Contents

Introduction

This edition is an improvement of the first edition. In this edition, I corrected some of the errors that appeared in the first edition. I added the following sections that were not included in the first edition: Simple groups, Classification of finite Abelian groups, General question on Groups, Euclidean domains, Gaussian Ring $(\mathcal{Z}[i])$, Galois field and Cyclotomic fields, and General question on rings and fields. I hope that students who use this book will obtain a solid understanding of the basic concepts of abstract algebra through doing problems, the best way to understand this challenging subject. So often I have encountered students who memorize a theorem without the ability to apply that theorem to a given problem. Therefore, my goal is to provide students with an array of the most typical problems in basic abstract algebra. At the beginning of each chapter, I state many of the major results in Group and Ring Theory, followed by problems and solutions. I do not claim that the solutions in this book are the shortest or the easiest; instead each is based on certain well-known results in the field of abstract algebra. If you wish to comment on the contents of this book, please email your thoughts to abadawi@aus.edu

I dedicate this book to my father Rateb who died when I was 9 years old. I wish to express my appreciation to my wife Rawya, my son Nadeem, my friend Brian Russo, and Nova Science Inc. Publishers for their superb assistance in this book. It was a pleasure working with them.

Ayman Badawi

Chapter 1

Tools and Major Results of Groups

1.1 Notations

1. e indicates the identity of a group G.
2. e_H indicates the identity of a group H
3. Ord(a) indicates the order of a in a group.
4. gcd(n,m) indicates the greatest common divisor of n and m.
5. lcm(n,m) indicates the least common divisor of n and m.
6. $H \lhd G$ indicates that H is a normal subgroup of G.
7. $Z(G) = \{x \in G : xy = yx \text{ for each } y \in G\}$ indicates the center of a group G.
8. Let H be a subgroup of a group G. Then $C(H) = \{g \in G : gh = hg \text{ for each } h \in H\}$ indicates the centralizer of H in G.
9. Let a be an element in a group G. Then $C(a) = \{g \in G : ga = ag\}$ indicates the centralizer of a in G.
10. Let H be a subgroup of a group G. Then $N(H) = \{g \in G : g^{-1}Hg = H\}$ indicates the normalizer of H in G.
11. Let H be a subgroup of a group G. Then [G : H] = number of all distinct left(right) cosets of H in G.

12. C indicates the set of all complex numbers.
13. Z indicates the set of all integers.
14. $Z_n = \{m : 0 \leq m < n\}$ indicates the set of integers module n
15. Q indicates the set of all rational numbers.
16. $U(n) = \{a \in Z_n : gcd(a, n) = 1\}$ indicates the unit group of Z_n under multiplication module n.
17. If G is a group and $a \in G$, then (a) indicates the cyclic subgroup of G generated by a.
18. If G is a group and $a_1, a_2, ..., a_n \in G$, then $(a_1, a_2, ..., a_n)$ indicates the subgroup of G generated by $a_1, a_2, ..., a_n$.
19. $GL(m, Z_n)$ indicates the group of all invertible $m \times m$ matrices with entries from Z_n under matrix-multiplication
20. If A is a square matrix, then det(A) indicates the determinant of A.
21. $Aut(G)$ indicates the set of all isomorphisms (automorphisms) from G onto G.
22. S_n indicates the group of all permutations on a finite set with n elements.
23. $A \cong B$ indicates that A is isomorphic to B.
24. $a \in A \setminus B$ indicates that a is an element of A but not an element of B.
25. $a \mid b$ indicates that a divides b.

1.2 Results

THEOREM 1.2.1 *Let a be an element in a group G. If* $a^m = e$ *, then Ord(a) divides m.*

THEOREM 1.2.2 *Let p be a prime number and n, m be positive integers such that p divides nm. Then either p divides n or p divides m.*

THEOREM 1.2.3 *Let n, m be positive integers. Then gcd(n,m) = 1 if and only if am +bm = 1 for some integers a and b.*

THEOREM 1.2.4 *Let n and m be positive integers. If a = n/gcd(n,m) and b = m/gcd(n,m), then gcd(a,b) = 1.*

THEOREM 1.2.5 *Let n, m, and c be positive integers. If gcd(c,m) = 1 and c divides nm, then c divides n.*

THEOREM 1.2.6 *Let n and m and c be positive integers such that gcd(n,m) =1. If n divides c and m divides c, then nm divides c.*

THEOREM 1.2.7 *Let H be a subset of a group G. Then H is a subgroup of G if and only if $a^{-1}b \in H$ for every a and $b \in H$.*

THEOREM 1.2.8 *Let H be a finite set of a group G. Then H is a subgroup of G if and only if H is closed.*

THEOREM 1.2.9 *Let a be an element of a group G. If a has an infinite order, then all distinct powers of a are distinct elements. If a has finite order, say, n, then the cyclic group $(a) = \{e, a, a^2, a^3, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.*

THEOREM 1.2.10 *Every subgroup of a cyclic group is cyclic.*

THEOREM 1.2.11 *If G = (a), a cyclic group generated by a, and Ord(G) = n, then the order of any subgroup of G is a divisor of n.*

THEOREM 1.2.12 *Let G = (a) such that Ord(G) = n. Then for each positive integer k divides n, the group G = (a) has exactly one subgroup of order k namely $(a^{n/k})$.*

THEOREM 1.2.13 *Let $n = P_1^{\alpha_1}...P_k^{\alpha_k}$, where the P_i's are distinct prime numbers and each α_i is a positive integer ≥ 1. Then $\phi(n) = (P_1 - 1)P_1^{\alpha_1 - 1}...(P_k - 1)P_k^{\alpha_k - 1}$, where $\phi(n)$ = number of all positive integers less than N and relatively prime to n.*

THEOREM 1.2.14 *Let G be a cyclic group of order n, and let d be a divisor of n. Then number of elements of G of order d is $\phi(d)$. In particular, number of elements of G of order n is $\phi(n)$.*

THEOREM 1.2.15 *Z is a cyclic group and each subgroup of Z is of the form nZ for some $n \in Z$.*

THEOREM 1.2.16 *Z_n is a cyclic group and if k is a positive divisor of n, then (n/k) is the unique subgroup of Z_n of order k.*

THEOREM 1.2.17 *Let n be a positive integer, and write $n = P_1^{\alpha_1} P_2^{\alpha_2} ... P_k^{\alpha_k}$ where the P_i's are distinct prime numbers and each α_i is a positive integer ≥ 1. Then number of all positive divisors of n (including 1 and n) is $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$.*

THEOREM 1.2.18 *Let n, m, k be positive integers. Then lcm(n,m) =nm/gcd(n,m). If n divides k and m divides k, then lcm(n,m) divides k.*

THEOREM 1.2.19 *Let $\alpha = (a_1, a_2, ..., a_n)$ and $\beta = (b_1, b_2, ..., b_m)$ be two cycles. If α and β have no common entries, then $\alpha\beta = \beta\alpha$.*

THEOREM 1.2.20 *Let α be a permutation of a finite set. Then α can be written as disjoint cycles and $Ord(\alpha)$ is the least common multiple of the lengths of the disjoint cycles.*

THEOREM 1.2.21 *Every permutation in $S_n (n > 1)$ is a product of 2-cycles.*

THEOREM 1.2.22 *Let α be a permutation. If $\alpha = B_1 B_2 ... B_n$ and $\alpha = A_1 A_2 ... A_m$, where the B_i's and the A_i's are 2-cycles, then m and n are both even or both odd.*

THEOREM 1.2.23 *Let $\alpha = (a_1, a_2, ..., a_n) \in S_m$. Then $\alpha = (a_1, a_n)$ $(a_1, a_{n-1})(a_1, a_{n-2})...(a_1, a_2)$.*

THEOREM 1.2.24 *The set of even permutations A_n is a subgroup of S_n.*

THEOREM 1.2.25 *Let $\alpha = (a_1, a_2, ..., a_n) \in S_m$. Then $\alpha^{-1} = (a_n, a_{n-1}, ..., a_2, a_1)$.*

THEOREM 1.2.26 *Let H be a subgroup of G, and let $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$. In particular, if $gH = H$ for some $g \in G$, then $g \in H$*

THEOREM 1.2.27 *Let G be a finite group and let H be a subgroup of G. Then Ord(H) divides Ord(G).*

THEOREM 1.2.28 *Let G be a finite group and let H be a subgroup of G. Then the number of distinct left(right) cosets of H in G is Ord(G)/Ord(H).*

THEOREM 1.2.29 *Let G be a finite group and $a \in G$. Then $Ord(a)$ divides $Ord(G)$.*

THEOREM 1.2.30 *Let G be a group of order n, and let $a \in G$. Then $a^n = e$.*

THEOREM 1.2.31 *Let G be a finite group, and let p be a prime number such that p divides $Ord(G)$. Then G contains an element of order p.*

THEOREM 1.2.32 *Let H be a subgroup of a group G. Then H is normal if and only if $gHg^{-1} = H$ for each $g \in G$.*

THEOREM 1.2.33 *Let H be a normal subgroup of G. Then $G/H = \{gH : g \in G\}$ is a group under the operation $aHbH = abH$. Furthermore, If $[G : H]$ is finite, then $Ord(G/H) = [G : H]$.*

THEOREM 1.2.34 *Let Φ be a group homomorphism from a group G to a group H and let $g \in G$ and D be a subgroup of G. Then :*

1. *Φ carries the identity of G to the identity of H.*
2. *$\Phi(g^n) = (\Phi(g))^n$.*
3. *$\Phi(D)$ is a subgroup of H.*
4. *If D is normal in G, then $\Phi(D)$ is normal in $\Phi(H)$.*
5. *If D is Abelian, then $\Phi(D)$ is Abelian.*
6. *If D is cyclic, then $\Phi(D)$ is cyclic. In particular, if G is cyclic and D is normal in G, then G/D is cyclic.*

THEOREM 1.2.35 *Let Φ be a group homomorphism from a group G to a group H. Then $Ker(\Phi)$ is a normal subgroup of G and $G/Ker(\Phi) \cong \Phi(G)$ (the image of G under Φ).*

THEOREM 1.2.36 *Suppose that $H_1, H_2, ..., H_n$ are finite groups. Let $D = H_1 \oplus H_2 ... \oplus H_n$. Then D is cyclic if and only if each H_i is cyclic and if $i \neq j$, then $gcd(Ord(H_i), Ord(H_j) = 1$.*

THEOREM 1.2.37 *Let $H_1, ..., H_n$ be finite groups, and let $d = (h_1, h_2, ..., h_n) \in D = H_1 \oplus H_2 ... \oplus H_n$. Then $Ord(d) = Ord((h_1, h_2, ..., h_n)) = lcm(Ord(h_1), Ord(h_2), ..., Ord(h_n))$.*

THEOREM 1.2.38 *Let $n = m_1m_2...m_k$ where $gcd(m_i, m_j) = 1$ for $i \neq j$. Then $U(n) = U(m_1) \oplus U(m_2)... \oplus U(m_k)$.*

THEOREM 1.2.39 *Let H, K be normal subgroups of a group G such that $H \cap K = \{e\}$ and $G = HK$. Then $G \cong H \oplus K$.*

THEOREM 1.2.40 *Let p be a prime number. Then $U(p) \cong Z_{p-1}$ is a cyclic group. Furthermore, if p is an odd prime, then $U(p^n) \cong Z_{\phi(p^n)} = Z_{p^n-p^{n-1}} = Z_{(p-1)p^{n-1}}$ is a cyclic group. Furthermore, $U(2^n) \cong Z_2 \oplus Z_{2^{n-2}}$ is not cyclic for every $n \geq 3$.*

THEOREM 1.2.41 *$Aut(Z_n) \cong U(n)$.*

THEOREM 1.2.42 *Every group of order n is isomorphic to a subgroup of S_n.*

THEOREM 1.2.43 *Let G be a finite group and let p be a prime. If p^k divides $Ord(G)$, then G has a subgroup of order p^k.*

THEOREM 1.2.44 *If H is a subgroup of a finite group G such that $Ord(H)$ is a power of prime p, then H is contained in some Sylow p-subgroup of G.*

THEOREM 1.2.45 *Let n be the number of all Sylow p-subgroups of a finite group G. Then n divides $Ord(G)$ and p divides $(n-1)$.*

THEOREM 1.2.46 *A Sylow p-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p-subgroup of G.*

THEOREM 1.2.47 *Suppose that G is a group of order p^n for some prime number p and for some $n \geq 1$. Then $Ord(Z(G)) = p^k$ for some $0 < k \leq n$.*

THEOREM 1.2.48 *Let H and K be finite subgroups of a group G. Then $Ord(HK) = Ord(H)Ord(K)/Ord(H \cap K)$.*

THEOREM 1.2.49 *Let G be a finite group. Then any two Sylow-p-subgroups of G are conjugate, i.e., if H and K are Sylow-p-subgroups, then $H = g^{-1}Kg$ for some $g \in G$.*

THEOREM 1.2.50 *Let G be a finite group, H be a normal subgroup of G, and let K be a Sylow p-subgroup of H. Then $G = HN_G(K)$ and $[G : H]$ divides $Ord(N_G(K))$, where $N_G(K) = \{g \in G : g^{-1}Kg = K\}$ (the normalizer of K in G).*

THEOREM 1.2.51 *Let G be a finite group, n_p be the number of Sylow-p-subgroups of G, and suppose that p^2 does not divide $n_p - 1$. Then there are two distinct Sylow-p-subgroups K and H of G such that $[K : H \cap K] = [H : H \cap K] = p$. Furthermore, $H \cap K$ is normal in both K and H, and thus $HK \subset N(H \cap K)$ and $Ord(N(H \cap K)) > Ord(HK) = Ord(H)ORD(K)/Ord(H \cap K)$.*

THEOREM 1.2.52 *Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the factorization is unique except for rearrangement of the factors.*

THEOREM 1.2.53 *Let G be a finite Abelian group of order n. Then for each positive divisor k of n, there is a subgroup of G of order k.*

THEOREM 1.2.54 *We say a is a conjugate of b in a group G if $g^{-1}bg = a$ for some $g \in G$. The conjugacy class of a is denoted by $CL(a) = \{b \in G : g^{-1}ag = b \text{ for some } g \in G\}$. Recall that $C(a) = \{g \in G : ga = ag\}$ is a subgroup of G and $C(a)$ is called the centralizer of a in G. Also, we say that two subgroups H, K of a group G are conjugate if $H = g^{-1}Kg$ for some $g \in G$. The conjugacy class of a subgroup H of a group G is denoted by $CL(H) = \{g^{-1}Hg : g \in G\}$. Let G be a finite group, $a \in G$, and let H be a subgroup of G. Then $Ord(CL(a)) = [G : C(a)] = Ord(G)/Ord(C(a))$ and $Ord(CL(H)) = [G : N(H)]$, where $N(H) = \{g \in G : g^{-1}Hg = H\}$ the normalizer of H in G.*

We say that a group is simple if its only normal subgroups are the identity subgroup and the group itself.

THEOREM 1.2.55 *If $Ord(G) = 2n$, where n is an odd number greater than 1, then G is not a simple group.*

THEOREM 1.2.56 *Let H be a subgroup of a finite group G and let $n = [G : H]$ (the index of H in G). Then there is a group homomorphism, say Φ, from G into S_n (recall that S_n is the group of all permutations on a set with n elements) such that $Ker(\Phi)$ is contained in H. Moreover, if K is a normal subgroup of G and K is contained in H, then K is contained in $Ker(\Phi)$.*

THEOREM 1.2.57 *Let H be a proper subgroup of a finite non-Abelian simple group G and let $n = [G : H]$ (the index of H in G). Then G is isomorphic to a subgroup of A_n.*

THEOREM 1.2.58 *For each $n \geq 5$, A_n (the subgroup of all even permutation of S_n) is a simple group.*

THEOREM 1.2.59 *Let G be a group of order p^n, where $n \geq 1$ and p is prime number. Then if H is a normal subgroup of G and $Ord(H) \geq p$, then $Ord(H \cap Z(G)) \geq p$, i.e., $H \cap Z(G) \neq \{e\}$. In particular, every normal subgroup of G of order p is contained in $Z(G)$ (the center of G).*

Chapter 2

Problems in Group Theory

2.1 Elementary Properties of Groups

QUESTION 2.1.1 *For any elements a, b in a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^na$.*

Solution: The claim is clear for n = 0. We assume $n \geq 1$. We use math. induction. The result is clear for n = 1. Hence, assume it is true for $n \geq 1$. We prove it for n+1. Now, $(a^{-1}ba)^{n+1} = (a^{-1}ba)^n(a^{-1}ba) = (a^{-1}b^na)(a^{-1}ba) = a^{-1}b^n(aa^{-1})ba = a^{-1}b^{n+1}a$, since aa^{-1} is the identity in the group. Now, we assume $n \leq -1$. Since $-n \geq 1$, we have $(a^{-1}ba)^n = [(a^{-1}ba)^{-1}]^{-n} = (a^{-1}b^{-1}a)^{-n} = a^{-1}(b^{-1})^{-n}a = a^{-1}b^na$. (We assume that the reader is aware of the fact that $(b^{-1})^{-n} = (b^{-n})^{-1} = b^n$.)

QUESTION 2.1.2 *Let a and b be elements in a finite group G. Prove that Ord(ab) = Ord(ba).*

Solution: Let n = Ord(ab) and m = Ord(ba). Now, by the previous Question, $(ba)^n = (a^{-1}(ab)a)^n = a^{-1}(ab)^na = e$. Thus, m divides n by Theorem 1.2.1. Also, $(ab)^m = (b^{-1}(ba)b)^m = b^{-1}(ba)^mb = e$. Thus, n divides m. Since n divides m and m divides n, we have n = m.

QUESTION 2.1.3 *Let g and x be elements in a group. Prove that $Ord(x^{-1}gx) = Ord(g)$.*

Solution: Let $a = x^{-1}g$ and $b = x$. By the previous Question, Ord(ab) = Ord(ba). But ba = g. Hence, $Ord(x^{-1}gx) = Ord(g)$.

QUESTION 2.1.4 *Suppose that a is the only element of order 2 in a group G. Prove that $a \in Z(G)$*

Solution: Deny. Then $xa \neq ax$ for some $x \in G$. Hence,$x^{-1}ax \neq a$. Hence, by the previous question we have $Ord(x^{-1}ax) = Ord(a) = 2$,a contradiction, since a is the only element of order 2 in G. Thus, our denial is invalid. Hence, $a \in Z(G)$.

QUESTION 2.1.5 *In a group, prove that* $(a^{-1})^{-1} = a$.

Solution: Since $aa^{-1} = e$, we have$(aa^{-1})^{-1} = e$. But we know that $(aa^{-1})^{-1} = (a^{-1})^{-1}a^{-1}$. Hence,$(a^{-1})^{-1}a^{-1} = e$. Also by a similar argument as before, since $a^{-1}a = e$, we conclude that $a^{-1}(a^{-1})^{-1} = e$. Since the inverse of a^{-1} is unique, we conclude that $(a^{-1})^{-1} = a$.

QUESTION 2.1.6 *Prove that if* $(ab)^2 = a^2b^2$, *then* $ab = ba$.

Solution: $(ab)^2 = abab = a^2b^2$. Hence, $a^{-1}(abab)b^{-1} = a^{-1}(a^2b^2)b^{-1}$. Thus, $(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1})$. Since $a^{-1}a = bb^{-1} = e$, we have ba = ab.

QUESTION 2.1.7 *Let a be an element in a group. Prove that Ord(a)=* $Ord(a^{-1})$.

Solution: Suppose that Ord(a) = n and $Ord(a^{-1}) = m$. We may assume that $m < n$. Hence, $a^n(a^{-1})^m = a^n a^{-m} = a^{n-m} = e$. Thus, by Theorem 1.2.1 Ord(a) = n divides n - m,which is impossible since $n - m < n$.

QUESTION 2.1.8 *Let a be a non identity element in a group G such that Ord(a) = p is a prime number. Prove that* $Ord(a^i) = p$ *for each* $1 \leq i < p$.

