1^{-1}g_2 \in N \leq M$. Then $g_1M = g_2M$.

To show that g is a homomorphism, note that for any $g_1N, g_2N \in G/N$, $\phi(g_1Ng_2N) = \phi(g_1g_2N) = g_1g_2M = g_1Mg_2M = \phi(g_1N)\phi(g_2N)$.

To show that g is surjective, let $gM \in G/M$, then $\phi(gN) = gM$.

Consider the kernel of ϕ, we have $\phi(gN) = gM = M$ if and only if $g \in M$, i.e., $gN \in M/N = \{mN : m \in M\}$.

Now the image of ϕ is isomorphic to $(G/N)/Ker(\phi)$, the result follows.

40. (a) Give an example of a subset of a ring that is a subgroup under addition but not a subring.

(b) Give an example of a finite non-commutative ring.

Solution. (a) Let $H = \langle(2,3)\rangle \in \mathbb{Z} \oplus \mathbb{Z}$. Then $H = \{(2k, 3k) : k \in \mathbb{Z}\}$ is a subgroup under addition. But $(2,3)(2,3) = (4,9) \notin H$.

(b) Let $R = M_2(\mathbb{Z}_2)$. Then there are 2^4 elements because each entries has two choices. Clearly, $AB \neq BA$ if $A = B^t = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

41. Show that if m, n are integers and a, b are elements in a ring. Then $(ma)(nb) = (mn)(ab)$.

Solution. If m or n is zero, then both sides equal 0. If $m, n \in \mathbb{N}$, then

$$(\underbrace{a + \cdots + a}_{m})(\underbrace{b + \cdots + b}_{n}) = (\underbrace{ab + \cdots + ab}_{mn}) = (mn)(ab).$$

If m is negative and n is positive, then $(ma)(nb) + (|m|a)(nb) = ((m + |m|)a)(nb) = 0$ so that $(ma)(nb) = -(|m|n)(ab) = (mn)(ab)$. Similarly, if m is positive and n is negative, then $(ma)(nb) = (mn)(ab)$. Finally, if m, n are negative, then $(ma)(nb) = (-|m|a)(-|n|b) = |mn|(ab) = (mn)(ab)$.

42. Let R be a ring.

(a) Suppose $a \in R$. Shown that $S = \{x \in R : ax = xa\}$ is a subring.

(b) Show that the center of R defined by $Z(R) = \{x \in R : ax = xa \text{ for all } a \in R\}$ is a subring.

Solution. (a) Note that $0 \in S$ is non-empty. Suppose $x, y \in S$. Then $ax = xa$ and $ay = ya$. So, $a(x - y) = ax - ay = xa - ya = (x - y)a$. So, $x - y \in S$. Also, $a(xy) = (xa)y = (xy)a$. So, $xy \in S$. It follows that S is a subring.

(b) Note that $0 \in S$ is non-empty. Suppose $x, y \in Z(R)$. Then $ax = xa$ and $ay = ya$. So, $a(x - y) = ax - ay = xa - ya = (x - y)a$ for any $a \in R$. So, $x - y \in Z(R)$. Also, $a(xy) = (xa)y = (xy)a$ for any $a \in R$. So, $xy \in Z(R)$. It follows that $Z(R)$ is a subring.

43. Let R be a ring.

(a) Prove that R is commutative if and only if $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

(b) Prove that R is commutative if $a^2 = a$ for all $a \in R$.

Solution. (a) If R is commutative, then $(a+b)(a-b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Suppose $(a+b)(a-b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Then $ab - ba = 0$, i.e., $ab = ba$.

(b) Suppose $a^2 = a$ for all $a \in R$. Then for any $a, b \in R$, $a^2 + b^2 = a + b = (a+b)^2 = a^2 + ab + ba + b^2$ so that $ab + ba = 0$. Hence, $ab = -ba$ so that $ab = (ab)^2 = (-ba)^2 = (-1)^2(ba)^2 = ba$.