Solution: Let $1 \leq i < p$. Since Ord(a) = p, $(a^i)^p = a^{pi} = e$ the identity in G. Hence, we may assume that $Ord(a^i) = m < p$. Thus, $(a^i)^m = a^{im} = e$. Thus, by Theorem 1.1 Ord(a) = p divides im. Thus, by Theorem 1.2.2 either p divides i or p divides m. Since $i < p$ and $m < p$, neither p divides i nor p divides m. Hence, $Ord(a^i) = m = p$.

QUESTION 2.1.9 *Let G be a finite group. Prove that number of elements x of G such that* $x^7 = e$ *is odd.*

Solution: Let x be a non identity element of G such that $x^7 = e$. Since 7 is a prime number and $x \neq e$, Ord(x) = 7 by Theorem 1.2.1. Now, By the previous question $(x^i)^7 = e$ for each $1 \leq i \leq 6$. Thus, number of non identity elements x of G such that $x^7 = e$ is 6n for some positive integer n. Also, Since $e^7 = e$, number of elements x of G such that $x^7 = e$ is $6n + 1$ which is an odd number.

QUESTION 2.1.10 *Let a be an element in a group G such that $a^n = e$ for some positive integer n. If m is a positive integer such that gcd(n,m) = 1, then prove that $a = b^m$ for some b in G.*

Solution: Since gcd(n,m) = 1, cn + dm = 1 for some integers c and d by Theorem 1.2.3. Hence, $a = a^1 = a^{cn+dm} = a^{cn}a^{dm}$. Since $a^n = e$, $a^{cn} = e$. Hence, $a = a^{dm}$. Thus, let $b = a^d$. Hence, $a = b^m$.

QUESTION 2.1.11 *Let G be a group such that $a^2 = e$ for each $a \in G$. Prove that G is Abelian.*

Solution: Since $a^2 = e$ for each a in G, $a = a^{-1}$ for each a in G. Now, let a and b be elements in G. Then $(ab)^2 = abab = e$. Hence, (abab)ba = ba. But (abab)ba = aba(bb)a= aba(e)a = ab(aa) = ab(e) = ab. Thus, ab = ba.

QUESTION 2.1.12 *Let a be an element in a group such that Ord(a) = n. If i is a positive integer, then prove that $Ord(a^i) = n/gcd(n, i)$.*

Solution: Let k = n/gcd(n,i) and let $m = Ord(a^i)$. Then $(a^i)^k = (a^n)^{i/gcd(n,i)} = e$ since $a^n = e$. Since $(a^i)^k = e$, m divides k by Theorem 1.2.1. Also, since $Ord(a^i) = m$, we have $(a^i)^m = a^{im} = e$. Hence, n divides im (again by Theorem 1.2.1). Since n =[n/gcd(i,n)]gcd(i,n) divides im = m[i/gcd(i,n)]gcd(i,n), we have k = n/gcd(n,i) divides m[i/gcd(i,n)]. Since gcd(k, i/gcd(n,i)) = 1 by Theorem 1.2.4 and k divides m[i/gcd(i,n)], we have k divides m by Theorem 1.2.5. Since m divides k and k divides m, m = k. Hence, $Ord(a^i) = k = n/gcd(i, n)$.

QUESTION 2.1.13 *Let a be an element in a group such that Ord(a) = 20. Find $Ord(a^6)$ and $Ord(a^{13})$.*

Solution: By the previous problem, $Ord(a^6) = 20/gcd(6, 20) = 20/2 = 10$. Also, $Ord(a^{13}) = 20/gcd(13, 20) = 20/1 = 20$.

QUESTION 2.1.14 *Let a and b be elements in a group such that ab = ba and Ord(a) = n and Ord(b) = m and gcd(n,m) = 1. Prove that Ord(ab) = lcm(n,m) = nm.*

Solution: Let c = Ord(ab). Since ab = ba, we have $(ab)^{nm} = a^{nm}b^{nm} = e$. Hence, c divides nm by Theorem 1.2.1. Since c = Ord(ab) and ab=ba, we have $(ab)^{nc} = a^{nc}b^{nc} = (ab^c)^n = e$. Hence, since $a^{nc} = e$, we have

$b^{nc} = e$. Thus, m divides nc since m = Ord(b). Since gcd(n,m) = 1, we have m divides c by Theorem 1.2.5. Also, we have $(ab)^{mc} = a^{mc}b^{mc} = (ab^c)^m = e$. Since $b^{mc} = e$, we have $a^{mc} = e$. Hence, n divides mc. Once again, since gcd(n,m) =1, we have n divides c. Since n divides c and m divides c and gcd(n,m) = 1, we have nm divides c by Theorem 1.2.6. Since c divides nm and nm divides c, we have nm = c = Ord(ab).

QUESTION 2.1.15 *In view of the previous problem, find two elements a and b in a group such that ab = ba and Ord(a) = n and Ord(b) = m but* $Ord(ab) \neq lcm(n, m)$.

Solution: Let a be a non identity element in a group and let $b = a^{-1}$. Then $Ord(a) = Ord(a^{-1}) = n > 1$ by Question 2.1.7 and ab = ba. But $Ord(ab) = Ord(e) = 1 \neq lcm(n, n) = n$.

QUESTION 2.1.16 *Let x and y be elements in a group G such that* $xy \in Z(G)$. *Prove that xy = yx.*

Solution: Since $xy = x^{-1}x(xy)$ and $xy \in Z(G)$, we have $xy = x^{-1}x(xy) = x^{-1}(xy)x = (x^{-1}x)yx = yx$.

QUESTION 2.1.17 *Let G be a group with exactly 4 elements. Prove that G is Abelian.*

Solution: Let a and b be non identity elements of G. Then e, a, b,ab,and ba are elements of G. Since G has exactly 4 elements, ab = ba. Thus, G is Abelian.

QUESTION 2.1.18 *Let G be a group such that each non identity element of G has prime order. If* $Z(G) \neq \{e\}$, *then prove that every non identity element of G has the same order.*

Solution: Let $a \in Z(G)$ such that $a \neq e$. Assume there is an element $b \in G$ such that $b \neq e$ and $Ord(a) \neq Ord(b)$. Let n = Ord(a) and m = Ord(b). Since n, m are prime numbers, gcd(n,m) = 1. Since $a \in Z(G)$, ab = ba. Hence, Ord(ab) = nm by Question 2.1.14. A contradiction since nm is not prime. Thus, every non identity element of G has the same order.

QUESTION 2.1.19 *Let a be an element in a group. Prove that* $(a^n)^{-1} = (a^{-1})^n$ *for each* $n \geq 1$.

Solution: We use Math. induction on n. For $n = 1$, the claim is clearly valid. Hence, assume that $(a^n)^{-1} = (a^{-1})^n$. Now, we need to prove the claim for $n + 1$. Thus, $(a^{n+1})^{-1} = (aa^n)^{-1} = (a^n)^{-1}a^{-1} = (a^{-1})^n a^{-1} = (a^{-1})^{n+1}$.

QUESTION 2.1.20 *Let $g \in G$, where G is a group. Suppose that $g^n = e$ for some positive integer n. Show that $Ord(g)$ divides n.*

Solution : Let $m = Ord(g)$. It is clear that $m \leq n$. Hence $n = mq + r$ for some integers q, r where $0 \leq r < m$. Since $g^n = e$, we have $e = g^n = g^{mq+r} = g^{mq}g^r = eg^r = g^r$. Since $g^r = e$ and $r < Ord(g) = m$, we conclude that $r = 0$. Thus $m = Ord(g)$ divides n.

2.2 Subgroups

QUESTION 2.2.1 *Let H and D be two subgroups of a group such that neither $H \subset D$ nor $D \subset H$. Prove that $H \cup D$ is never a group.*

Solution: Deny. Let $a \in H \setminus D$ and let $b \in D \setminus H$. Hence, $ab \in H$ or $ab \in D$. Suppose that $ab = h \in H$. Then $b = a^{-1}h \in H$, a contradiction. In a similar argument, if $ab \in D$, then we will reach a contradiction. Thus, $ab \notin H \cup D$. Hence, our denial is invalid. Therefore, $H \cup D$ is never a group.

QUESTION 2.2.2 *Give an example of a subset of a group that satisfies all group-axioms except closure.*

Solution: Let H = 3Z and D = 5Z. Then H and D are subgroups of Z. Now, let $C = H \cup D$. Then by the previous question, C is never a group since it is not closed.

QUESTION 2.2.3 *Let H and D be subgroups of a group G. Prove that $C = H \cap D$ is a subgroup of G.*

Solution: Let a and b be elements in C. Since $a \in H$ and $a \in D$ and the inverse of a is unique and H, D are subgroups of G, $a^{-1} \in H$ and $a^{-1} \in D$. Now, Since $a^{-1} \in C$ and $b \in C$ and H, D are subgroups of G, $a^{-1}b \in H$ and $a^{-1}b \in D$. Thus, $a^{-1}b \in C$. Hence, C is a subgroup of G by Theorem 1.2.7.

QUESTION 2.2.4 *Let $H = \{a \in Q : a = 3^n 8^m$ for some n and m in $Z\}$. Prove that H under multiplication is a subgroup of $Q \setminus \{0\}$.*

Solution: Let $a, b \in H$. Then $a = 3^{n_1}8^{n_2}$ and $b = 3^{m_1}8^{m_2}$ for some $n_1, n_2, m_1, m_2 \in Z$. Now, $a^{-1}b = 3^{m_1-n_1}8^{m_2-n_2} \in H$. Thus, H is a subgroup of $Q \setminus \{0\}$ by Theorem 1.2.7.

QUESTION 2.2.5 *Let D be the set of all elements of finite order in an Abelian group G. Prove that D is a subgroup of G.*

Solution: Let a and b be elements in D, and let n = Ord(a) and m = Ord(b). Then $Ord(a^{-1}) = n$ by Question 2.1.7. Since G is Abelian, $(a^{-1}b)^{nm} = (a^{-1})^{nm}b^{nm} = e$. Thus, $Ord(a^{-1}b)$ is a finite number (in fact $Ord(a^{-1}b)$ divides nm). Hence, $a^{-1}b \in D$. Thus, D is a subgroup of G by Theorem 1.2.7.

QUESTION 2.2.6 *Let a, x be elements in a group G. Prove that $ax = xa$ if and only if $a^{-1}x = xa^{-1}$.*

Solution: Suppose that ax = xa. Then $a^{-1}x = a^{-1}xaa^{-1} = a^{-1}axa^{-1} = exa^{-1} = xa^{-1}$. Conversely, suppose that $a^{-1}x = xa^{-1}$. Then $ax = axa^{-1}a = aa^{-1}xa = exa = xa$.

QUESTION 2.2.7 *Let G be a group. Prove that Z(G) is a subgroup of G.*

Solution: Let $a, b \in Z(G)$ and $x \in G$. Since ax = xa, we have $a^{-1}x = xa^{-1}$ by the previous Question. Hence, $a^{-1}bx = a^{-1}xb = xa^{-1}b$. Thus, $a^{-1}b \in Z(G)$. Thus, Z(G) is a subgroup of G by Theorem 1.2.7.

QUESTION 2.2.8 *Let a be an element of a group G. Prove that C(a) is a subgroup of G.*

Solution: Let $x, y \in C(a)$. Since ax = xa, we have $x^{-1}a = ax^{-1}$ by Question 2.2.6. Hence, $x^{-1}ya = x^{-1}ay = ax^{-1}y$. Thus, $x^{-1}y \in C(a)$. Hence, C(a) is a subgroup of G by Theorem 1.2.7.

Using a similar argument as in Questions 2.2.7 and 2.2.8, one can prove the following:

QUESTION 2.2.9 *Let H be a subgroup of a group G. Prove that N(H) is a subgroup of G.*

QUESTION 2.2.10 *Let $H = \{x \in C : x^{301} = 1\}$. Prove that H is a subgroup of $C \setminus \{0\}$ under multiplication.*

Solution: First, observe that H is a finite set with exactly 301 elements. Let $a, b \in H$. Then $(ab)^{301} = a^{301}b^{301} = 1$. Hence, $ab \in H$. Thus, H is closed. Hence, H is a subgroup of $C \setminus \{0\}$ by Theorem 1.2.8.

QUESTION 2.2.11 *Let $H = \{A \in GL(608, Z_{89}) : det(A) = 1\}$. Prove that H is a subgroup of $GL(608, Z_{89})$.*

Solution: First observe that H is a finite set. Let $C, D \in H$. Then $det(CD) = det(C)det(D) = 1$. Thus, $CD \in H$. Hence, H is closed. Thus, H is a subgroup of $GL(608, Z_{89})$ by Theorem 1.2.8.

QUESTION 2.2.12 *Suppose G is a group that has exactly 36 distinct elements of order 7. How many distinct subgroups of order 7 does G have?*

Solution: Let $x \in G$ such that Ord(x) = 7. Then, $H = \{e, x, x^2, ..., x^6\}$ is a subgroup of G and Ord(H) = 7. Now, by Question 2.1.8, $Ord(x^i) = 7$ for each $1 \leq i \leq 6$. Hence, each subgroup of G of order 7 contains exactly 6 distinct elements of order 7. Since G has exactly 36 elements of order 7, number of subgroups of G of order 7 is $36/6 = 6$.

QUESTION 2.2.13 *Let $H = \{x \in U(40) : 5 \mid x - 1\}$. Prove that H is a subgroup of U(40).*

Solution: Observe that H is a finite set. Let $x, y \in H$. $xy - 1 = xy - y + y - 1 = y(x - 1) + y - 1$. Since 5 divides $x - 1$ and 5 divides $y - 1$, we have 5 divides $y(x-1)+y-1 = xy-1$. Thus, $xy \in H$. Hence, H is closed. Thus, H is a subgroup of G by Theorem 1.2.8

QUESTION 2.2.14 *Let G be an Abelian group, and let $H = \{a \in G : Ord(a) \mid 26\}$. Prove that H is a subgroup of G.*

Solution: Let $a, b \in H$. Since $a^{26} = e$, Ord(a) divides 26 by Theorem 1.2.1. Since $Ord(a) = Ord(a^{-1})$ and Ord(a) divides 26, $Ord(a^{-1})$ divides 26. Thus, $(a^{-1})^{26} = e$. Hence, $(a^{-1}b)^{26} = (a^{-1})^{26}b^{26} = e$. Thus, H is a subgroup of G by Theorem 1.2.7.

QUESTION 2.2.15 *Let G be an Abelian group, and let $H = \{a \in G : Ord(a) = 1$ or $Ord(a) = 13\}$. Prove that H is a subgroup of G.*

Solution: Let $a, b \in H$.If a = e or b = e, then it is clear that $(a^{-1}b) \in H$. Hence, assume that neither a = e nor b = e. Hence, Ord(a) = Ord(b) = 13. Thus, $Ord(a^{-1}) = 13$. Hence, $(a^{-1}b)^{13} = (a^{-1})^{13}b^{13} = e$. Thus, $Ord(a^{-1}b)$ divides 13 by Theorem 1.2.1. Since 13 is prime, 1 and 13 are the only divisors of 13. Thus, $Ord(a^{-1}b)$ is either 1 or 13. Thus, $a^{-1}b \in H$. Thus, H is a subgroup of G by Theorem 1.2.7.

2.3 Cyclic Groups

QUESTION 2.3.1 *Find all generators of Z_{22}.*

Solution: Since $Ord(Z_{22}) = 22$, if a is a generator of Z_{22}, then Ord(a) must equal to 22. Now, let b be a generator of Z_{22}, then b = $1^b = b$. Since $Ord(1) = 22$, we have Ord(b) = $Ord(1^b) = 22/gcd(b, 22) = 22$ by Question 2.1.12. Hence, b is a generator of Z_{22} iff gcd(b,22) = 1. Thus, 1,3,5,7,9,11,13,15,17,19,21 are all generators of Z_{22}.

QUESTION 2.3.2 *Let G = (a), a cyclic group generated by a, such that Ord(a) = 16. List all generators for the subgroup of order 8.*

Solution: Let H be the subgroup of G of order 8. Then $H = (a^2) = (a^{16/8})$ is the unique subgroup of G of order 8 by Theorem 1.2.12. Hence, $(a^2)^k$ is a generator of H iff gcd(k,8) = 1. Thus, $(a^2)^1 = a^2, (a^2)^3 = a^6, (a^2)^5 = a^{10}, (a^2)^7 = a^{14}$.

QUESTION 2.3.3 *Suppose that G is a cyclic group such that Ord(G) = 48. How many subgroups does G have?*

Solution: Since for each positive divisor k of 48 there is a unique subgroup of order k by Theorem 1.2.12, number of all subgroups of G equals to the number of all positive divisors of 48. Hence, Write $48 = 3^1 2^3$. Hence, number of all positive divisors of 48 = (1+1)(3+1) = 8 by Theorem 1.2.17. If we do not count G as a subgroup of itself, then number of all proper subgroups of G is $8 - 1 = 7$.

QUESTION 2.3.4 *Let a be an element in a group,and let i, k be positive integers. Prove that $H = (a^i) \cap (a^k)$ is a cyclic subgroup of (a) and $H = (a^{lcm(i,k)})$.*

Solution: Since (a) is cyclic and H is a subgroup of (a), H is cyclic by Theorem 1.2.10. By Theorem 1.2.18 we know that lcm(i,k) = ik/gcd(i,k).

Since k/gcd(i,k) is an integer, we have $a^{lcm(i,k)} = (a^i)^{k/gcd(i,k)}$. Thus, $(a^{lcm(i,k)}) \subset (a^i)$. Also, since $k/gcd(i,k)$ is an integer, we have $a^{lcm(i,k)} = (a^k)^{i/gcd(i,k)}$. Thus, $(a^{lcm(i,k)}) \subset (a^k)$. Hence, $(a^{lcm(i,k)}) \subset H$. Now, let $h \in H$. Then $h = a^j = (a^i)^m = (a^k)^n$ for some $j, m, n \in Z$. Thus, i divides j and k divides j. Hence, lcm(i,k) divides j by Theorem 1.2.18. Thus, h = $a^j = (a^{lcm(i,k)})^c$ where j = lcm(i,k)c. Thus, $h \in (a^{lcm(i,k)})$. Hence, $H \subset (a^{lcm(i,k)})$. Thus, $H = (a^{lcm(i,k)})$.

QUESTION 2.3.5 *Let a be an element in a group. Describe the subgroup* $H = (a^{12}) \cap (a^{18})$.

Solution: By the previous Question, H is cyclic and $H = (a^{lcm(12,18)}) = (a^{36})$.

QUESTION 2.3.6 *Describe the Subgroup* $8Z \cap 12Z$.

Solution: Since $Z = (1)$ is cyclic and $8Z = (1^8) = (8)$ and $12Z = (1^{12}) = (12)$, $8Z \cap 12Z = (1^{lcm(8,12)}) = (lcm(8,12)) = 24Z$ by Question 2.3.4

QUESTION 2.3.7 *Let G be a group and* $a \in G$. *Prove* $(a) = (a^{-1})$.

Solution: Since $(a) = \{a^m : m \in Z\}$, $a^{-1} \in (a)$. Hence, $(a^{-1}) \subset (a)$. Also, since $(a^{-1}) = \{(a^{-1})^m : m \in Z\}$ and $(a^{-1})^{-1} = a$, $a \in (a^{-1})$. Hence, $(a) \subset (a^{-1})$. Thus, $(a) = (a^{-1})$.

QUESTION 2.3.8 *Let a be an element in a group such that a has infinite order. Prove that* $Ord(a^m)$ *is infinite for each* $m \in Z$.

Solution: Deny. Let $m \in Z$. Then, $Ord(a^m) = n$. Hence, $(a^m)^n) = a^{mn} = e$. Thus, $Ord(a)$ divides nm by Theorem 1.2.1. Hence, $Ord(a)$ is finite, a contradiction. Hence, Our denial is invalid. Therefore, $Ord(a^m)$ is infinite.

QUESTION 2.3.9 *Let* $G = (a)$, *and let H be the smallest subgroup of G that contains* a^m *and* a^n. *Prove that* $H = (a^{gcd(n,m)})$.