44. Show that every nonzero element of $\mathbb{Z}_n$ is a unit (element with multiplicative inverse) or a zero-divisor.

Solution. Let $k \in \mathbb{Z}_n$ be nonzero. If $\gcd(k, n) = d$, then for $m = n/d \neq 0$ in $\mathbb{Z}_n$, we have $km = rn = 0$ for some $r \in \mathbb{Z}$. So, k (also, m) is a zero divisor. If $\gcd(k, n) = 1$, then by the Euclidean algorithm, there are $x, y \in \mathbb{Z}$ such that $kx + ny = 1$. Thus, in $\mathbb{Z}_n$ we have $1 = kx + ny = kx$. Thus, $x \in \mathbb{Z}_n$ satisfies $kx = 1$. So, k is a unit.

45. (a) Given an example of a commutative ring without zero-divisors that is not an integral domain.

(b) Find two elements a and b in a ring such that a, b are zero-divisors, $a + b$ is a unit.

Solution. (a) Let $R = 2\mathbb{Z}$. Then R has is a commutative ring without zero-divisors. But R has no unit. So, R is not an integral domain.

(b) Consider $2, 3 \in \mathbb{Z}_6$. Then $2, 3$ are zero-divisors, and $2 + 3 = 5$ is a unit as $5^2 = 1$.

46. (a) Give an example to show that the characteristic of a subring of a ring R may be different from that of R.

(b) Show that the characteristic of a subdomain of an integral domain D is the same as that of D.

Solution. (a) Consider $\mathbb{Z}_4$ and $S = \{0, 2\} \subseteq \mathbb{Z}_4$. Then $\text{char}(\mathbb{Z}_4) = 2$ and $\text{char}(S) = 2$.

(b) Suppose D' is a subdomain of D with unity 1. Then D' has a unity $1'$. Note that$1' = 1 \cdot 1'$ in D, and $1' \cdot 1' = 1'$ in D'. So, $1' \cdot 1' = 1 \cdot 1'$ and $1 = 1'$ by cancellation. So, $\text{char}(D) = \text{char}(D') = |1|$.

47. An element a of a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$.

(a) Show that if a and b are nilpotent elements of a commutative ring, then $a + b$ is also nilpotent.

(b) Show that a ring R has no nonzero nilpotent element if and only if 0 is the only solution of $x^2 = 0$ in R.

Solution. (a) Suppose $a^n = 0 = b^m$ with $n, m \in \mathbb{N}$. Because R is commutative, the Binomial theorem applies and

$$(a+b)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} a^j b^{m+n-j} = 0$$

by the fact that $a^j = 0$ or $b^{n+m-j} = 0$ depending on $j \geq n$ or $j < n$.

(b) If there is a nonzero $x \in R$ satisfies $x^2 = 0$, then x is a nilpotent. If $y \in R$ is a nonzero nilpotent and $k > 1$ is the smallest positive integer such that $y^k = 0$, then $x = y^{k-1}$ satisfies $x^2 = y^{2k-2} = y^k y^{k-2} = 0$.

48. Show that the set of all nilpotent elements of a communtative ring is an ideal.

Solution. Let A be the set of nilpotent elements of a commutative ring R. First, $0 \in A$; if $x, y \in A$ so that $x^n = 0 = y^m$, then $(x-y)^{m+n} = 0$ by the same proof as in (a) of the previous question. Thus, $x - y \in A$. Moreover, if $z \in R$, then $(xz)^n = x^n z^n = 0$. So, A is an ideal.

49. (a) Given an example to show that a factor ring of an integral domain may have zero-divisors.

(b) Give an example to show that a factor ring of a ring with zero-divisors may be an integral domain.

Solution. (a) Let $R = \mathbb{Z}$ and $S = 4\mathbb{Z}$. Then R/S is isomorphic to $\mathbb{Z}_4$, which has zero divisors.

(b) Let $R = \mathbb{Z}_4$ and $S = \{0, 2\}$. Then R has zero divisor 2, and R/S is isomorphic to $\mathbb{Z}_2$ has no zero divisors.

50. Suppose R is a commutative ring with unity and $\text{char}R = p$, where p is a prime. Show that $\phi : R \to R$ defined by $\phi(x) = x^p$ is a ring homomorphism.

Solution. Note that for $k = 1, \ldots, p-1$, $\binom{p}{k} = p!/(k!(p-k)!)$ is divisible by p. Thus, $\phi(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p = \phi(x) + \phi(y)$, and $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$. So, ϕ is a ring homomophism.

51. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism such that $\phi(R) \neq \{0'\}$.

(a) Show that if R_1 has unity and R_2 has no zero-divisors, then $\phi(1)$ is a unity of R_2.

(b) Show that the conclusion in (a) may fail if R_2 has zero-divisors.

Solution. (a) Let $\phi(x) = y$ be nonzero in R_2. Then $\phi(1)^2\phi(x) = \phi(x) = \phi(1)\phi(x)$. Thus, $\phi(1)^2 = \phi(1)$ and $\phi(1) \neq 0$. For any $z \in R_2$, $\phi(1)^2 z = \phi(1)z$ so that $\phi(1)z = z$, and $z\phi(1) = z\phi(1)^2$ so that $z = z\phi(1)$. The result follows.

(b) Suppose $\phi : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ such that $\phi(n) = (n, 0)$. Then $\phi(1) = (1, 0)$ is not the unity in $\mathbb{Z} \oplus \mathbb{Z}$.

52. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism.

(a) Show that if A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

(b) Give an example to show that $\phi(A)$ may not be an ideal of R_2.

(c) (Optional, extra 2 points) Show that if B is an ideal of R_2, then $\phi^{-1}(B)$ is an ideal of R_1.

Solution. (a) Suppose A is an ideal in R_1. Then $0 \in R_1$, for any $a_1, a_2 \in A$ and $x \in R_1$, $a_1 - a_2, a_1 y, y a_1 \in A$. Thus, for any $b_1, b_2 \in \phi(A)$ and $y \in \phi(R_1)$, we have $a_1, a_2 \in A$ and $x \in R_1$ such that $\phi(a_1) = b_1, \phi(a_2) = b_2$ and $\phi(x) = y$ so that $b_1 - b_2 = \phi(a_1) - \phi(a_2) = \phi(a_1 - a_2), b_1 y = \phi(a_1)\phi(x) = \phi(a_1 x), y b_1 = \phi(x)\phi(a_1) = \phi(x a_1) \in \phi(A)$. Thus, $b_1 - b_2, b_1 y, y b_1 \in \phi(A)$. Hence $\phi(A)$ is an ideal in $\phi(R_1)$.

(b) Consider $\phi : \mathbb{R} \to M_2(\mathbb{R})$ defined by $\phi(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$. Then ϕ is a ring homomorphism, and $\phi(\mathbb{R})$ is not an ideal.

(c) Suppose B is an ideal in R_2. Then $0' \in R_2$, for any $b_1, b_2 \in B$ and $y \in R_2$, $b_1 - b_2, b_1 y, y b_1 \in B$. Now, for any $a_1, a_2 \in \phi^{-1}(B)$ and $x \in R_1$, we have $\phi(a_1), \phi(a_2) \in B$ and $\phi(x) \in R_2$ so that $\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2), \phi(a_1 x) = \phi(a_1)\phi(x), \phi(x a_1) = \phi(x)\phi(a_1) \in B$. Thus, $a_1 - a_2, a_1 x, x a_1 \in \phi^{-1}(B)$. Hence $\phi^{-1}(B)$ is an ideal in R_1.