Solution: Since G is cyclic, H is cyclic by Theorem 1.2.10. Hence, $H = (a^k)$ for some positive integer k. Since $a^n \in H$ and $a^m \in H$, k divides both n and m. Hence, k divides gcd(n,m). Thus, $a^{gcd(n,m)} \in H = (a^k)$. Hence, $(a^{gcd(n,m)}) \subset H$. Also, since gcd(n,m) divides both n and m, $a^n \in (a^{gcd(n,m}$) and $a^m \in (a^{gcd(n,m)})$. Hence, Since H is the smallest subgroup of G containing a^n and a^m and $a^n, a^m \in (a^{gcd(n,m)}) \subset H$, we conclude that $H = (a^{gcd(n,m)})$.

QUESTION 2.3.10 *Let $G = (a)$. Find the smallest subgroup of G containing a^8 and a^{12}.*

Solution: By the previous Question, the smallest subgroup of G containing a^8 and a^{12} is $(a^{gcd(8,12)}) = (a^4)$.

QUESTION 2.3.11 *Find the smallest subgroup of Z containing 32 and 40.*

Solution: Since $Z = (1)$ is cyclic, once again by Question 2.3.4, the smallest subgroup of Z containing $1^{32} = 32$ and $1^{40} = 40$ is $(1^{gcd(32,40)}) = (8)$.

QUESTION 2.3.12 *Let $a \in G$ such that $Ord(a) = n$, and let $1 \leq k \leq n$. Prove that $Ord(a^k) = Ord(a^{n-k})$.*

Solution: Since $a^k a^{n-k} = a^n = e$, a^{n-k} is the inverse of a^k. Hence, $Ord(a^k) = Ord(a^{n-k})$.

QUESTION 2.3.13 *Let G be an infinite cyclic group. Prove that e is the only element in G of finite order.*

Solution: Since G is an infinite cyclic group, $G = (a)$ for some $a \in G$ such that Ord(a) is infinite. Now, assume that there is an element $b \in G$ such that Ord(b) = m and $b \neq e$. Since G = (a), $b = a^k$ for some $k \geq 1$. Hence, $e = b^m = (a^k)^m = a^{km}$. Hence, Ord(a) divides km by Theorem 1.2.1, a contradiction since Ord(a) is infinite. Thus, e is the only element in G of finite order.

QUESTION 2.3.14 *Let $G = (a)$ be a cyclic group. Suppose that G has a finite subgroup H such that $H \neq \{e\}$. Prove that G is a finite group.*

Solution: First, observe that H is cyclic by Theorem 1.2.10. Hence, $H = (a^n)$ for some positive integer n. Since H is finite and $H = (a^n)$, $Ord(a^n) = Ord(H) = m$ is finite. Thus, $(a^n)^m = a^{nm} = e$. Hence, Ord(a) divides nm by Theorem 1.2.1. Thus, (a) = G is a finite group.

QUESTION 2.3.15 *Let G be a group containing more than 12 elements of order 13. Prove that G is never cyclic.*

Solution: Deny. Then G is cyclic. Let $a \in G$ such that Ord(a) = 13. Hence, (a) is a finite subgroup of G. Thus, G must be finite by the previous Question. Hence, by Theorem 1.2.14 there is exactly $\phi(13) = 12$ elements in G of order 13. A contradiction. Hence, G is never cyclic.

QUESTION 2.3.16 *Let $G = (a)$ be an infinite cyclic group. Prove that a and a^{-1} are the only generators of G.*

solution: Deny. Then $G = (b)$ for some $b \in G$ such that neither $b = a$ nor $b = a^{-1}$. Since $b \in G = (a)$, $b = a^m$ for some $m \in Z$ such that neither $m = 1$ nor $m = -1$. Thus, $G = (b) = (a^m)$. Hence $a = b^k = (a^m)^k = a^{mk}$ for some $k \in Z$. Since a is of infinite order and $a = a^{mk}$, 1 = mk by Theorem 1.2.9, a contradiction since neither m = 1 nor m = -1 and mk = 1. Thus, our denial is invalid. Now, we show that $G = (a^{-1})$. Since G = (a), we need only to show that $a \in (a^{-1})$. But this is clear since $a = (a^{-1})^{-1}$ by Question 2.1.5.

QUESTION 2.3.17 *Find all generators of Z.*

Solution: Since $Z = (1)$ is an infinite cyclic group, 1 and -1 are the only generators of Z by the previous Question.

QUESTION 2.3.18 *Find an infinite group G such that G has a finite subgroup $H \neq e$.*

Solution: Let $G = C \setminus \{0\}$ under multiplication, and let $H = \{x \in G : x^4 = 1\}$. Then H is a finite subgroup of G of order 4.

QUESTION 2.3.19 *Give an example of a noncyclic Abelian group.*

Solution: Take $G = Q \setminus \{0\}$ under normal multiplication. It is easy to see that G is a noncyclic Abelian group.

QUESTION 2.3.20 *Let a be an element in a group G such that Ord(a) is infinite. Prove that $(a), (a^2), (a^3), ...$ are all distinct subgroups of G, and Hence, G has infinitely many proper subgroups.*

Solution: Deny. Hence, $(a^i) = (a^k)$ for some positive integers i, k such that $k > i$. Thus, $a^i = (a^k)^m$ for some $m \in Z$. Hence, $a^i = a^{km}$. Thus, $a^{i-km} = e$. Since $k > i$, $km \neq i$ and therefore $i - km \neq 0$. Thus, Ord(a) divides $i - km$ by Theorem 1.2.1. Hence, Ord(a) is finite, a contradiction.

QUESTION 2.3.21 *Let G be an infinite group. Prove that G has infinitely many proper subgroups.*

Solution:Deny. Then G has finitely many proper subgroups. Also, by the previous Question, each element of G is of finite order. Let $H_1, H_2, ..., H_n$ be all proper subgroups of finite order of G, and let $D = \cup_{i=1}^{n} H_i$. Since G is infinite, there is an element $b \in G \setminus D$. Since Ord(b) is finite and $b \in G \setminus D$, (b) is a proper subgroup of finite order of G and $(b) \neq H_i$ for each $1 \leq i \leq n$. A contradiction.

QUESTION 2.3.22 *Let a, b be elements of a group such that Ord(a) = n and Ord(b) = m and gcd(n,m) = 1. Prove that $H = (a) \cap (b) = \{e\}$.*

Solution: Let $c \in H$. Since (c) is a cyclic subgroup of (a), Ord(c) = Ord((c)) divides n. Also, since (c) is a cyclic subgroup of (b), Ord(c) = Ord((c)) divides m. Since gcd(n,m) and Ord(c) divides both n and m, we conclude Ord(c) = 1. Hence, c =e. Thus, $H = \{e\}$.

QUESTION 2.3.23 *Let a, b be two elements in a group G such that Ord(a) = 8 and Ord(b) = 27. Prove that $H = (a) \cap (b) = \{e\}$.*

Solution: Since gcd(8,27) = 1, by the previous Question H = $\{e\}$.

QUESTION 2.3.24 *Suppose that G is a cyclic group and 16 divides Ord(G). How many elements of order 16 does G have?*

Solution: Since 16 divides Ord(G), G is a finite group. Hence, by Theorem 1.2.14, number of elements of order 16 is $\phi(16) = 8$.

QUESTION 2.3.25 *Let a be an element of a group such that Ord(a) = n. Prove that for each $m \geq 1$, we have $(a^m) = (a^{gcd(n,m)})$*

Solution: First observe that $gcd(n, m) = gcd(n, (n, m))$. Since $Ord(a^m) = n/gcd(n, m)$ and $Ord(a^{gcd(n,m)}) = n/gcd(n, gcd(n, m)) = n/gcd(n, m)$ by Question 2.1.12 and (a) contains a unique subgroup of order n/gcd(n,m) by Theorem 1.2.12, we have $(a^m) = (a^{gcd(n,m)})$.

2.4 Permutation Groups

QUESTION 2.4.1 *Let $\alpha = (1, 3, 5, 6)(2, 4, 7, 8, 9, 12) \in S_{12}$. Find $Ord(\alpha)$.*

Solution: Since α is a product of disjoint cycles, $Ord(\alpha)$ is the least common divisor of the lengths of the disjoint cycles by Theorem 1.2.20. Hence, $Ord(\alpha) = 12$

QUESTION 2.4.2 *Determine whether* $\alpha = (1,2)(3,6,8)(4,5,7,8) \in S_9$ *is even or odd.*

Solution: First write α as a product of 2-cycles. By Theorem 1.2.23 $\alpha = (1,2)(3,8)(3,6)(4,8)(4,7)(4,5)$ is a product of six 2-cycles. Hence, α is even.

QUESTION 2.4.3 *Let* $\alpha = (1,3,7)(2,5,7,8) \in S_{10}$. *Find* α^{-1}.

Solution: Let $A = (1,3,7)$ and $B = (2,5,7,8)$. Hence, $\alpha = AB$. Thus, $\alpha^{-1} = B^{-1}A^{-1}$. Hence, By Theorem 1.2.25, $\alpha^{-1} = (8,7,5,2)(7,3,1)$.

QUESTION 2.4.4 *Prove that if* α *is a cycle of an odd order, then* α *is an even cycle.*

Solution: Let $\alpha = (a_1, a_2, ..., a_n)$. Since $Ord(\alpha)$ is odd, n is an odd number by Theorem 1.2.20. Hence, $\alpha = (a_1, a_n)(a_1, a_{n-1})...(a_1, a_2)$ is a product of $n-1$ 2-cycles. Since n is odd, $n-1$ is even. Thus, α is an even cycle.

QUESTION 2.4.5 *Prove that* $\alpha = (3,6,7,9,12,14) \in S_{16}$ *is not a product of 3-cycles.*

Solution: Since $\alpha = (3,14)(3,12)...(3,6)$ is a product of five 2-cycles, α is an odd cycle. Since each 3-cycle is an even cycle by the previous problem, a permutation that is a product of 3-cycles must be an even permutation. Thus, α is never a product of 3-cycles.

QUESTION 2.4.6 *Find two elements, say,a and b, in a group such that Ord(a) = Ord(b) = 2, and Ord(ab)=3.*

Solution: Let $a = (1,2), b = (1,3)$. Then $ab = (1,2)(1,3) = (1,3,2)$. Hence, Ord(a) = Ord(b) = 2, and Ord(ab) = 3.

QUESTION 2.4.7 *Let* $\alpha = (1,2,3)(1,2,5,6) \in S_6$. *Find* $Ord(\alpha)$, *then find* α^{35}.

Solution: First write α as a product of disjoint cycles. Hence, $\alpha = (1,3)(2,5,6)$. Thus, $Ord(\alpha) = 6$ by Theorem 1.2.20. Now, since $Ord(\alpha) = 6$, $\alpha^{35}\alpha = \alpha^{36} = e$. Hence, $\alpha^{35} = \alpha^{-1}$. Thus, $\alpha^{-1} = (6,5,2)(3,1) = (6,5,2,1)(3,2,1)$.

QUESTION 2.4.8 *Let $1 \leq n \leq m$. Prove that S_m contains a subgroup of order n.*

Solution: Since $1 \leq n \leq m$, $\alpha = (1, 2, 3, 4, ..., n) \in S_m$. By Theorem 1.2.20, $Ord(\alpha) = n$. Hence, the cyclic group (α) generated by α is a subgroup of S_m of order n.

QUESTION 2.4.9 *Give an example of two elements, say, a and b, such that Ord(a)=2, Ord(b)=3 and $Ord(ab) \neq lcm(2, 3) = 6$.*

Solution: Let $a = (1, 2), b = (1, 2, 3)$. Then $ab = (2, 3)$. Hence, Ord(a) = 2, Ord(b) = 3, and $Ord(ab) = 2 \neq lcm(2, 3) = 6$.

QUESTION 2.4.10 *Find two elements a, b in a group such that Ord(a) = 5, Ord(b) = 7, and Ord(ab) = 7.*

Solution: Let $G = S_7$, a = (1,2,3,4,5), *and*
b = (1,2,3,4,5,6,7). Then $ab = (1, 3, 5, 6, 7, 2, 4)$. Hence, Ord(a) = 5, Ord(b) = 7, and Ord(ab) = 7.

QUESTION 2.4.11 *Find two elements a, b in a group such that Ord(a) = 4, Ord(b) = 6, and Ord(ab) = 4.*

Solution: Let $G = S_6$, a = (1,2,3,4), b = (1,2,3,4,5,6). Then ab = (1,3)(2,4,5,6). By Theorem 1.2.20, Ord(ab) = 4.

QUESTION 2.4.12 *Find two elements a, b in a group such that Ord(a) = Ord(b) = 3, and Ord(ab) = 5.*

Solution: Let a = (1,2,3), b = (1,4,5) $\in S_5$. Then ab = (1,4,5,2,3). Hence, Ord(a) = Ord(b) = 3, and Ord(ab) = 5.

QUESTION 2.4.13 *Find two elements a, b in a group such that Ord(a) = Ord(b) = 4, and Ord(ab) = 7.*

Solution: Let a = (1,2,3,4), b = (1,5,6,7) $\in S_7$. Then ab = (1,5,6,7,2,3,4). Hence, Ord(a) = Ord(b) = 4, and Ord(ab) = 7.

QUESTION 2.4.14 *Let $2 \leq m \leq n$, and let a be a cycle of order m in S_n. Prove that $a \notin Z(S_n)$.*

Solution: Let $a = (a_1, a_2, ..., a_m)$, and let
$b = (a_1, a_2, a_3, ..., a_m, b_{m+1})$. Suppose that m is an odd number and $m < n$. Then
$ab = (a_1, a_3, a_5, ..., a_m, b_{m+1}, a_2, a_4, a_{m-1})$. Hence, Ord(ab) = $m + 1$. Now, assume that $a \in Z(S_n)$. Since Ord(a) = m and Ord(b) = m+1 and gcd(m,m+1) = 1 and ab = ba, we have Ord(ab) = m(m+1) by Question 2.1.14. A contradiction since ord(ab) = m+1. Thus, $a \notin Z(S_n)$. Now, assume that m is an even number and $m < n$. Then $ab = (a_1, a_3, a_5, ..., a_{m-1})(a_2, a_4, a_6, ..., a_m, b_{m+1})$. Hence, Ord(ab) = ((m-1)/2))((m-1)/2 + 1) by Theorem 1.2.20. Assume $a \in Z(S_n)$. Since Ord(a) = m and Ord(b) = m+1 and gcd(m,m+1) = 1 and ab = ba, Ord(ab) = m(m+1) by Question 2.1.14. A contradiction since $Ord(ab) = ((m-1)/2)((m-1)/2 + 1) \neq m(m+1)$. Thus, $a \notin Z(S_n)$. Now, assume m = n. Then $a = (1, 2, 3, 4, ..., n)$. Let $c = (1, 2)$. Then $ac = (1, 3, 4, 5, 6, ..., n)$ and $ca = (2, 3, 4, 5, ..., n)$. Hence, $ac \neq ca$. Thus, $a \notin Z(S_n)$.

QUESTION 2.4.15 *Let $H = \{\alpha \in S_n : \alpha(1) = 1\}$ $(n > 1)$. Prove that H is a subgroup of S_n.*

Solution: Let α and $\beta \in H$. Since $\alpha(1) = 1$ and $\beta(1) = 1$, $\alpha\beta(1) = \alpha(\beta(1) = 1$. Hence, $\alpha\beta \in H$. Since H is a finite set (being a subset of S_n) and closed, H is a subgroup of S_n by Theorem 1.2.8.

QUESTION 2.4.16 *Let $n > 1$. Prove that S_n contains a subgroup of order $(n-1)!$.*

Solution: Let H be the subgroup of S_n described in the previous Question. It is clear that Ord(H) = $(n-1)!$.

QUESTION 2.4.17 *Let $a \in A_5$ such that $Ord(a) = 2$. Show that $a = (a_1, a_2)(a_3, a_4)$, where a_1, a_2, a_3, a_4 are distinct elements.*

Solution: Since $Ord(a) = 2$, we conclude by Theorem 1.2.20 that we can write a as disjoint 2-cycles. Since the permutation is on a set of 5 elements, it is clear now that $a = (a_1, a_2)(a_3, a_4)$, where a_1, a_2, a_3, a_4 are distinct elements.

QUESTION 2.4.18 *Let $\alpha \in S_5$ be a 5-cycle, i.e., $Ord(\alpha) = 5$ (and hence $\alpha \in A_5$), and let $\beta = (b_1, b_2) \in S_5$ be a 2-cycle. If $\alpha(b_1) = b_2$ or $\alpha(b_2) = b_1$, then shhow that $Ord(\alpha\beta) = 4$. If $\alpha(b_1) \neq b_2$ and $\alpha(b_2) \neq b_1$, then show that $Ord(\alpha\beta) = 6$.*

Solution : Let $\beta = (b_1, b_2)$. We consider two cases: first assume that $\alpha(b_2) = b_1$. Then $\alpha(b_1) \neq b_2$ because α is a 5-cycle. Hence $\alpha\beta = (b_1)(b_2, b_3, b_4, b_5)$ where b_1, b_2, b_3, b_4, b_5 are distinct. Thus $Ord(\alpha\beta) = 4$ by Theorem 1.2.20. Also, if $\alpha(b_1) = b_2$, then $\alpha(b_2) \neq b_1$ again because α is a 5-cycle. Hence $\alpha\beta = (b_1, b_3, b_4, b_5)(b_2)$. Thus $Ord(\alpha\beta) = 4$ again by Theorem 1.2.20. Second case, assume that neither $\alpha(b_1) = b_2$ nor $\alpha(b_2) = b_1$. Hence $\alpha\beta(b_1) = b_3 \neq b_2$. Suppose that $\alpha\beta(b_3) = b_1$. Then $\alpha = (b_3, b_1, b_4, b_5, b_2)$ and thus $\alpha\beta = (b_1, b_3)(b_2, b_4, b_5)$ has order 6. Observe that $\alpha\beta(b_3) \neq b_2$ because $\alpha\beta(b_1) = \alpha(b_2) = b_3$ and $\alpha\beta(b_3) = \alpha(b_3)$ and α is a 5-cycle. Hence assume that $\alpha\beta(b_3) = b_4$, where $b_4 \neq b_1$ and $b_4 \neq b_2$. Then since $\alpha(b_1) \neq b_2$ and $\alpha(b_2) \neq b_1$, we conclude that $\alpha\beta = (b_1, b_3, b_4)(b_2, b_5)$ has order 6.

QUESTION 2.4.19 *Let $\alpha \in S_5$ be a 5-cycle, $\beta \in S_5$ be 2-cycle, and suppose that $Ord(\alpha\beta) = 4$. Show that $Ord(\alpha^2\beta) = 6$.*

Solution : Since $Ord(\alpha) = 5$, $Ord(\alpha^2) = 5$, and hence α^2 is a 5-cycle. Let $\beta = (b_1, b_2)$. Since $Ord(\alpha\beta) = 4$, we conclude $\alpha(b_1) = b_2$ or $\alpha(b_2) = b_1$ by Question 2.4.18. Suppose that $\alpha(b_1) = b_2$. Then α has the form $(..., b_1, b_2, ...)$ and $\alpha(b_2) \neq b_1$ because α is 5-cycle. Thus $\alpha^2(b_1) \neq b_2$ and $\alpha^2(b_2) \neq b_1$. Thus by Question 2.4.18 we conclude that $Ord(\alpha^2\beta) = 6$.

2.5 Cosets and Lagrange's Theorem

QUESTION 2.5.1 *Let $H = 4Z$ is a subgroup of Z. Find all left cosets of H in G.*

Solution: H, $1 + H = \{..., -11, -7, -3, 1, 5, 9, 13, 17, ...\}$, $2 + H = \{..., -14, -10, -6, -2, 2, 6, 10, 14, 18, ...\}$, $3 + H = \{..., -13, -9, -5, -1, 3, 7, 11, 15, 19, ...\}$.