53. If $\phi : R \to S$ is a ring homomorphism, prove that the map $\bar{\phi} : R[x] \to S[x]$ defined by

$$\bar{\phi}(a_0 + \cdots + a_n x_n) = \phi(a_0) + \cdots + \phi(a_n)x^n$$

is a ring homomorphism.

Solution. Let $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$. We may assume $m = n$ by adding terms of the form $0x^k$ to the polynomial with lower degree. Then

$$\bar{\phi}(f(x) + g(x)) = \phi(a_0 + b_0) + \cdots + \phi(a_n + b_n)x^n$$

$$= [\phi(a_0) + \cdots + \phi(a_n)x^n] + [\phi(b_0) + \cdots + \phi(b_n)x^n] = \bar{\phi}(f(x)) + \bar{\phi}(g(x)).$$

Also $f(x)g(x) = \sum_{k=0}^{2n} c_k x^k$ with $c_k = \sum_{i+j=k} a_i b_j$ for $k = 0, \ldots, 2n$. So,

$$\bar{\phi}(f(x))\bar{\phi}(g(x)) = \left(\sum \phi(a_i)x^i\right)\left(\sum \phi(b_j)x^j\right) = \tilde{c}_k x^k$$

such that $\tilde{c}_k = \sum_{i+j=k} \phi(a_i)\phi(b_j) = \phi(\sum_{i+j=k} a_i b_j) = \phi(c_k)$ for $k = 0, \ldots, 2n$. Thus,

$$\bar{\phi}(f(x))\bar{\phi}(g(x)) = \bar{\phi}(f(x)g(x)).$$

54. Let D be an integral domain.

(a) Show that for any two nonzero polynomials $f(x), g(x) \in D[x]$. Show that

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

(b) Show that a nonconstant polynomial in $D[x]$ has no multiplicative inverse.

Solution. (a) Let $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$ with $a_n \neq 0$ and $b_m \neq 0$. Then $f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k$ with $c_k = \sum_{i+j=k} a_i b_j$ for $k = 0, \ldots, m+n$. In particular, $c_{m+n} = a_n b_m \neq 0$ in D. Thus, $\deg(fg) = \deg(f)\deg(g)$.

(b) Suppose $f(x)$ has degree $n \geq 1$. Then for any nonzero $g(x) \in D[x]$, $f(x)g(x)$ has degree at least n by part (a). Thus, $g(x)$ cannot be an inverse of $f(x)$ in $D[x]$.

55. Find an multiplicative inverse of $2x + 1$ in $\mathbb{Z}_4[x]$, AND prove that the inverse is unique.

Solution. Suppose $f(x) = 2x + 1$. Then $f(x)f(x) = 4x^2 + 4x + 1 = 1 \in \mathbb{Z}_4[x]$. Thus, $f(x)$ is the inverse of itself. Suppose $g(x) = b_0 + \cdots + b_m x^m$ satisfies

$$1 = f(x)g(x) = (b_0 + \cdots + b_m x^m) + 2x(b_0 + \cdots + b_m x^m).$$

Then $b_0 = 1$, $2b_m = 0$, and $b_i + 2b_{i-1} = 0$ for $i = m, \ldots, 1$. We have $b_0 = 1$, $b_1 = 2$, and $b_i = 0$ for $i = 2, \ldots, m$. Thus, $g(x) = f(x)$.

56. Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$. Suppose $f(x)$ and $g(x)$ has degrees less than $p(x)$. Then

$$f(x) + \langle p(x) \rangle \neq g(x) + \langle p(x) \rangle$$

if and only if $f(x) \neq g(x)$.

Solution. If $f(x) \neq g(x)$, then $f(x) - g(x)$ is nonzero and not a multiple of $p(x)$. So, $f(x) - g(x) \notin \langle p(x) \rangle$. Thus, $f(x) + \langle p(x) \rangle \neq g(x) + \langle p(x) \rangle$.

The converse is clear.