QUESTION 2.5.2 *Let $H = \{1, 15\}$ is a subgroup of $G = U(16)$. Find all left cosets of H in G.*

Solution: Since $Ord(G) = \phi(16) = 8$ and Ord(H) = 2, [G:H] = number of all left cosets of H in G = Ord(G)/Ord(H) = 8/2 = 4 by Theorem 1.2.28. Hence, left cosets of H in G are : H, $3H = \{3, 13\}$, $5H = \{5, 11\}$, $7H = \{7, 9\}$.

QUESTION 2.5.3 *Let a be an element of a group such that $Ord(a) = 22$. Find all left cosets of (a^4) in (a).*

Solution: First, observe that $(a) = \{e, a, a^2, a^3, ..., a^{21}\}$. Also, Since $Ord(a^2) = Ord(a^4)$ by Question 2.3.25, we have $(a^4) = (a^2) = \{e, a^2, a^4, a^6, a^8, a^10, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}\}$ Hence, by Theorem 1.2.28, number of all left cosets of (a^4) in (a) is $22/11 = 2$. Thus, the left cosets of (a^4) in (a) are : (a^4), and $a(a^4) = \{a, a^3, a^5, a^7, a^9, ..., a^{21}\}$.

QUESTION 2.5.4 *Let G be a group of order 24. What are the possible orders for the subgroups of G.*

Solution: Write 24 as product of distinct primes. Hence, $24 = (3)(2^3)$. By Theorem 1.2.27, the order of a subgroup of G must divide the order of G. Hence, We need only to find all divisors of 24. By Theorem 1.2.17, number of all divisors of 24 is $(1 + 1)(3 + 1) = 8$. Hence, possible orders for the subgroups of G are : 1,3,2,4,8,6,12,24.

QUESTION 2.5.5 *Let G be a group such that $Ord(G) = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.*

Solution: Let H be a proper subgroup of G. Then Ord(H) must divide pq by Theorem 1.2.27. Since H is proper, the possible orders for H are : 1, p,q. Suppose Ord(H) = 1, then $H = \{e\}$ is cyclic. Suppose $Ord(H) = p$. Let $h \in H$ such that $h \neq e$. Then Ord(h) divide Ord(H) by Theorem 1.2.29. Since $h \neq e$ and Ord(h) divides p, Ord(h) = p. Thus, H = (h) is cyclic. Suppose Ord(H) = q. Then by a similar argument as before, we conclude that H is cyclic. Hence, every proper subgroup of G is cyclic.

QUESTION 2.5.6 *Let G be a group such that $Ord(G) = 77$. Prove that every proper subgroup of G is cyclic.*

Solution: Since Ord(G) = 77 = (7)(11) is a product of two primes, every proper subgroup of G is cyclic by the previous Question.

QUESTION 2.5.7 *Let $n \geq 2$, and let $a \in U(n)$. Prove that $a^{\phi(n)} = 1$ in $U(n)$.*

Solution : Since $Ord(U(n)) = \phi(n)$ and $a \in U(n)$, $a^{\phi(n)} = 1$ in $U(n)$ by Theorem 1.2.30.

QUESTION 2.5.8 *Let $3 \in U(16)$. Find 3^{19} in $U(16)$.*

Solution: Since $Ord(U(16)) = \phi(16) = 8$, $3^8 = 1$ by the previous Question. Hence,$3^{8k} = 1$ for each $k \geq 1$. Thus, $3^{19} = 3^{19 mod 8} = 3^3 = 27(mod 16) = 11$ in $U(16)$.

QUESTION 2.5.9 *Let H, K be subgroups of a group. If Ord(H) = 24 and Ord(K) = 55, find the order of $H \cap K$.*

Solution: Since $H \cap K$ is a subgroup of both H and K, $Ord(H \cap K)$ divides both Ord(H) and Ord(K) by Theorem 1.2.27. Since $gcd(24, 55) = 1$ and $Ord(H \cap K)$ divides both numbers 24 and 55, we conclude that $Ord(H \cap K) = 1$. Thus, $H \cap K = \{e\}$.

QUESTION 2.5.10 *Let G be a group with an odd number of elements. Prove that $a^2 \neq e$ for each non identity $a \in G$.*

Solution: Deny. Hence, for some non identity element $a \in G$, we have $a^2 = e$. Thus,$\{e, a\}$ is a subgroup of G of order 2. Hence, 2 divides Ord(G) by Theorem 1.2.27. A contradiction since 2 is an even integer and Ord(G) is an odd integer.

QUESTION 2.5.11 *Let G be an Abelian group with an odd number of elements. Prove that the product of all elements of G is the identity.*

Solution: By the previous Question, G does not have a non identity element that is the inverse of itself,i.e. $a^2 \neq e$ for each non identity $a \in G$. Hence, the elements of G are of the following form : $e, a_1, a_1^{-1}, a_2, a_2^{-1}, ..., a_m, a_m^{-1}$. Hence, $e, a_1 a_a^- 1 a_2 a_2^{-1} a_3 a_3^{-1} ... a_m a_m^{-1} = e(a_1 a_1^{-1})(a_2 a_2^{-1})(a_3 a_3^{-1}) ...(a_m a_m^{-1}) = e(e)(e)(e)...(e) = e$

QUESTION 2.5.12 *Let G be a group with an odd number of elements. Prove that for each $a \in G$, the equation $x^2 = a$ has a unique solution.*

Solution: First, we show that for each $a \in G$, the equation $x^2 = a$ has a solution. Let $a \in G$, and let $m = Ord(a)$. By Theorem 1.2.29, m must divide Ord(G). Since Ord(G) is an odd number and Ord(a) divides Ord(G), m is an odd number. Hence, let $x = a^{(m+1)/2}$. Then, $(a^{(m+1)/2})^2 = a^{m+1} = aa^m = a(e) = a$ is a solution to the equation $x^2 = a$. Now, we show that $a^{(Ord(a)+1)/2}$ is the only solution to the equation $x^2 = a$ for each $a \in G$. Hence, let $a \in G$. Assume there is a $b \in G$ such that $b^2 = a$. Hence, $(b^2)^{Ord(a)} = a^{Ord(a)} = e$. Thus, Ord(b) divides 2Ord(a). Since Ord(b) must be an odd number and hence gcd(2,Ord(b)) = 1, we conclude that Ord(b) must divide Ord(a) by Theorem 1.2.5. Thus, $b^{Ord(a)} = e$. Now, $b = bb^{Ord(a)} = b^{1+Ord(a)} = (b^2)^{Ord(a)+1} = a^{Ord(a)+1}$.

QUESTION 2.5.13 *Let a, b be elements of a group such that $b \notin (a)$ and Ord(a) = Ord(b) = p is a prime number. Prove that $(b^i) \cap (a^j) = \{e\}$ for each $1 \leq i < p$ and for each $1 \leq j < p$.*

Solution: Let $1 \leq i < p$ and $1 \leq j < p$, and let $H = (b^i) \cap (a^j)$. Since Ord(a) = Ord(b) = p is a prime number and H is a subgroup of both (b^i) and (a^j), Ord(H) divides p by Theorem 1.2.27. Hence, Ord(H) = 1 or Ord(H) = p. Suppose that Ord(H) = p. Then $(b^i) = (a^j)$. But since $Ord(b^i) = Ord(b)$ and $Ord(a) = Ord(a^j)$, we have $(b) = (b^i) = (a^j) = (a)$. Hence, $b \in (a)$ which is a contradiction. Thus, Ord(H) =1. Hence, $H = \{e\}$.

QUESTION 2.5.14 *Let G be a non-Abelian group of order $2p$ for some prime $p \neq 2$. Prove that G contains exactly $p-1$ elements of order p and it contains exactly p elements of order 2.*

Solution:Since p divides the order of G, G contains an element a of order p by Theorem 1.2.31. Hence, $H = (a)$ is a subgroup of G of order p. Hence, $[G : H] = 2p/p = 2$. Let $b \in G \setminus H$. Hence, H and bH are the only left cosets of H in G. Now, We show that $b^2 \notin bH$. Suppose that $b^2 \in bH$. Hence, $b^2 = bh$ for some $h \in H$. Thus, $b = h \in H$. A contradiction since $b \notin H$. Since $G = H \cup bH$ and $b^2 \notin bH$, we conclude that $b^2 \in H$. Since Ord(H) = p is a prime number and $b^2 \in H$, $Ord(b^2)$ must be 1 or p by Theorem 1.2.29. Suppose that $Ord(b^2) = p$. Then $b^{2p} = e$. Hence, Ord(b) = p or Ord(b) = 2p. Suppose that Ord(b) = 2p. Then G = (b) is a cyclic group. Hence, G is Abelian. A contradiction. Thus, assume that Ord(b) = p. Then $Ord(b) = Ord(b^2) = p$. Since Ord(H) = p and $Ord(b^2) = Ord(b) = p$ and $b^2 \in H$, we conclude that $(b) = (b^2) = H$. Hence, $b \in H$. A contradiction. Thus, $Ord(b^2)$ must be 1. Hence, $b^2 = e$. Thus, each element of G that lies outside H is of order 2. Since Ord(H) = p and Ord(G) = 2p, we conclude that G contains exactly p elements of order p. Hence, if $c \in G$ and Ord(c) = p, then $c \in H$. Thus, G contains exactly $p - 1$ elements of order p.

QUESTION 2.5.15 *Let G be a non-Abelian group of order 26. Prove that G contains exactly 13 elements of order 2.*

Solution. Since 26 = (2)(13), by the previous Question G contains exactly 13 elements of order 2.

QUESTION 2.5.16 *Let G be an Abelian group of order pq for some prime numbers p and q such that $p \neq q$. Prove that G is cyclic.*

Solution: Since p divides Ord(G) and q divides Ord(G), G contains an element, say, a, of order p and it contains an element, say,b, of order q. Since ab = ba and gcd(p,q) = 1, Ord(ab) = pq by Question 2.1.14. Hence, $G = (ab)$ is a cyclic group.

QUESTION 2.5.17 *Let G be an Abelian group of order 39. Prove that G is cyclic.*

Solution: Since 39 = (3)(13), G is cyclic by the previous Question.

QUESTION 2.5.18 *Find an example of a non-cyclic group,say, G, such that Ord(G) = pq for some prime numbers p and q and $p \neq q$.*

Solution: Let $G = S_3$. Then $Ord(G) = 6 = (2)(3)$. But we know that S_3 is not Abelian and hence it is not cyclic.

QUESTION 2.5.19 *Let G be a finite group such that Ord(G) = p is a prime number. Prove that G is cyclic.*

Solution: Let $a \in G$ such that $a \neq e$. Then Ord(a) = p by Theorem 1.2.29. Hence, $G = (a)$ is cyclic.

QUESTION 2.5.20 *Find an example of a non-Abelian group, say, G, such that every proper subgroup of G is cyclic.*

Solution: Let $G = S_3$. Then G is a non-Abelian group of order 6. Let H be a proper subgroup of G. Then Ord(H) = 1 or 2 or 3 by Theorem 1.2.27. Hence, by the previous Question H is cyclic.

QUESTION 2.5.21 *Let G be a group such that $H = \{e\}$ is the only proper subgroup of G. Prove that $Ord(G)$ is a prime number.*

Solution: Ord(G) can not be infinite by Question 2.3.21. Hence, G is a finite group. Let Ord(G) = m. Suppose that m is not prime. Hence, there is a prime number q such that q divides m. Thus, G contains an element, say,a, of of order q by Theorem 1.2.31. Thus, (a) is a proper subgroup of G of order q. A contradiction. Hence, Ord(G) = m is a prime number.

QUESTION 2.5.22 *Let G be a finite group with an odd number of elements, and suppose that H be a proper subgroup of G such that Ord(H) = p is a prime number. If $a \in G \setminus H$, then prove that $aH \neq a^{-1}H$.*

Solution: Since Ord(H) divides Ord(G) and Ord(G) is odd, we conclude that $p \neq 2$. Let $a \in G \setminus H$. Suppose that $aH = a^{-1}H$. Then $a^2 = h \in H$ for some $h \in H$ by Theorem 1.2.26. Hence, $a^{2p} = h^p = e$. Thus, Ord(a) divides 2p by Theorem 1.2.1. Since Ord(G) is odd and by Theorem 1.2.29 Ord(a) divides Ord(G), Ord(a) is an odd number. Since Ord(a) is odd and Ord(a) divides 2p and $p \neq 2$ and $a \notin H$, we conclude $Ord(a) = p$. Hence,$Ord(a^2) = p$ and therefore $(a) = (a^2)$. Since $Ord(H) = p$ and $a^2 \in H$ and Ord(a) = p, $(a) = (a^2) = H$. Thus, $a \in H$. A contradiction. Thus, $aH \neq a^{-1}H$ for each $a \in G \setminus H$.

QUESTION 2.5.23 *Suppose that H, K are subgroups a group G such that $D = H \cap K \neq \{e\}$. Suppose Ord(H) = 14 and Ord(K) = 35. Find $Ord(D)$.*

Solution: Since D is a subgroup of both H and K, Ord(D) divides both 14 and 35 by Theorem 1.2.27. Since 1 and 7 are the only numbers that divide both 14 and 35 and $H \cap K \neq \{e\}$, $Ord(D) \neq 1$. Hence, Ord(D) = 7.

QUESTION 2.5.24 *Let a, b be elements in a group such that $ab = ba$ and Ord(a) = 25 and Ord(b) = 49. Prove that G contains an element of order 35.*

Solution: Since ab = ba and gcd(25,49) = 1, Ord(ab) = (25)(49) by Question 2.1.14. Hence, let $x = (ab)^{35}$. Then, by Question 2.1.12, $Ord(x) = Ord(ab^{35}) =$
$ord(ab)/gcd(35, Ord(ab)) = (25)(49)/gcd(35, (25)(49)) = 35$. Hence, G contains an element of order 35.

QUESTION 2.5.25 *Let H be a subgroup of S_n. Show that either $H \subset A_n$ or exactly half of the elements of H are even permutation.*

Solution : Suppose that $H \not\subset A_n$. Let K be the set of all even permutations of H. Then K is not empty since $e \in K$ (e is the identity). It is clear that K is a subgroup of H. Let β be an odd permutation of H. Then the each element of the left coset βK is an odd permutation (recall that a product of odd with even gives an odd permutation). Now let α be an odd permutation H. Since H is a group, there is an element $k \in H$ such that $\alpha = \beta k$. Since α and β are odd, we conclude that k is even, and hence $k \in K$. Thus $\alpha \in \beta K$. Hence βK contains all odd permutation of H. Since $Ord(\beta K) = Ord(K)$ (because βK is a left coset of K), we conclude that exactly half of the elements of H are even permutation.

2.6 Normal Subgroups and Factor Groups

QUESTION 2.6.1 *Let H be a subgroup of a group G such that [G:H] = 2. Prove that H is a normal subgroup of G.*

Solution: Let $a \in G \setminus H$. Since [G:H] = 2, H and aH are the left cosets of H in G ,and H and Ha are the right cosets of H in G. Since $G = H \cup aH = H \cup Ha$, and $H \cap aH = \phi$, and $H \cap Ha = \phi$, we conclude that $aH = Ha$. Hence,$aHa^{-1} = H$. Thus, H is a normal subgroup of G by Theorem 1.2.32.

QUESTION 2.6.2 *Prove that A_n is a normal subgroup of S_n.*

Solution: Since $[S_n : A_n] = Ord(S_n)/Ord(A_n)$ by Theorem 1.2.28, we conclude that $[S_n : A_n] = 2$. Hence, A_n is a normal subgroup of S_n by the previous Question.

QUESTION 2.6.3 *Let a be an element of a group G such that Ord(a) is finite. If H is a normal subgroup of G, then prove that Ord(aH) divides Ord(a).*

Solution: Let $m = Ord(a)$. Hence, $(aH)^m = a^m H = eH = H$. Thus, Ord(aH) divides m = Ord(a) by Theorem 1.2.1.

QUESTION 2.6.4 *Let H be a normal subgroup of a group G and let $a \in G$. If $Ord(aH) = 5$ and $Ord(H) = 4$, then what are the possibilities for the order of a.*

Solution: Since Ord(aH) = 5, $(aH)^5 = a^5 H = H$. Hence, $a^5 \in H$ by Theorem 1.2.26. Thus, $a^5 = h$ for some $h \in H$. Thus, $(a^5)^4 = h^4 = e$. Thus, $a^{20} = e$. Hence, Ord(a) divides 20 by Theorem 1.2.1. Since $Ord(aH) \mid Ord(a)$ by the previous Question and $Ord(a) \mid 20$, we conclude that all possibilities for the order of a are : $5, 10, 20$.

QUESTION 2.6.5 *Prove that $Z(G)$ is a normal subgroup of a group G.*

Solution: Let $a \in G$, and let $z \in Z(G)$. Then $aza^{-1} = aa^{-1}z = ez = z$. Thus, $aZ(G)a^{-1} = Z(G)$ for each $a \in G$. Hence, $Z(G)$ is normal by Theorem 1.2.32.

QUESTION 2.6.6 *Let G be a group and let L be a subgroup of $Z(G)$ (note that we may allow $L = Z(G)$), and suppose that G/L is cyclic. Prove that G is Abelian.*

Solution: Since G/L is cyclic, $G/Z(G) = (wL)$ for some $w \in G$. Let $a, b \in G$. Since $G/L = (wL)$, $aL = w^nL$ and $bL = w^mL$ for some integers n, m. Hence, $a = w^n z_1$ and $b = w^m z_2$ for some $z_1, z_2 \in L$ by Theorem 1.2.26. Since $z_1, z_2 \in L \subset Z(G)$ and $w^n w^m = w^m w^n$, we have $ab = w^n z_1 w^m z_2 = w^m z_2 w^n z_1 = ba$. Thus, G is Abelian.

QUESTION 2.6.7 *Let G be a group such that $Ord(G) = pq$ for some prime numbers p, q. Prove that either $Ord(Z(G)) = 1$ or G is Abelian.*

Solution: Deny. Hence $1 < Ord(Z(G)) < pq$. Since Z(G) is a subgroup of G, Ord(Z(G)) divides Ord(G) = pq by Theorem 1.2.27. Hence, Ord(Z(G)) is either p or q. We may assume that Ord(Z(G)) = p. Hence, Ord(G/Z(G)) = [G:Z(G)] = Ord(G)/Ord(Z(G)) = q is prime. Thus, $G/Z(G)$ is cyclic by Question 2.5.19. Hence, by the previous Question, G is Abelian, A contradiction. Thus, our denial is invalid. Therefore, either Ord(Z(G)) = 1 or Ord(Z(G)) = pq,i.e. G is Abelian.

QUESTION 2.6.8 *Give an example of a non-Abelian group, say,G, such that G has a normal subgroup H and G/H is cyclic.*

Solution: Let $G = S_3$, and let $a = (1, 2, 3) \in G$. Then Ord(a) = 3. Let $H = (a)$. Then $Ord(H) = Ord(a) = 3$. Since [G:H] = 2, H is a normal subgroup of G by Question 2.6.1. Thus, G/H is a group and Ord(G/H) = 2. Hence, G/H is cyclic by Question 2.5.19. But we know that $G = S_3$ is not Abelian group.

QUESTION 2.6.9 *Prove that every subgroup of an Abelian group is normal.*

Solution: Let H be a subgroup of an Abelian group G. Let $g \in G$. Then $gHg^{-1} = gg^{-1}H = eH = H$. Hence, H is normal by Theorem 1.2.32.

QUESTION 2.6.10 *Let Q^+ be the set of all positive rational numbers, and let Q^* be the set of all nonzero rational numbers. We know that Q^+ under multiplication is a (normal) subgroup of $Q*$. Prove that $[Q^* : Q^+] = 2$.*

Solution: Since $-1 \in Q^* \setminus Q^+$, $-1Q^+$ is a left coset of Q^+ in Q^*. Since $Q^+ \cap -1Q^+ = \{0\}$ and $Q^+ \cup -1Q^+ = Q^*$, we conclude that Q^+ and $-1Q^+$ are the only left cosets of Q^+ in Q^*. Hence, $[Q^* : Q^+] = 2$.

QUESTION 2.6.11 *Prove that Q (the set of all rational numbers) under addition, has no proper subgroup of finite index.*

Solution : Deny. Hence Q under addition, has a proper subgroup, say, H, such that [Q : H] = n is a finite number. Since Q is Abelian, H is a normal subgroup of Q by Question 2.6.9. Thus, Q/H is a group and $Ord(Q/H) = [Q : H] = n$. Now, let $q \in Q$. Hence, by Theorem 1.2.30, $(qH)^n = q^nH = H$. Thus, $q^n = h \in H$ by Theorem 1.2.26. Since addition is the operation on Q, q^n means nq. Thus, $q^n = nq \in H$ for each $q \in Q$. Since $ny \in H$ for each $y \in Q$ and $q/n \in Q$, we conclude that $q = n(q/n) \in H$. Thus, $Q \subset H$. A contradiction since H is a proper subgroup of Q. Hence, our denial is invalid. Thus, Q has no proper subgroup of finite index.

QUESTION 2.6.12 *Prove that R^* (the set of all nonzero real numbers) under multiplication, has a proper subgroup of finite index.*

Solution: Let $H = R^+$(the set of all nonzero positive real numbers). Then, it is clear that H is a (normal) subgroup of R^*. Since $R = R^+ \cup -1R^+$ and $R^+ \cap -1R^+ = \{0\}$, we conclude that R^+ and $-1R^+$ are the only left cosets of R^+ in R^*. Hence, $[R^* : R^+] = 2$.

QUESTION 2.6.13 *Prove that R^+ (the set of all nonzero positive real numbers) under multiplication, has no proper subgroup of finite index.*

Solution: Deny. Hence, R^+ has a proper subgroup, say, H, such that $[R^+ : H] = n$ is a finite number. Let $r \in R^+$. Since $rH \in R^+/H$ and $Ord(R^+/H) = n$, we conclude that $(rH)^n = r^nH = H$ by Theorem 1.2.30. Thus, $r^n \in H$ for each $r \in R^+$. In particular, $r = (\sqrt[n]{r})^n \in H$. Thus, $R^+ \subset H$. A contradiction since H is a proper subgroup of R^+. Hence, R^+ has no proper subgroups of finite index.

QUESTION 2.6.14 *Prove that C^* (the set of all nonzero complex numbers) under multiplication, has no proper subgroup of finite index.*

Solution : Just use similar argument as in the previous Question.

QUESTION 2.6.15 *Prove that R^+(the set of all positive nonzero real numbers) is the only proper subgroup of R^*(the set of all nonzero real numbers) of finite index.*

Solution: Deny. Then R^* has a proper subgroup $H \neq R^+$ such that $[R^* : H] = n$ is finite. Since $Ord(R^*/H) = [R^* : H] = n$, we have $(xH)^n = x^nH = H$ for each $x \in R^*$ by Theorem 1.2.30. Thus,$x^n \in H$ for each $x \in R^*$. Now, let $x \in R^+$. Then $x = (\sqrt[n]{x})^n \in H$. Thus, $R^+ \subset H$. Since $H \neq R^+$ and $R^+ \subset H$, we conclude that H must contain a negative number, say, -y, for some $y \in R^+$. Since $1/y \in R^+ \subset H$ and $-y \in H$ and H is closed, we conclude that $-y(1/y) = -1 \in H$. Since H is closed and $R^+ \subset H$ and $-1 \in H$, $-R^+$(the set of all nonzero negative real numbers) $\subset H$. Since $R^+ \subset H$ and $-R^+ \subset H$, we conclude that $H = R^*$. A contradiction since H is a proper subgroup of R^*. Hence,R^+ is the only proper subgroup of R^* of finite index.

QUESTION 2.6.16 *Let N be a normal subgroup of a group G. If H is a subgroup of G, then prove that $NH = \{nh : n \in N \text{ and } h \in H\}$ is a subgroup of G.*

Solution: Let $x, y \in NH$. By Theorem 1.2.7 We need only to show that $x^{-1}y \in NH$. Since $x, y \in NH$, $x = n_1h_1$ and $y = n_2h_2$ for some $n_1, n_2 \in N$ and for some $h_1, h_2 \in H$. Hence, we need to show that $(n_1h_1)^{-1}n_2h_2 = h_1^{-1}n_1^{-1}n_2h_2 \in NH$. Since N is normal, we have $h_1^{-1}n_1^{-1}n_2h_1 = n_3 \in N$. Hence, $h_1^{-1}n_1^{-1}n_2h_2 = (h_1^{-1}n_1^{-1}n_2h_1)h_1^{-1}h_2 = n_3h_1^{-1}h_2 \in NH$. Thus, NH is a subgroup of G.

QUESTION 2.6.17 *Let N, H be normal subgroups of a group G. Prove that $NH = \{nh : n \in N \text{ and } h \in H\}$ is a normal subgroup of G.*

Solution: Let $g \in G$. Then $g^{-1}NHg = g^{-1}Ngg^{-1}Hg = (g^{-1}Ng)(g^{-1}Hg) = NH$.

QUESTION 2.6.18 *Let N be a normal cyclic subgroup of a group G. If H is a subgroup of N, then prove that H is a normal subgroup of G.*

Solution: Since N is cyclic, N = (a) for some $a \in N$. Since H is a subgroup of N and every subgroup of a cyclic group is cyclic and N = (a), we have $H = (a^m)$ for some integer m. Let $g \in G$, and let $b \in H = (a^m)$. Then $b = a^{mk}$ for some integer k. Since N =(a) is normal in G, we have $g^{-1}ag = a^n \in N$ for some integer n. Since $g^{-1}ag = a^n$ and by Question 2.1.1 $(g^{-1}a^{mk}g) = (g^{-1}ag)^{mk}$, we have $g^{-1}bg = g^{-1}a^{mk}g = (g^{-1}ag)^{mk} = (a^n)^{mk} = a^{mkn} \in H = (a^m)$

QUESTION 2.6.19 *Let G be a finite group and H be a subgroup of G with an odd number of elements such that [G:H] = 2. Prove that the product of all elements of G(taken in any order) does not belong to H.*

Solution: Since [G:H] = 2, by Question 2.6.1 we conclude that H is normal in G. Let $g \in G \setminus H$. Since [G:H] = 2, H and gH are the only elements of the group G/H. Since [G:H] = Ord(G)/Ord(H) = 2, Ord(G) = 2Ord(H). Since Ord(H) = m is odd and Ord(G) = 2Ord(H) = 2m, we conclude that there are exactly m elements that are in G but not in H. Now, say, $x_1, x_2, x_3, ..., x_{2m}$ are the elements of G. Since $x_iH = gH$ for each $x_i \in G\setminus H$ and $x_iH = H$ for each $x_i \in H$ and G/H is Abelian(cyclic), we have $x_1x_2x_3...x_{2m}H = x_1Hx_2H...x_{2m}H = g^mHH = g^mH$. Since m is odd and Ord(gH) = 2 in G/H and 2 divides $m-1$, we have $g^{m-1}H = H$ and hence $g^mH = g^{m-1}HgH = HgH = gH \neq H$. Since $x_1x_2x_3...x_{2m}H \neq H$, the product $x_1x_2x_3...x_{2m}$ does not belong to H by Theorem 1.2.26.

QUESTION 2.6.20 *Let H be a normal subgroup of a group G such that Ord(H) = 2. Prove that $H \subset Z(R)$.*

Solution: Since Ord(H) = 2, we have $H = \{e, a\}$. Let $g \in G$ and $g \neq a$. Since $g^{-1}Hg = H$, we conclude that $g^{-1}ag = a$. Hence, $ag = ga$. Thus, $a \in Z(R)$. Thus, $H \subset Z(R)$.

QUESTION 2.6.21 *Let G be a finite group and H be a normal subgroup of G. Suppose that $Ord(aH) = n$ in G/H for some $a \in G$. Prove that G contains an element of order n.*

Solution: Since Ord(aH) = n, Ord(aH) divides Ord(a) by Question 2.6.3. Hence, Ord(a) = nm for some positive integer m. Thus, by Question 2.1.12, we have $Ord(a^m) = Ord(a)/gcd(m, nm) = nm/m = n$. Hence, $a^m \in G$ and $Ord(a^m) = n$.

QUESTION 2.6.22 *Find an example of an infinite group, say, G, such that G contains a normal subgroup H and Ord(aH) = n in G/H but G does not contain an element of order n.*

Solution: Let $G = Z$ under normal addition, and n = 3, and $H = 3Z$. Then H is normal in Z and Ord(1+3Z) = 3, but Z does not contain an element of order 3.

QUESTION 2.6.23 *Let H, N be finite subgroups of a group G, say, Ord(H) = k and Ord(N) = m such that gcd(k,m) = 1. Prove that $HN = \{hn : h \in H \text{ and } n \in N\}$ has exactly km elements.*

Solution: Suppose that $h_1n_1 = h_2n_2$ for some $n_1, n_2 \in N$ and for some $h_1, h_2 \in H$. We will show that $h_1 = h_2$ and $n_1 = n_2$. Hence, $n_1n_2^{-1} = h_1^{-1}h_2$. Since Ord(N) = m, we have $e = (n_1n_2^{-1})^m = (h_1^{-1}h_2)^m$. Thus, $Ord(h_1h_2^{-1})$ divides m. Since gcd(k,m) = 1 and $Ord(h_1h_2^{-1})$ divides both k and m, we conclude that $Ord(h_1^{-1}h_2) = 1$. Hence, $h_1^{-1}h_2 = e$. Thus, $h_2 = h_1$. Also, since Ord(H) = k, we have $e = (h_1^{-1}h_2)^k = (n_1n_2^{-1})^k$. Thus, by a similar argument as before, we conclude that $n_1 = n_2$. Hence, HN has exactly km elements.

QUESTION 2.6.24 *Let N be a normal subgroup of a finite group G such that Ord(N) = 7 and ord(aN) = 4 in G/N for some $a \in G$. Prove that G has a subgroup of order 28.*

Solution: Since G/N has an element of order 4 and G is finite, G has an element, say, b, of order 4 by Question 2.6.21. Thus, $H = (b)$ is a cyclic subgroup of G of order 4. Since N is normal, we have NH is a subgroup of G by Question 2.6.16. Since gcd(7,4) = 1, Ord(NH) = 28 by the previous Question.

QUESTION 2.6.25 *Let G be a finite group such that $Ord(G) = p^nm$ for some prime number p and positive integers n, m and gcd(p,m) = 1. Suppose that N is a normal subgroup of G of order p^n. Prove that if H is a subgroup of G of order p^k, then $H \subset N$.*

Solution: Let H be a subgroup of G of order p^k, and let $x \in H$. Then $xN \in G/N$. Since Ord(G/N) = [G:N] = m, we have $x^mN = N$ by Theorem 1.2.30. Since $x \in H$ and Ord(H) = p^k, we conclude that $Ord(x) = p^j$. Thus, $x^{p^j}N = N$. Since $x^mN = x^{p^j}N = N$, we conclude that Ord(xN) divides both m and p^j. Hence, since $gcd(p, m) = gcd(p^j, m) = 1$, we have Ord(xN) = 1. Thus, xN = N. Hence, $x \in N$ by Theorem 1.2.26.

QUESTION 2.6.26 *Let H be a subgroup of a group G, and let $g \in G$. Prove that $D = g^{-1}Hg$ is a subgroup of G. Furthermore, if Ord(H) = n,then $Ord(g^{-1}Hg) = Ord(H) = n$.*

Solution: Let $x, y \in D$. Then x = $g^{-1}h_1g$ and $y = g^{-1}h_2g$ for some $h_1, h_2 \in H$. Hence, $x^{-1}y = (g^{-1}h_1^{-1}g)(g^{-1}h_2g) = g^{-1}h_1^{-1}h_2g \in g^{-1}Hg$

since $h_1^{-1}h_2 \in H$. Thus, $D = g^{-1}Hg$ is a subgroup of G by Theorem 1.2.7. Now, suppose that Ord(H) = n. Let $g \in G$. We will show that $Ord(g^{-1}Hg) = n$. Suppose that $g^{-1}h_1g = g^{-1}h_2g$. Since G is a group and hence it satisfies left-cancelation and right-cancelation, we conclude that $h_1 = h_2$. Thus, $Ord(g^{-1}Hg) = Ord(H) = n$.

QUESTION 2.6.27 *Suppose that a group G has a subgroup, say, H, of order n such that H is not normal in G. Prove that G has at least two subgroups of order n.*

Solution: Since H is not normal in G, we have $g^{-1}Hg \neq H$ for some $g \in G$. Thus, by Question 2.6.26, $g^{-1}Hg$ is another subgroup of G of order n.

QUESTION 2.6.28 *Let n be a positive integer and G be a group such that G has exactly two subgroups, say, H and D, of order n. Prove that if H is normal in G, then D is normal in G.*

Solution: Suppose that H is normal in G and D is not normal in G. Since D is not normal in G, we have $g^{-1}Dg \neq D$ for some $g \in G$. Since $g^{-1}Dg$ is a subgroup of G of order n by Question 2.6.26 and $g^{-1}Dg \neq D$ and D, H are the only subgroups of G of order n, We conclude that $g^{-1}Dg = H$. Hence, $D = gHg^{-1}$. But, since H is normal in G, we have $g^{-1}Hg = H = gHg^{-1} = D$. A contradiction. Thus,$g^{-1}Dg = D$ for each $g \in G$. Hence, D is normal in G.

QUESTION 2.6.29 *Let H be a subgroup of a group G. Prove that H is normal in G if and only if $g^{-1}Hg \subset H$ for each $g \in G$.*

Solution: We only need to prove the converse. Since $g^{-1}Hg \subset H$ for each $g \in G$, we need only to show that $H \subset g^{-1}Hg$ for each $g \in G$. Hence, let $h \in H$ and $g \in G$. Since $gHg^{-1} \subset H$, we have $ghg^{-1} \in H$. Since $g^{-1}Hg \subset H$ and $ghg^{-1} \in H$, we conclude that $g^{-1}(ghg^{-1})g = h \in g^{-1}Hg$. Thus, $H \subset g^{-1}Hg$ for each $g \in G$. Hence, $g^{-1}Hg = H$ for each $g \in G$. Thus, H is normal in G.

QUESTION 2.6.30 *Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a normal subgroup of G.*

Solution: Let D be the intersection of all subgroups of G of order n. Let $g \in G$. If $g^{-1}Dg$ is a subset of each subgroup of G of order n, then $g^{-1}Dg$ is a subset of the intersection of all subgroups of G of order n. Hence, $g^{-1}Dg \subset D$ for each $g \in G$ and therefore D is normal in G. Hence, assume that $g^{-1}Dg$ is not contained in a subgroup, say, H, of G of order n for some $g \in G$. Thus D is not contained in gHg^{-1}, for if D is contained in gHg^{-1}, then $g^{-1}Dg$ is contained in H which is a contradiction. But gHg^{-1} is a subgroup of G of order n by Question 2.6.26, and Hence $D \subset gHg^{-1}$, a contradiction. Thus, $g^{-1}Dg = D$ for each $g \in G$. Hence, D is normal in G.

QUESTION 2.6.31 *Suppose that H and K are Abelian normal subgroups of a group G such that $H \cap K = \{e\}$. Prove that HK is an Abelian normal subgroup of G.*

Solution: Let $h \in H$ and $k \in K$. Since $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ and K is normal, $hkh^{-1} \in K$. Thus, $(hkh^{-1})k^{-1} \in K$. Also, since $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ and H is normal, we have $kh^{-1}k^{-1} \in H$. Thus, $h(kh^{-1}k^{-1}) \in H$. Since $H \cap K = \{e\}$, we conclude that $hkh^{-1}k^{-1} = e$. Thus, $hk = kh$. Hence, HK is Abelian. Now, HK is normal by Question 2.6.17.

2.7 Group Homomorphisms and Direct Product

Observe that when we say that a map Φ from G ONTO H, then we mean that $\Phi(G) = H$, i.e., ϕ is surjective.

QUESTION 2.7.1 *Let Φ be a group homomorphism from a group G to a group H. Let D be a subgroup of G of order n. Prove that $Ord(\Phi(D))$ divides n.*

Solution: Define a new group homomorphis, say $\alpha : D \longrightarrow \Phi(D)$ such that $\alpha(d) = \Phi(d)$ for each $d \in D$. Clearly, α is a group homomorphism from D ONTO $\alpha(D) = \Phi(D)$. Hence, by Theorem 1.2.35, we have $D/Ker(\alpha) \cong \alpha(D) = \Phi(D)$. Thus, Ord(D)/Ord(Ker($\alpha$)) = Ord($\Phi(D)$). Hence, n = $Ord(ker(\alpha))Ord(\Phi(D))$. Thus, Ord(D) divides n.

QUESTION 2.7.2 *Let Φ be a group homomorphism from a group G ONTO a group H. Prove that $G \cong H$ if and only if $Ker(\Phi) = \{e\}$.*

Solution: Suppose that $G \cong H$. Hence, $\Phi(x) = e_H$(the identity in H) iff $x = e$ (the identity of G). Hence, $Ker(\Phi) = \{e\}$. Conversely, suppose that $Ker(\Phi) = \{e\}$. Hence, by Theorem 1.2.35, we have $G/Ker(\Phi) = G/\{e\} = G \cong \Phi(G) = H$.

QUESTION 2.7.3 *Let Φ be a group homomorphism from a group G to a group H. Let K be a subgroup of H. Prove that $\Phi^{-1}(K) = \{x \in G : \Phi(x) \in K\}$ is a subgroup of G.*

Solution: Let $x, y \in \Phi^{-1}(K)$. Then $\Phi(x) = k \in K$. Hence, by Theorem 1.2.34(2), $\Phi(x^{-1}) = (\Phi(x))^{-1} = k^{-1} \in K$. Thus, $x^{-1} \in \Phi^{-1}(K)$. Since $\Phi(x^{-1}y) = \Phi(x^{-1})\Phi(y) = k^{-1}\Phi(y) \in K$, we have $x^{-1}y \in \Phi^{-1}(K)$. Hence, $\Phi^{-1}(K)$ is a subgroup of G by Theorem 1.2.7.

QUESTION 2.7.4 *Let Φ be a group homomorphism from a group G to a group H, and let K be a normal subgroup of H. Prove that $D = \Phi^{-1}(K)$ is a normal subgroup of G.*

Solution: Let $g \in G$. Then $\Phi(g^{-1}Dg) = (\Phi(g))^{-1}\Phi(D)\Phi(g) = (\Phi(g))^{-1}K\Phi(g) = K$. Since $\Phi(g^{-1}Dg) = K$ for each $g \in G$, we conclude that $g^{-1}Dg \subset D$ for each $g \in G$. Thus, D is normal in G by Question 2.6.29.

QUESTION 2.7.5 *Let Φ be a ring homomorphism from a group G to a group H. Suppose that D is a subgroup of G and K is a subgroup of H such that $\Phi(D) = K$. Prove that $\Phi^{-1}(K) = Ker(\Phi)D$.*

Solution: Let $x \in Ker(\Phi)D$. Then $x = zd$ for some $z \in Ker(\Phi)$ and for some $d \in D$. Hence, $\Phi(x) = \Phi(zd) = \Phi(z)\Phi(d) = e_H\Phi(d) = \Phi(d) \in K$. Thus, $Ker(\Phi)D \subset \Phi^{-1}(K)$. Now, let $y \in \Phi^{-1}(K)$. Then $\Phi(w) = y$ for some $w \in G$. Since $\Phi(D) = K$, we have $\Phi(d) = y$ for some $d \in D$. Since G is group, we have $w = ad$ for some $a \in G$. Now, we show that $a \in Ker(\Phi)$. Hence, $y = \Phi(w) = \Phi(ad) = \Phi(a)\Phi(d) = \Phi(a)y$. Thus, $\Phi(a)y = y$. Hence, $\Phi(a) = e_H$. Thus, $a \in Ker(\Phi)$. Hence, $w = ad \in Ker(\Phi)D$. Thus, $\Phi^{-1}(K) \subset Ker(\Phi)D$. Hence, $\Phi^{-1}(K) = Ker(\Phi)D$.

QUESTION 2.7.6 *Let Φ be a group homomorphism from a group G to a group H. Suppose that $\Phi(g) = h$ for some $g \in G$ and for some $h \in H$. Prove that $\Phi^{-1}(h) = \{x \in G : \Phi(x) = h\} = Ker(\Phi)g$. Furthermore, if $Ord(Ker(\Phi)) = n$ and $\Phi(g) = h$, then $Ord(\Phi^{-1}(h)) = n$, i.e., There are exactly n elements in G that map to $h \in H$. Hence, if Φ is*

onto and $Ord(Ker(\Phi)) = n$ and D is a subgroup of H of order m, then $Ord(\Phi^{-1}(D)) = nm$. In particular, if N is a normal subgroup of G of order n and G/N has a subgroup of order m, then $\Phi^{-1}(D)$ is a subgroup of G of order nm.

Solution: We just use a similar argument as in the previous Question. Now, suppose that $Ord(Ker(\Phi)) = n$ and $\Phi(g) = h$. Since $\Phi^{-1}(h) = gKer(\Phi)$, we conclude that $Ord(\Phi^{-1}(h)) = Ord(gKer(\Phi)) = n$.

QUESTION 2.7.7 *Let H be an infinite cyclic group. Prove that H is isomorphic to Z.*

Solution: Since H is cyclic, $H = (a)$ for some $a \in H$. Define $\Phi : H \longrightarrow Z$ such that $\Phi(a^n) = n$ for each $n \in Z$. It is easy to check that Φ is onto. Also, $\Phi(a^n a^m) = \Phi(a^{n+m}) = n + m = \Phi(a^n)\Phi(a^m)$. Hence, Φ is a group homomorphism. Now, we show that Φ is one to one. Suppose that $\Phi(a^n) = \Phi(a^m)$. Then n = m. Thus, Φ is one to one. Hence, Φ is an isomorphism. Thus, $H \cong Z$.

QUESTION 2.7.8 *Let G be a finite cyclic group of order n. Prove that $G \cong Z_n$.*

Solution: Since G is a finite cyclic group of order n, we have $G = (a) = \{a^0 = e, a^1, a^2, a^3, ..., a^{n-1}\}$ for some $a \in G$. Define $\Phi : G \longrightarrow Z_n$ such that $\Phi(a^i) = i$. By a similar argument as in the previous Question, we conclude that $G \cong Z_n$.

QUESTION 2.7.9 *Let k, n be positive integers such that k divides n. Prove that $Z_n/(k) \cong Z_k$.*

Solution: Since Z_n is cyclic, we have $Z_n/(k)$ is cyclic by Theorem 1.2.34(6). Since Ord((k)) = n/k, we have order$(Z_n/(k))$ = k. Since $Z_n/(k)$ is a cyclic group of order k, $Z_n/(k) \cong Z_k$ by the previous Question.

QUESTION 2.7.10 *Prove that Z under addition is not isomorphic to Q under addition.*

Solution: Since Z is cyclic and Q is not cyclic, we conclude that Z is not isomorphic to Q.

QUESTION 2.7.11 *Let Φ be a group homomorphism from a group G to a group H. Prove that Φ is one to one if and only if $Ker(\Phi) = \{e\}$.*

Solution: Suppose that Φ is one to one. Hence, $\Phi(x) = e_H$ iff $x = e_G$ the identity in G. Hence, $Ker(\Phi) = \{e\}$. Now, suppose that $Ker(\Phi) = \{e\}$. Let $x, y \in G$ such that $\Phi(x) = \Phi(y)$. Hence, $\Phi(x)[\Phi(y)]^{-1} = \Phi(x)\Phi(y^{-1}) = \Phi(xy^{-1}) = e_H$. Since $Ker(\Phi) = \{e\}$, we conclude that $xy^{-1} = e_G$ the identity in G. Hence, $x = y$. Thus, Φ is one to one.

QUESTION 2.7.12 *Suppose that G is a finite Abelian group of order n and m is a positive integer such that $gcd(n, m) = 1$. Prove that $\Phi : G \longrightarrow G$ such that $\Phi(g) = g^m$ is an automorphism (group isomorphism) from G onto G.*

Solution: Let $g_1, g_2 \in G$. Then $\Phi(g_1g_2) = (g_1g_2)^m = g_1^m g_2^m$ since G is Abelian. Hence, $\Phi(g_1g_2) = g_1^m g_2^m = \Phi(g_1)\Phi(g_2)$. Thus, Φ is a group homomorphism. Now, let $b \in G$. Since $b^n = e$ and gcd(n,m) = 1 , By Question 2.1.10 we have $b = g^m$ for some $g \in G$. Hence, $\Phi(g) = b$. Thus, Φ is Onto. Now, we show that Φ is one to one. By the previous Question, it suffices to show that $Ker(\Phi) = \{e\}$. Let $g \in Ker(\Phi)$. Then $\Phi(g) = g^m = e$. Thus, $Ord(g)$ divides m. Since $Ord(g)$ divides m and $Ord(g)$ divides n and $gcd(n, m) = 1$, we conclude that $Ord(g) = 1$. Hence, $g = e$. Thus, $Ker(\Phi) = \{e\}$. Hence, Φ is an isomorphism from G Onto G.

QUESTION 2.7.13 *Suppose that G is a finite Abelian group such that G has no elements of order 2. Prove that $\Phi : G \longrightarrow G$ such that $\Phi(g) = g^2$ is a group isomorphism (an automorphism) from G onto G.*

Solution: Since G has no elements of order 2 and 2 is prime, we conclude that 2 does not divide n by Theorem 1.2.31. Hence, n is an odd number. Thus, since $gcd(2, n) = 1$, we conclude that Φ is an isomorphism by the previous Question.

QUESTION 2.7.14 *Let $n = m_1m_2$ such that $gcd(m_1, m_2) = 1$. Prove that $H = Z_{m_1} \oplus Z_{m_2} \cong Z_n$.*

Solution: Since Z_{m_1} and Z_{m_2} are cyclic and $gcd(m_1, m_2) = 1$, By Theorem 1.2.36 we conclude that H is a cyclic group of order $n = m_1m_2$. Hence, $H \cong Z_n$ by Question 2.7.8.

QUESTION 2.7.15 *Is there a nontrivial group homomorphism from Z_{24} onto $Z_6 \oplus Z_2$?*

Solution: No. For suppose that Φ is a group homomorphism from Z_{24} onto $Z_6 \oplus Z_2$. Then by Theorem 1.2.35 we have $Z_{24}/Ker(\Phi) \cong Z_6 \oplus Z_2$. A contradiction since $Z_{24}/Ker(\Phi)$ is cyclic by Theorem 1.2.34(6) and by Theorem 1.2.36 $Z_6 \oplus Z_2$ is not cyclic (observe that $gcd(2,6) = 2 \neq 1$).

QUESTION 2.7.16 *Let G be a group of order $n > 1$. Prove that $H = Z \oplus G$ is never cyclic.*

Solution: Deny. Then H is cyclic. Since Z = (1) and $Ord(G) > 1$, we have H = ((1,g)) for some $g \in G$ such that $g \neq e$. Since $(1, e) \in H$, we have $(1, g)^n = (1, e)$ for some $n \in Z$. Thus, $(n, g^n) = (1, e)$. Hence, $n = 1$. Thus, $g = e$. A contradiction since $g \neq e$. Hence, H is never cyclic.

QUESTION 2.7.17 *Suppose That $G = H \oplus K$ is cyclic such that $Ord(K) > 1$ and $Ord(H) > 1$. Prove that H and K are finite groups.*

Solution: Since G is cyclic, we have H and K are cyclic. We may assume that H is infinite. By Question 2.7.7, $H \cong Z$. Hence, $Z \oplus K$ is cyclic, which is a contradiction by the previous Question.

QUESTION 2.7.18 *Let $G = Z_n \oplus Z_m$ and $d = p^k$ for some prime number p such that d divides both n and m. Prove that G has exactly $d\phi(d) + [d - \phi(d)]\phi(d)$ elements of order d.*

Solution: Since Z_n is cyclic, by Theorem 1.2.14 we have exactly $\phi(d)$ elements of order d in Z_n. Hence, let $g = (z_1, z_2) \in G$ such that Ord(g) = d. Since $d = p^k$ and p is prime and by Theorem 1.2.37 Ord(g) = $lcm(Ord(z_1), Ord(z_2)) = p^k = d$, we conclude that either $Ord(z_1) = d$ and $dz_2 = 0$ or $Ord(z_2) = d$ and $dz_1 = 0$. Hence, if $Ord(z_1) = d$ and $dz_2 = 1$, then $Ord(g) = d$. Thus, there are exactly $d\phi(d)$ elements in D of this kind. If $Ord(z_2) = d$ and $dz_1 = 0$, then $Ord(g) = d$. Hence, we have exactly $d\phi(d)$ elements in G of this kind. If $Ord(z_1) = d$ and $Ord(z_2) = d$, then there are exactly $\phi(d)\phi(d)$ elements of this kind, but this kind of elements has been included twice in the first calculation and in the second calculation. Hence, number of all elements in G of order d is $d\phi(d) + d\phi(d) - \phi(d)\phi(d) = d\phi(d) + [d - \phi(d)]\phi(d)$

QUESTION 2.7.19 *How many elements of order 4 does $G = Z_4 \oplus Z_4$ have ?*

Solution: Since $4 = 2^2$, By the previous Question, number of elements of order 4 in G is $4\phi(4) + [4 - \phi(4)]\phi(4) = [4]2 + [2]2 = 8 + 4 = 12$.

QUESTION 2.7.20 *How many elements of order* 6 *does the group* $G = Z_6 \oplus Z_6$ *have?*

Solution: Let $g = (z_1, z_2) \in G$ such that $Ord(g) = 6$. Since $Ord(g) = lcm(Ord(z_1), Ord(z_2)) = 6$, we conclude that $Ord(z_1) = 6$ and $6z_2 = 0$ or $Ord(z_2) = 6$ and $6z_1 = 0$ or $Ord(z_1) = 2$ and $Ord(z_2) = 3$ or $Ord(z_1) = 3$ and $Ord(z_2) = 2$. Hence, number of elements in G of order 6 is $(6\phi(6) + 6\phi(6) - \phi(6)\phi(6)) + (\phi(2)\phi(3)) + (\phi(3)\phi(2)) = (12 + 12 - 4) + 2 + 2 = 20 + 2 + 2 = 24$.

QUESTION 2.7.21 *How many elements of order* 6 *does* $G = Z_{12} \oplus Z_2$ *have?*

Solution: Let $g = (z_1, z_2) \in G$. Since $Ord(g) = lcm(Ord(z_1), Ord(z_2)) = 6$, we conclude that $Ord(z_1) = 6$ and $6z_2 = 2z_2 = 0$ or $Ord(z_1) = 3$ and $Ord(z_2^2) = 2$. Hence number of elements of order 6 in G is $2\phi(6) + \phi(3)\phi(2) = 4 + 2 = 6$.

QUESTION 2.7.22 *Find the order of* $g = (6, 4) \in G = Z_{24} \oplus Z_{16}$.

Solution: $Ord(g) = lcm(Ord(6), Ord(4)) = lcm(4, 4) = 4$.

QUESTION 2.7.23 *Prove that* $H = Z_8 \oplus Z_2 \ncong G = Z_4 \oplus Z_4$.

Solution: We just observe that G has no elements of order 8, but the element $(1, 0) \in H$ has order equal to 8. Thus, $H \ncong G$.

QUESTION 2.7.24 *Let* Φ *be a group homomorphism from* Z_{13} *to a group* G *such that* Φ *is not one to one. Prove that* $\Phi(x) = e$ *for each* $x \in Z_{13}$.

Solution: Since Φ is not one to one, we have $Ord(Ker(\Phi)) > 1$. Since $Ord(Ker(\Phi)) > 1$ and it must divide 13 and 13 is prime, we conclude that $Ord(Ker(\Phi)) = 13$. Hence, $\Phi(x) = e$ for each $x \in Z_{13}$.

QUESTION 2.7.25 *Let* Φ *be a group homomorphism from* Z_{24} *onto* Z_8. *Find* $Ker(\Phi)$.

Solution: Since $Z_{24}/Ker(\Phi) \cong Z_8$ by Theorem 1.2.35 and $Ord(Z_8) = 8$ and $Ord(Z_{24}) = 24$, we conclude that $Ord(Ker(\Phi)) = 3$. Since Z_{24} is cyclic, by Theorem 1.2.12 Z_{24} has a unique subgroup of order 3. Since $Ker(\Phi)$ is a subgroup of Z_{24} and $Ord(Ker(\Phi)) = 3$, $Ker(\Phi)$ is the only subgroup of Z_{24} of order 3. Hence, we conclude that $Ker(\Phi) = \{0, 8, 16\}$.

QUESTION 2.7.26 *Is there a group homomorphism from Z_{28} onto Z_6?*

Solution: NO. For let Φ be a group homomorphism from Z_{28} onto Z_6. Then by Question 2.7.1 we conclude that 6 divides 28. A Contradiction. Hence, there is no group homomorphism from Z_{28} onto Z_6.

QUESTION 2.7.27 *Let Φ be a group homomorphism from Z_{20} to Z_8 such that $Ker(\Phi) = \{0, 4, 8, 12, 16\}$ and $\Phi(1) = 2$. Find all elements of Z_{20} that map to 2, i.e., find $\Phi^{-1}(2)$.*

Solution: Since $\Phi(1) = 2$, By Question 2.7.6 we have $\Phi^{-1}(2) = Ker(\Phi) + 1 = \{1, 5, 9, 13, 17\}$.

QUESTION 2.7.28 *Let Φ be a group homomorphism from Z_{28} to Z_{16} such that $\Phi(1) = 12$. Find $Ker(\Phi)$.*

Solution: Since Z_{28} is cyclic and $Z_{28} = (1)$ and $\Phi(1) = 12$, we conclude that $\Phi(Z_{28}) = (\Phi(1)) = (12)$. Hence, $Ord(\Phi(Z_{28})) = Ord(\Phi(1)) = Ord(12) = 4$. Since $Z_{28}/Ker(\Phi) \cong \Phi(Z_{28})$ by Theorem 1.2.35 and $Ord(\Phi(Z_{28}) = 4$, we conclude that $Ord(Ker(\Phi)) = 7$. Since Z_{28} is cyclic, Z_{28} has a unique subgroup of order 7 by Theorem 1.2.12. Hence, $Ker(\Phi) = \{0, 4, 8, 12, 16, 20, 24\}$.

QUESTION 2.7.29 *Let Φ be a group homomorphism from Z_{36} to Z_{20}. Is it possible that $\Phi(1) = 2$?*

Solution: NO. because $Ord(\Phi(1)) = Ord(2)$ must divide Ord(1) by Theorem 1.2.34. But since $1 \in Z_{36}$ and $\Phi(1) = 2 \in Z_{20}$, Ord(1) = 36 and Ord(2) = 5. Hence, 5 does not divide 36.

QUESTION 2.7.30 *Find all group homomorphism from Z_8 to Z_6.*

Solution: Since Z_8 is cyclic and $Z_8 = (1)$, a group homomorphism, say,Φ, from Z_8 to Z_6 is determined by $\Phi(1)$. Now, by Theorem 1.2.34 $Ord(\Phi(1) \in Z_6)$ must divide $Ord(1 \in Z_8)$. Also, since $\Phi(1) \in Z_6$,

$Ord(\Phi(1))$ must divide 6. Hence, $Ord(\Phi(1) \in Z_6)$ must divide both numbers 8 and 6. Hence, $Ord(\Phi(1)) = 1$ or 2. Since $0 \in Z_6$ has order 1 and $3 \in Z_6$ is the only element in Z_6 has order 2, we conclude that the following are all group homomorphisms from Z_8 to Z_6 : (1) $\Phi(1) = 0$. (2) $\Phi(1) = 3$.

QUESTION 2.7.31 *Find all group homomorphism from Z_{30} to Z_{20}.*

Solution: Once again, since $Z_{30} = (1)$ is cyclic, a group homomorphism Φ from Z_{30} to Z_{20} is determined by $\Phi(1)$. Now, since $\Phi(1)$ divides both numbers 20 and 30, we conclude that the following are all possibilities for $Ord(\Phi(1))$: 1, 2, 5, 10. By Theorem there are exactly $\phi(1) = 1$ element in Z_{20} of order 1 and $\phi(2) = 1$ element in Z_{20} of order 2 and $\phi(5) = 4$ elements in Z_{20} of order 5 and $\phi(10) = 4$ elements in Z_{20} of order 10. Now, 0 is of order 1, 10 is the only element in Z_{20} of order 2, each element in $\{4, 8, 12, 16\}$ is of order 5, and each element in $\{2, 6, 14, 18\}$ is of order 10. Thus, the following are all group homomorphisms from Z_{30} to Z_{20} : (1) $\Phi(1) = 0$. (2) $\Phi(1) = 10$. (3)$\Phi(1) = 4$. (4)$\Phi(1) = 8$. (5)$\Phi(1) = 12$. (6)$\Phi(1) = 16$. (7)$\Phi(1) = 2$. (8)$\Phi(1) = 6$. (9)$\Phi(1) = 14$. (10) $\Phi(1) = 18$. Hence, there are exactly 10 group homomorphisms from Z_{30} to Z_{20}.

QUESTION 2.7.32 *Let m_1, m_2, m_3,...,m_k be all positive integers that divide both numbers n and m. Prove that number of all group homomorphisms from Z_n to Z_m is $\phi(m_1)+\phi(m_2)+\phi(m_3)+...+\phi(m_k) = gcd(n, m)$.*

Solution: As we have seen in the previous two Questions, a homomorphism Φ from Z_n to Z_m is determined by $\Phi(1)$. Since $Ord(\Phi(1))$ must divide both numbers n and m, we conclude that $Ord(\Phi(1))$ must be m_1 or m_2, or...or m_k. Since Z_m has exactly $\phi(m_1)$ elements of order m_1 and $\phi(m_2)$ elements of order m_2 and...and $\phi(m_k)$ elements of order m_k, we conclude that number of all group homomorphisms from Z_n to Z_m is $\phi(m_1) + \phi(m_2) + ... + \phi(m_k) = gcd(n, m)$.

QUESTION 2.7.33 *Let Φ be a group homomorphism from Z_{30} to Z_6 such that $Ker(\Phi) = \{0, 6, 12, 18, 24\}$. Prove that Φ is onto. Also, find all possibilities for $\Phi(1)$.*

Solution: Since $Z_{30}/Ker(\Phi) \cong \Phi(Z_{30}) \subset Z_6$ by Theorem 1.2.35 and $Ord(Ker(\Phi)) = 5$, we conclude that $Ord(Z_{30}/Ker(\Phi)) = Ord(\Phi(Z_{30}) = 30/5 = 6$. Hence, $\Phi(Z_{30}) = Z_6$. Thus, Φ is onto. Now, since $Z_{30} = (1)$ is cyclic and a group homomorphism from Z_{30} to Z_6 is determined by $\Phi(1)$

and Φ is onto, we conclude $Ord(\Phi(1)) = 6$. Hence, there are $\phi(6) = 2$ elements in Z_6 of order 6, namely, 1 and 5. Thus, all possibilities for $\Phi(1)$ are : (1) $\Phi(1) = 1$. (2)$\Phi(1) = 5$.

QUESTION 2.7.34 *Let Φ be a group homomorphism from G onto H, and suppose that H contains a normal subgroup K such that $[H : K] = n$. Prove that G has a normal subgroup D such that [G:D] = n.*

Solution: Since $\alpha : H \longrightarrow H/K$ such that $\alpha(h) = hK$ is a group homomorphism from H onto H/K, we conclude that $\alpha \circ \Phi$ is a group homomorphism from G onto H/K. Thus, by Theorem 1.2.35 $G/Ker(\alpha \circ \Phi) \cong H/K$. Since $n = [H : K] = Ord(H/K)$, we conclude that $Ord(G/Ker(\alpha \circ \Phi)) = [G : Ker(\alpha \circ \Phi] = n$. Thus, let $D = Ker(\alpha \circ \Phi)$. Then [G : D] = n and D is a normal subgroup of G by Theorem 1.2.35.

QUESTION 2.7.35 *Let Φ be a group homomorphism from G onto Z_{15}. Prove that G has normal subgroups of index 3 and 5.*

Solution: Since Z_{15} is cyclic and both numbers 3, 5 divide 15, Z_{15} has a subgroup, say, H, of order 3 and it has a subgroup, say, K, of order 5. Since Z_{15} is Abelian, H and K are normal subgroups of Z_{15}. Since $[Z_{15} : H] = 5$, by the previous Question we conclude that G has a normal subgroup of index 5. Also, since $[Z_{15} : K] = 3$, once again by the previous Question we conclude that G has a normal subgroup of index 3.

QUESTION 2.7.36 *Let H be a subgroup of G and N be a subgroup of K. Prove that $H \oplus N$ is a subgroup of $G \oplus K$.*

Solution: Let $(h_1, n_1), (h_2, n_2) \in H \oplus N$. Then $(h_1, n_1)^{-1}(h_2, n_2) = (h_1^{-1}, n_1^{-1})(h_2, n_2) = (h_1^{-1}h_2, n_1^{-1}n_2) \in H \oplus N$. Hence, by Theorem 1.2.7 $H \oplus N$ is a subgroup of $G \oplus K$.

QUESTION 2.7.37 *Let H be a normal subgroup of G and N be a normal subgroup of K. Prove that $H \oplus N$ is a normal subgroup of $G \oplus K$.*

Solution: Let $(g, k) \in G \oplus K$. Then $(g, k)^{-1}[H \oplus N](g_1, k_1) = (g^{-1}, k^{-1})[H \oplus N](g, k) = g^{-1}Hg \oplus k^{-1}Nk = H \oplus N$ since $g^{-1}Hg = H$ and$k^{-1}Nk = N$. Thus, $H \oplus N$ is a normal subgroup of $G \oplus K$.

QUESTION 2.7.38 *Let H be a normal subgroup of G such that $[G : H] = n$ and N be a normal subgroup of K such that $[K : N] = m$. Prove that $H \oplus N$ is a normal subgroup of $G \oplus K$ of index nm.*

Solution: Let $\Phi : G \oplus K \longrightarrow G/H \oplus K/N$ such that $\Phi(g,k) = (gH, kN)$. Then clearly that Φ is a group homomorphism from $G \oplus K$ onto $G/H \oplus K/N$ and $Ker(\Phi) = H \oplus N$. Hence, by Theorem 1.2.35 we have $G \oplus K/Ker(\Phi) = G \oplus K/H \oplus N \cong G/H \oplus K/N$. Since [G : H] = n and [K : N] = m, Ord(G/H) = n and Ord(K/N) = m. Hence, $Ord(G/H \oplus K/N) = nm$. Thus, $Ord(G \oplus K/H \oplus N) = nm$. Hence, $[G \oplus K : H \oplus N] = nm$.

QUESTION 2.7.39 *Prove that $Z_4 \oplus Z_8$ has a normal subgroup of index 16.*

Solution: Let $H = \{0\} \subset Z_4$, and let $N = \{0, 4\} \subset Z_8$. Then H is a normal subgroup of Z_4 of index 4 and N is a normal subgroup of Z_8 of index 4. Hence, by the previous Question $H \oplus N$ is a normal subgroup of $G \oplus K$ of index 16.

QUESTION 2.7.40 *Let Φ be a group homomorphism from G onto $Z_8 \oplus Z_6$ such that $Ord(Ker(\Phi)) = 3$. Prove that G has a normal subgroup of order 36.*

Solution: Let H be a normal subgroup of Z_8 of order 4 and let N be a normal subgroup of Z_6 of order 3. Then $H \oplus N$ is a normal subgroup of $Z_8 \oplus Z_6$ of order 12. Now, let $a \in H \oplus N$. Then $Ord(\Phi^{-1}(a)) = Ord(Ker(\Phi)) = 3$ by Question 2.7.6. Hence, since $Ord(\Phi^{-1}(a)) = 3$ for each $a \in H \oplus N$ and $Ord(H \oplus N) = 12$, we conclude that $Ord(\Phi^{-1}(H \oplus N)) = (12)(3) = 36$. Now, by Question 2.7.4 $D = \Phi^{-1}(H \oplus N)$ is a normal subgroup of G. (by a similar argument, one can prove that G has normal subgroups of order 6, 9, 12, 18, 24.)

QUESTION 2.7.41 *Let G be a group of order pq for some prime numbers p, q, $p \neq q$ such that G has a normal subgroup H of order p and a normal subgroup K of order q. Prove that G is cyclic and hence $G \cong Z_{pq}$.*

Solution: Since gcd(p,q) = 1, by Question 2.6.23 we have Ord(HK) = pq. Thus, HK = G. Also, since gcd(p,q) = 1, we conclude that $H \cap K = \{e\}$. Hence, by Theorem 1.2.39 $G \cong H \oplus K$. Since $Ord(H) = p$ and Ord(K) = q, H and K are cyclic groups. Hence, since H and K are cyclic groups and gcd(p,q) = 1, by Theorem 1.2.36 we conclude that $G \cong H \oplus K$ is cyclic. Hence, $G \cong Z_{pq}$ by Question 2.7.8.

QUESTION 2.7.42 *Let G be a group of order 77 such that G has a normal subgroup of order 11 and a normal subgroup of order 7. Prove that G is cyclic and hence $G \cong Z_{77}$.*

Solution: Since Ord(G) = 77 is a product of two distinct prime numbers, the result is clear by the previous Question.

QUESTION 2.7.43 *Prove that $Aut(Z_{125})$ is a cyclic group.*

Solution: Since $Aut(Z_{125}) \cong U(125) = U(5^3)$ by Theorem 1.2.41 and $U(5^3)$ is cyclic by Theorem 1.2.40, we conclude that $Aut(Z_{125})$ is cyclic.

QUESTION 2.7.44 *Let p be an odd prime number and n be a positive integer. Then prove that $U(2p^n)$ is a cyclic group.*

Solution: By Theorem 1.2.38, we have $U(2p^n) \cong U(2) \oplus U(p^n)$. Since $U(2)$ and $U(p^n)$ are cyclic groups by Theorem 1.2.40 and $gcd(Ord(U(2)), Ord(U(p^n))) = gcd(1, (p-1)p^{n-1}) = 1$, we conclude that $U(2p^n) \cong U(2) \oplus U(p^n)$ is cyclic by Theorem 1.2.36.

QUESTION 2.7.45 *Prove that $U(54)$ is a cyclic group.*

Solution: Since $54 = 2(3^3)$, $U(54)$ is cyclic by the previous Question.

QUESTION 2.7.46 *Let p and q be two distinct odd prime numbers and n, m be positive integers. Prove that $U(p^n q^m)$ is never a cyclic group.*

Solution: By Theorem 1.2.38, we have $U(p^n q^m) \cong U(p^n) \oplus U(p^m) \cong Z_{(p-1)p^{n-1}} \oplus Z_{(q-1)q^{m-1}}$ by Theorem 1.2.40. Since $(p-1)p^{n-1}$ and $(q-1)q^{m-1}$ are even numbers, we conclude that $gcd((p-1)p^{n-1}, (q-1)q^{m-1}) \neq 1$. Hence, by Theorem 1.2.36 $U(p^n q^m)$ is not cyclic.

QUESTION 2.7.47 *Let n be a positive integer. Prove that up to isomorphism there are finitely many groups of order n.*

Solution : Let G be a group of order n. By Theorem 1.2.42, G is isomorphic to a subgroup of S_n. Hence, number of groups of order n up to isomorphism equal number of all subgroups of S_n of order n. Since S_n is a finite group, S_n has finitely many subgroups of order n.

QUESTION 2.7.48 *Let p be a prime number in Z. Suppose that H is a subgroup of Q^* under multiplication such that $p \in H$. Prove that there is no group homomorphism from Q under addition onto H. Hence, $Q \ncong H$.*

Solution: Deny. Then there is a group homomorphism Φ from Q onto H. Since $p \in H$, there is an element $x \in Q$ such that $\Phi(x) = p$. Hence, $p = \Phi(x) = \Phi(x/2+x/2) = \Phi(x/2)\Phi(x/2) = (\Phi(x/2))^2$. Since $\Phi(x/2)^2 = p$, we conclude $\Phi(x/2) = \sqrt{p}$. A contradiction, since p is prime and $\Phi(x/2) \in H \subset Q^*$ and $\sqrt{p} \notin Q$.

QUESTION 2.7.49 *Prove that Q under addition is not isomorphic to Q^* under multiplication.*

Solution: This result is now clear by the previous Question.

QUESTION 2.7.50 *Let H be a subgroup of C^* under multiplication, and let Φ be a group homomorphism from Q under addition to H. Then prove that there is a positive real number $a \in H$ such that $\Phi(n/m) = a^{n/m}$ for each $n/m \in Q$, n and m are integers.*

Solution: Now $\Phi(1) = a \in H$. Let n be a positive integer. Then $\Phi(n) = \Phi(1 + 1 + ... + 1) = \Phi(1)\Phi(1)...\Phi(1) = \Phi(1)^n = a^n$. Also, $a = \Phi(1) = \Phi(n(1/n)) = \Phi(1/n+1/n+...+1/n) = \Phi(1/n)\Phi(1/n)...\Phi(1/n) = \Phi(1/n)^n$. Since $\Phi(1/n)^n = a$, we have $\Phi(1/n) = \sqrt[n]{a}$. Now, if n is a negative number, then since $1 = \Phi(0) = \Phi(n - n)$ and $\Phi(-n) = a^{-n}$ we have $\Phi(n) = a^n$. Also, if n is negative, then $\Phi(1/n) = a^{1/n}$. Hence, if n and m are integers and $m \neq 0$, then $\Phi(n/m) = a^{n/m}$. Since $\Phi(1/2) = \sqrt{a}$, we conclude that a is a positive real number.

QUESTION 2.7.51 *Prove that Q under addition is not isomorphic to R^* under multiplication.*

Solution : By the previous Question, a group homomorphism Φ from Q to R^* is of the form $\Phi(x) = a^x$ for each $x \in Q$ for some positive real number a. Since $a^x \geq 0$ for each $x \in Q$, There is no element in Q maps to -1. Hence, $Q \ncong R^*$.

QUESTION 2.7.52 *Prove that Q under addition is not isomorphic to R^+ (the set of all nonzero positive real numbers) under multiplication.*

Solution: Deny. Then Φ is an isomorphism from Q onto R^+. Hence, by Question 2.7.50 there is a positive real number a such that $\Phi(n/m) = a^{n/m}$. Now, suppose that $a = \pi$. Then there is no $x \in Q$ such that $a^x = \pi^x = 2$. Thus, Φ is not onto. Hence, assume that $a \neq \pi$. Then there is no $x \in Q$ such that $a^x = \pi$. Thus, once again, Φ is not onto. Hence, $Q \ncong R^+$.

QUESTION 2.7.53 *Give an example of a non-Abelian group of order* 48.

Solution: Let $G = S_4 \oplus Z_2$. Then $Ord(G) = 48$. Since S_4 is a non-Abelian group, G is non-Abelian.

QUESTION 2.7.54 *Let Φ be a group homomorphism from a group G into a group H. If D is a subgroup of H, then $Ker(\Phi)$ is a subgroup of $\Phi^{-1}(D)$. In particular, if K is a normal subgroup of G and D is a subgroup of G/K, then K is a subgroup of $\Phi^{-1}(D)$ where $\Phi : G \longrightarrow G/K$ given by $\Phi(g) = gK$.*

Solution : Let D be a subgroup of H. Since $e_H \in D$, we have $\Phi(b) = e_H$ for each $b \in Ker(\Phi)$. Thus, $Ker(\Phi) \subset \Phi^{-1}(D)$. The remaining part is now clear.

QUESTION 2.7.55 *Let G be a group and H be a cyclic group and Φ be a group homomorphism from G onto H. Is $\Phi^{-1}(H) = G$ an Abelian group?*

Solution: No. Let $G = S_4$, and $K = A_4$. Now, $H = G/K$ is a cyclic group of order 2 and Φ from G into H given by $\Phi(g) = gK$ is a group homomorphism from G onto H. Now, $\Phi^{-1}(H) = G = S_4$ is not Abelian.

QUESTION 2.7.56 *Let H be a subgroup of a finite group G. Prove that $C(H)$ is a normal subgroup of $N(H)$ and $Ord(N(H)/C(H))$ divides $Ord(Aut(H))$. In particular, prove that if H is a normal subgroup of G, then Ord(G/C(H)) divides Ord(Aut(H)).*

Solution : We know that $C(H)$ is a subgroup of G. By the definitions $C(H) \subset N(H)$. Now, let $g \in N(H)$. We need to show that $g^{-1}C(H)g \subset C(H)$. Let $c \in C(H)$. We need to show that $g^{-1}cg \in C(H)$. Hence, let $h \in H$. We show that $(g^{-1}cg)h = h(g^{-1}cg)$. Now, since H is normal in N(H), we have $gh = fg$ for some $f \in H$. Hence, $g^{-1}f = hg^{-1}$. Since $gh = fh$ and $g^{-1}f = hg^{-1}$ and $cf = fc$, we have $g^{-1}cgh = g^{-1}cfg = g^{-1}fcg = hg^{-1}cg$. Thus, $g^{-1}cg \in C(H)$. Hence, $C(H)$ is normal in N(H). Let α be a map from $N(H)$ to Aut(H) such that $\alpha(x) = \Phi_x$ for each $x \in N(H)$, where Φ_x is an automorphism from H onto H such that $\Phi_x(h) = x^{-1}hx$ for each $h \in H$. It is easy to check that α is a group homomorphism from $N(H)$ to $Aut(H)$. Now, $Ker(\alpha) = \{y \in N(H) : \Phi_y = \Phi_e\}$. But $\Phi_y = \Phi_e$ iff $y^{-1}hy = e$ for each $h \in H$ iff $hy = yh$

for each $h \in H$. Thus, $Ker(\alpha) = C(H)$. Hence, by Theorem 1.2.35 we have $N(H)/C(H) \cong Image(\alpha)$. But Image($\alpha$) is a subgroup of $Aut(H)$. Thus, Ord(Image(α)) divides $Ord(Aut(H))$. So, since $N(H)/C(H) \cong Image(\alpha)$, we have $Ord(N(H)/C(H))$ divides $Ord(Aut(H))$. For the remaining part, just observe that if H is normal in G, then $N(H) = G$.

QUESTION 2.7.57 *Let p be a prime number > 3. We know that Z_p^* under multiplication modulo p is a cyclic group of order $p-1$. Let $H = \{a^2 : a \in Z_p^*\}$. Prove that H is a subgroup of Z_p^* such that $[Z_p^* : H] = 2$.*

Solution : Let $\Phi : Z_p^* \longrightarrow Z_p^*$ such that $\Phi(a) = a^2$. It is trivial to check that Φ is a group homomorphism. Clearly $\Phi(Z_p^*) = H$. Thus, H is a subgroup of Z_p^*. Now, $Ker(\Phi) = \{a \in Z_p^* : a^2 = 1\}$. Since $2 \mid p-1$ and Z_p^* is cyclic, there are exactly two elements, namely 1 and $p-1$ in Z_p^* whose square is 1. Thus $Ker(\Phi) = \{1, p-1\}$. Hence, by Theorem 1.2.35 $Z_p^*/Ker(\Phi) \cong \Phi(Z_p^*) = H$. Thus, $Ord(H) = (p-1)/2$. Hence, $[Z_p^* : H] = 2$

QUESTION 2.7.58 *Let p be a prime number > 3, and let $H = \{a^2 : a \in Z_p^*\}$. Suppose that $p-1 \notin H$. Prove that if $a \in Z_p^*$, then either $a \in H$ or $p - a \in H$.*

Solution : By the previous Question, since H is a subgroup of $G = Z_p^*$ and $[G : H] = 2$, we conclude that the group G/H has exactly two elements. Since $p-1 \notin H$, we conclude that H and $(p-1)H = -H$ are the elements of G/H. Now, let $a \in Z_p^*$ and suppose that $a \notin H$. Hence, $aH \neq H$. Thus,$aH = (p-1)H = -H$. Hence, $H = -H - H = -aH = (p-a)H$. Thus, $p - a \in H$.

2.8 Sylow Theorems

QUESTION 2.8.1 *Let H be a Sylow p-subgroup of a finite group G. We know that (the normalizer of H in G) $N(H) = \{x \in G : x^{-1}Hx = H\}$ is a subgroup of G. Prove that H is the only Sylow p-subgroup of G contained in $N(H)$.*

Solution: Let $h \in H$. Then $h^{-1}Hh = H$. Hence, $h \in N(H)$. Thus, $H \subset N(H)$. Now, we show that H is the only Sylow p-subgroup of G contained in $N(H)$. By the definition of $N(H)$, we observe that H is a normal subgroup of $N(H)$. Hence, H is a normal Sylow p-subgroup of $N(H)$. Thus, by Theorem 1.2.46, we conclude that H is the only Sylow p-subgroup of G contained in $N(H)$.

QUESTION 2.8.2 *Let H be a Sylow p-subgroup of a finite group G. Let $x \in N(H)$ such that $Ord(x) = p^n$ for some positive integer n. Prove that $x \in H$.*

Solution: Since $Ord(x) = p^n$, $Ord((x)) = p^n$. Since $N(H)$ is a group (subgroup of G) and $x \in N(H)$ and $Ord((x)) = p^n$, by Theorem 1.2.44 (x) is contained in a Sylow p-subgroup of N(H). By the previous Question H is the only Sylow p-subgroup of G contained in $N(H)$. Hence, $x \in H$.

QUESTION 2.8.3 *Let G be a group of order p^2 . Prove that G is Abelian.*

Solution: Since $Ord(G) = p^2$, by Theorem 1.2.47 we have $Ord(Z(G)) = p$ or p^2. If $Ord(Z(G)) = p^2$, then G is Abelian. Thus, assume that $Ord(Z(G)) = p$. Hence, $Ord(G/Z(G)) = p$. Thus, $G/Z(G)$ is cyclic. Hence, G is Abelian by Question 2.6.6.

QUESTION 2.8.4 *Let G be a non-Abelian group of order* 36*. Prove that G has more than one Sylow 2-subgroup or more than one Sylow 3-subgroup.*

Solution: Deny. Since $36 = 2^2 3^2$, G has exactly one Sylow 3-subgroup, say, H, and it has exactly one Sylow 2-subgroup, say, K. Thus, H and K are normal subgroups of G by Theorem 1.2.46. Since $Ord(H) = 3^2 = 9$ and $Ord(K) = 2^2 = 4$ and gcd(4,9) = 1, we have $H \cap K = \{e\}$ and $Ord(HK) = 36 = Ord(G)$ by Question 2.6.23. Hence, HK = G and by Theorem 1.2.39 we have $G \cong H \oplus K$. Since $Ord(H) = 3^2 = 9$ and $Ord(K) = 2^2 = 4$, we conclude that H and K are Abelian groups by the previous Question. Thus, $G \cong H \oplus K$ is Abelian. A contradiction since G is a non-Abelian group by the hypothesis.

QUESTION 2.8.5 *Let G be a group of order* 100*. Prove that G has a normal subgroup of order* 25*.*

Solution: Since $Ord(G) = 100 = 2^2 5^2$, we conclude that G has a Sylow 5-subgroup, say, H. Then $Ord(H) = 25$. Let n be the number of all Sylow 5-subgroups. Then 5 divides (n-1) and n divides $Ord(G) = 100$ by Theorem 1.2.45. Hence, $n = 1$. Thus, H is the only Sylow 5-subgroup of G. Hence, H is normal by Theorem 1.2.46.

QUESTION 2.8.6 *Let G be a group of order* 100*. Prove that G has a normal subgroup of order* 50*.*

Solution:Since 2 divides 100, G has a subgroup, say, K, of order 2 by Theorem 1.2.43. By the previous Question, G has a normal subgroup of order 25, say, H. Hence, HK is a subgroup of G by Question 2.6.16. Since gcd(2,25) = 1, Ord(HK) = 50 by Question 2.6.23. Thus, $[G : HK] = 2$. Hence, HK is normal by Question 2.6.1.

QUESTION 2.8.7 *Let G be a group such that $Ord(G) = pq$ for some primes $p < q$ and p does not divide $q - 1$. Prove that $G \cong Z_{pq}$ is cyclic.*

Solution: Let n be the number of all Sylow q-subgroups and let m be the number of all Sylow p-subgroups. Then n divides pq and q divides $n-1$ and m divides pq and p divides $m-1$. Since $p < q$, we conclude that $n = 1$. Also, since p does not divide $q - 1$, $m = 1$. Hence, G has exactly one Sylow q-subgroup, say, H and it has exactly one Sylow p-subgroup, say, K. Thus, H and K are normal subgroups of G by Theorem 1.2.46. Since gcd(p,q) = 1, Ord(HK) = pq = Ord(G) and $H \cap K = \{e\}$ by Question 2.6.23. Thus, $G \cong H \oplus K$ by Theorem 1.2.39. Since Ord(H) = q and Ord(K) = p, we conclude that H and K are cyclic and hence $G \cong H \oplus K$ is cyclic. Since G is a cyclic group of order pq, we conclude that $G \cong Z_{pq}$ is cyclic by Question 2.7.8.

QUESTION 2.8.8 *Let G be a group of order 35. Prove that G is a cyclic group and $G \cong Z_{35}$.*

Solution: Let p = 5 and q = 7. Then $Ord(G) = pq$ such that $p < q$ and p does not divide $q - 1$. Hence, $G \cong Z_{35}$ is cyclic by the previous Question.

QUESTION 2.8.9 *Let G be a noncyclic group of order 57. Prove that G has exactly 38 elements of order 3.*

Solution: Since $57 = (3)(19)$ and 19 does not divide $3 - 1$, by Theorem 1.2.45 G has exactly one Sylow 19-subgroup, say, H. Let $a \in G$ such that $a \neq e$. Since $Ord(a)$ divides $Ord(G) = 57 = (3)(19)$ and G is not cyclic and $a \neq e$, we conclude that the possibilities for $Ord(a)$ are : 3, 19. Since H is the only Sylow 19-subgroup of order 19, we have exactly 18 elements in G of order 19. Hence, there are exactly 38 elements in G of order 3.

QUESTION 2.8.10 *Let G be a group of order 56. Prove that H has a proper normal subgroup, say, H, such that $H \neq \{e\}$.*

Solution: Since $56 = 72^3$, we conclude that G has a Sylow 7-subgroup, say, H, and it has a Sylow 2-subgroup, say, K, by Theorem 1.2.43. If H is the only Sylow 7-subgroup of G, then by Theorem 1.2.46 we conclude that H is normal and we are done. Hence, let n be the number of all Sylow 7-subgroups of G such that $n > 1$. Since n divides 56 and 7 divides $n-1$ and $n > 1$, we conclude that $n = 8$. Since each non identity element in a Sylow 7-subgroup of G has order 7, we conclude that there are (8)(6) = 48 elements in G of order 7. Since there are exactly 48 elements in G of order 7 and K is a Sylow 2-subgroup of order 8, we conclude that K is the only Sylow 2-subgroup of G. Thus, K is normal by Theorem 1.2.46.

QUESTION 2.8.11 *Let G be a group of order* 105*. Prove that it is impossible that $Ord(Z(G)) = 7$.*

Solution: Deny. Hence, Ord(Z(G)) = 7. Then Ord(G/Z(G)) = 15. Since 15 = (3)(5) and 3 does not divide $5 - 1 = 4$, by Question 2.8.7 we conclude that $G/Z(G)$ is cyclic. Hence, G is Abelian by Question 2.6.6. Hence, Z(G) = G, a contradiction. Thus, it is impossible that Ord(Z(G)) = 7.

QUESTION 2.8.12 *Let G be a group of order 30. Prove that G has an element of order* 15*.*

Solution: Since 30 = (2)(3)(5), by Theorem 1.2.43 there is a subgroup of order 2 and a subgroup of order 3 and a subgroup of order 5. Let n be the number of all subgroups of G of order 3. Then by Theorem 1.2.45 we conclude that either $n = 1$ or $n = 10$. Suppose that $n = 1$. Let H be the subgroup of G of order 3. Then H is normal by Theorem 1.2.46. Since $Ord(G/H) = 10 = (2)(5)$, by Theorem 1.2.45 we conclude that G/H has exactly one subgroup of order 5. Hence, by Question 2.7.6 , we conclude that G has a subgroup, say, D, of order 15. Since 15 = (3)(5) and 3 does not divide $5 - 1$, by Question 2.8.7 we conclude that D is cyclic. Hence, there is an element in G of order 15. Now, assume that $n = 10$. Let m be the number of all subgroups of G of order 5. Then by Theorem 1.2.45 we conclude that either $m = 1$ or $m = 6$. Since n = 10, there are exactly (10)(2) = 20 elements of order 3. Hence, $m = 1$, for if $m = 6$, then there are exactly (6)(4) = 24 elements of order 5, which is impossible since Ord(G) = 30 and there are 20 elements of order 3. Let K be the subgroup of G of order 5. Then by Theorem 1.2.46 we conclude that K is normal. Since $Ord(G/K) = 6$, by Theorem 1.2.45 we conclude that G/K has a subgroup of order 3. Hence, by Question 2.7.6 we conclude

that G has a subgroup, say, L, of order 15. Thus, as mentioned earlier in the solution G has an element of order 15.

QUESTION 2.8.13 *Let G be a group of order* 30*. Prove that G has exactly one subgroup of order* 3 *and exactly one subgroup of order* 5*.*

Solution: Since $30 = (2)(3)(5)$, by Theorem 1.2.43 G has a subgroup of order 2 and a subgroup of order 3 and a subgroup of order 5. Let n be the number of all subgroups of G of order 3, and let m be the number of all subgroups of G of order 5. By Theorem 1.2.45 we conclude that either $n = 1$ or $n = 10$ and either $m = 1$ or $m = 6$. Suppose that $n = 10$. Then G has exactly $(10)(2) = 20$ elements of order 3. Since by the previous Question G has an element of order 15, we conclude by Theorem 1.2.14 that G has at least $\phi(15) = 8$ elements of order 15. Since Ord(G) = 30 and there are 20 elements of order 3 and 8 elements of order 15, we conclude that there are no subgroups of G of order 5, a contradiction. Hence, $n = 1$. Now, suppose that $m = 6$. By an argument similar to the one just given, we will reach to a contradiction. Hence, we conclude that $m = 1$.

QUESTION 2.8.14 *Let G be a group of order 30. Prove that G has a normal subgroup of order* 3 *and a normal subgroup of order* 5*.*

Solution: By the previous Question there are exactly one Sylow 3-subgroup of G ,say, H, and exactly one Sylow 5-subgroup of G,say, K. Hence, by Theorem 1.2.46 we conclude that H and K are normal in G.

QUESTION 2.8.15 *Let G be a group of order* 60 *such that G has a normal subgroup of order* 2*. Prove that G has a normal subgroup of order* 6 *and a normal subgroup of order* 10 *and a normal subgroup of order 30.*

Solution: Let H be a normal subgroup of G of order 2. Then G/H is a group of order 30. Hence, by the previous Question G/H has a normal subgroup of order 3, say , K. Thus, by Question 2.7.6 G has a normal subgroup of order 6. Since G/H has a normal subgroup of order 5, by an argument similar to the one just given we conclude that G has a normal subgroup of order 10. Also, by the previous Question G/H has a normal subgroup of order 5, say, D. Hence, by Question 2.7.6 KD is a normal subgroup of G/H. Since gcd(3,5) = 1, we conclude that $Ord(KD) = 15$. Thus, by Question 2.7.6 we conclude that G has a normal subgroup of order 30.

QUESTION 2.8.16 *Let G be a group of order* 60 *such that G has a normal subgroup of order* 2*. Prove that G has a subgroup of order* 20 *and a subgroup of order* 12*.*

Solution: By the previous Question G has a normal subgroup of order 10, say, H. Hence, $Ord(G/H) = 6$. Since $6 = (2)(3)$, by Theorem 1. 2.43 G/H has a subgroup of order 2. Hence, by Question 2.7.6 G has a subgroup of order 20. Also, by the previous Question G has a normal subgroup of order 6, say, K. Since $Ord(G/K) = 10$ and $10 = (2)(5)$, by Theorem 1.2.43 G/K has a subgroup of order 2. Thus, by Question 2.7.6 we conclude that G has a subgroup of order 12.

QUESTION 2.8.17 *Let G be a group of order* 60 *such that G has a normal subgroup of order* 2*. Prove that G has a cyclic subgroup of order* 30*, that is, show that G has an element of order* 30*.*

Solution: Let K be a normal subgroup of G of order 2. Set $H = G/K$. Since $Ord(H) = 30$, By Question 2.8.12 H has an element a of order 15. Hence, $D = (a)$ is a subgroup of H of order 15. Thus, by Question 2.7.6 G has a subgroup, V, of order 30 and by Question 2.7.54 $K \subset V$. By Question 2.8.12 V has an element m of order 15. Thus, $M = (m)$ is a subgroup of V of order 15. Since [V : M] = 2, by Question 2.6.1 M is a normal subgroup of V. Since K is normal in G and $K \subset V$, K is a normal subgroup of V. Since gcd(2,15) = 1, $K \cap M = \{e\}$. Since K, M are Abelian normal subgroups of V and $K \cap M = \{e\}$, by Question 2.6.31 KM is an Abelian group. Hence, let $k \in K$ such that Ord(k) = 2. Since K = (k) and M = (m) and KM is Abelian, we have km = mk. Since mk = km and gcd(2,15) = 1, by Question 2.1.14 Ord(km) = 30. Thus, G has a cyclic subgroup of order 30, namely (km).

QUESTION 2.8.18 *Let G be a group of order* 345*. Prove that G is cyclic.*

Solution : Since $345 = (3)(5)(23)$, by Theorem 1.2.43 there are subgroups of G of order 3 and 5 and 23. Let H be a subgroup of G of order 23. By Theorem 1.2.45, we conclude that H is the only subgroup of G of order 23. Thus, by Theorem 1.2.46, H is normal in G. Hence, by Question 2.7.56 we have $Ord(G/C(H))$ divides $Ord(Aut(H))$. By Theorem 1.2.41 we have Ord(Aut(H)) = Ord(U(23)) = 22. Thus, $Ord(G/C(H))$ divides 22. Since $Ord(G/C(H))$ divides both numbers 365 and 22, we conclude that $Ord(G/C(H)) = 1$. Hence, $C(H) = G$. Hence, by the definition

of $C(H)$ we conclude that $C(H) = G$ means that every element in H commute with every element in G. Hence, $H \subset Z(G)$. Thus, Ord(Z(G)) $\geq$ 23. Hence, $Ord(G/Z(G)) = 1$ or 3 or 5 or 15. In each case, we conclude that $G/Z(G)$ is cyclic. Thus, by Question 2.6.6, G must be Abelian. Now, since G has subgroups of order 3 and 5 and 23, G has an element a of order 3 and an element of b of order 5 and an element c of order 23. Since a, b, c commute with each other , by Question 2.1.14 Ord(abc) = Ord(a(bc)) = Ord((ab)c) = (3)(5)(23) = 345. Thus, $G = (abc)$ is cyclic.

QUESTION 2.8.19 *let H, K be two distinct Sylow p-subgroups of a finite group G. Prove that HK is never a subgroup of G.*

Solution: Since H and K are Sylow p-subgroups of G, we conclude $Ord(H) = Ord(K) = p^n$ such that p^{n+1} does not divide Ord(G). Since H and K are distinct, $Ord(H \cap K) = p^m$ such that $0 \leq m < n$. Hence, by Theorem 1.2.48 we conclude $Ord(HK) = p^n p^n / p^m = p^{2n-m} > p^n$. Since order of any subgroup of G must divide Ord(G) and p^{2n-m} does not divide Ord(G), HK is not a subgroup of G.

QUESTION 2.8.20 *Let H be a subgroup of order p (prime) of a finite group G such that $p^2 > Ord(G)$. Prove that H is the only subgroup of G of order p and hence it is normal in G.*

Solution: Suppose that there is another subgroup, say, K, of G of order p. Hence, $H \cap K = \{e\}$. By Theorem 1.2.48, $Ord(HK) = p^2/1 = p^2 > Ord(G)$ which is impossible since $HK \subset G$. Thus, H is the only subgroup of order p of G. Since $p^2 > Ord(G)$, we conclude that p^2 does not divide Ord(G). Thus, H is a Sylow p-subgroup of G. Hence, by Theorem 1.2.46, we conclude that H is normal in G.

QUESTION 2.8.21 *Let G be a group of order* 46 *such that G has a normal subgroup of order* 2*. Prove that G is cyclic, that is, $G \cong Z_{46}$.*

Solution: Since 46 = (2)(23). By Theorem 1.2.43, G has a Sylow 23-subgroup ,H, of G. By Theorem 1.2.45, we conclude that H is the only subgroup of G of order 23. By Theorem 1.2.46, H is normal in G. By hypothesis, let K be a normal subgroup of G of order 2. Hence, $H \cap K = \{e\}$. By Theorem 1.2.48 we have $HK = G$. Since $H \cap K = \{e\}$ and $HK = G$ and H, K are normal in G, by Theorem 1.2.39, $G \cong H \oplus K$. But $K \cong Z_2$ and $H \cong Z_{23}$. Hence, $G \cong Z_2 \oplus Z_{23}$. Thus, by Theorem 1.2.36, G is a cyclic group of order 46. Hence, by Question 2.7.8 we have $G \cong Z_{46}$.

QUESTION 2.8.22 *Let G be a group of order p^n for some prime number p such that for each $0 \leq m \leq n$ there is exactly one subgroup of G of order p^m. Prove that G is cyclic.*

Solution: Let $x \in G$ of maximal order. Then $Ord(x) = p^k$ for some $1 \leq k \leq n$. Now, let $y \in G$. Then $Ord(y) = p^i$ for some $i \leq k$. Since $Ord((y)) = p^i$ and G has exactly one subgroup of order p^i and the subgroup (x) of G, being cyclic, has a subgroup of order p^i, we conclude that $(y) \subset (x)$. Hence, $y \in (x)$. Thus, $G \subset (x)$. Hence, G = (x) is cyclic.

QUESTION 2.8.23 *Let G be a finite Abelian group. Show that A Sylow-p-subgroup of G is unique.*

Solution: Let H be a Sylow-p-subgroup of G. Since G is Abelian, we conclude that H is normal. Hence H is the only Sylow-p-subgroup of G by Theorem 1.2.46

QUESTION 2.8.24 *Let G be a group of order p^2q, where p and q are distinct prime numbers, p does not divide $q-1$, and q does not divide p^2-1. Show that G is Abelian.*

Solution : Let n_p be the number of Sylow-p-subgroups and n_q be the number of Sylow-q-subgroups. Then since q does not divide p^2-1 and p does not divide $q-1$, by Theorem 1.2.45 we conclude that $n_p = n_q = 1$. Let H be a Sylow-p-subgroup and K be a Sylow-q-subgroup. Then H and K are both normal in G by Theorem 1.2.46. Since $H \cap K = \{e\}$ and $Ord(G) = p^2q$, we conclude that $G \cong H \oplus K$. Since q is prime, K is cyclic and hence Abelian. Also, since p is prime and $Ord(H) = p^2$, we conclude that H is Abelian by Question 2.8.3.

2.9 Simple Groups

QUESTION 2.9.1 *Prove that there is no simple groups of order* $300 = (2^2)(3)(5^2)$.

Solution : Let G be a group of order 300. Let n_5 be the number of Sylow-5-subgroups of G. Then by Theorem 1.2.45 we have $n_5 = 1$ or $n_5 = 6$. If $n_5 = 1$, then a Sylow-5-subgroup of G is normal in G by Theorem 1.2.46, and hence G is not simple. Hence assume that $n_5 = 6$. Since 25 does not divide $n_5 - 1$, by Theorem 1.2.51 we conclude that there are two distinct Sylow-5-subgroups H and K of G, such that

$Ord(H \cap K) = 5$ and $HK \subset N(H \cap K)$. Again by Theorem 1.2.51 we have $Ord(N(H \cap K)) > Ord(HK) = Ord(H)Ord(K)/Ord(H \cap K) = (25)(25)/5 = 125$. So, let $m = Ord(N(H \cap K))$. Since $m > 125$ and m divides 300, we conclude that $m = 150$ or $m = 300$. If $m = 300$, then $H \cap K$ is normal in G, and since $Ord(H \cap K) = 5$, we conclude that G is not simple. Thus assume that $m = 150$. Hence $[G : N(H \cap K)] = 2$. Since $n_5 \neq 1$, we conclude that G is non-Abelian (see Question 2.8.23) and hence if G is simple, then G is isomorphic to a subgroup of A_2 by Theorem 1.2.57 which is clearly impossible because $Ord(G) = 300$ where $Ord(A_2) = 1$.

QUESTION 2.9.2 *Prove that there is no simple groups of order* 500.

Solution : Since $500 = 2(125)$ and 125 is an odd number, we conclude that there is no simple groups of order 500 by Theorem 1.2.55.

QUESTION 2.9.3 *Show that there is no simple groups of order* $396 = (2^2)(3^2)(11)$.

Solution : Let G be a group of order 396. Let n_{11} be the number of Sylow-11-subgroups. Then by Theorem 1.2.45 we have $n_{11} = 1$ or $n_{11} = 12$. If $n_{11} = 1$, then a Sylow-11-subgroup of G is normal in G by Theorem 1.2.46, and hence G is not simple. Thus assume that $n_{11} = 12$. Let H be a Sylow-11-subgroup of G. Then by Theorems 1.2.49 and 1.2.54 we conclude that $12 = n_{11} = [G : N(H)]$. Thus $Ord(N(H)) = Ord(G)/12 = 33$. Hence $N(H)$ is cyclic by Question 2.8.7. Thus G has an element of order 33. Now since $n_{11} \neq 1$, we conclude that G is non-Abelian. Since $N(H)$ is a subgroup of G and $[G : N(H)] = 12$, if G is simple, then we conclude that G is isomorphic to a subgroup of A_{12} by Theorem 1.2.57. But A_{12} does not have an element of order 33, for if $\beta \in A_{12}$ of order 33, then by Theorem 1.2.22, β is a product of DISJOINT cycles of length 11 and 3, which is clearly impossible.

QUESTION 2.9.4 *Show that there is no simple groups of order* $525 = (3)(5^2)(7)$.

Solution : Let G be a group of order 525. Let n_7 be the number of Sylow-7-subgroups of G. Then by Theorem 1.2.45 we have $n_7 = 1$ or $n_7 = 15$. If $n_7 = 1$, then a Sylow-7-subgroup of G is normal in G by Theorem 1.2.46, and hence G is not simple. Hence assume that

$n_7 = 15$. Let H be a Sylow-7-subgroup of G. Thus by Theorems 1.2.54 and 1.2.49, we conclude that $15 = n_7 = [G : N(H)]$. Hence $N(H) = Ord(G)/15 = 35$. Thus $N(H)$ is cyclic (and hence Abelian) by Question 2.8.7. Now let K be a subgroup of $N(H)$ of order 5. Since $N(H)$ is Abelian, $N(H) \subset N(K)$. Also, since K is a 5-subgroup of G, K is contained in a Sylow-5-subgroup of G by Theorem 1.2.44. Hence there is a Sylow-5-subgroup, say D, such that $K \subset D$. Since $Ord(D) = 5^2$, we conclude that D is Abelian by Question 2.8.3. Thus $D \subset N(K)$. Since $N(H) \subset N(K)$ and $D \subset N(K)$, we conclude that $Ord(N(K)) \geq (5)(35) = 175$. Thus $m = [G : N(K)] \leq 3$. Hence if G is simple, then G is isomorphic to a subgroup of A_m, which is impossible because $m \leq 3$ and $Ord(G) > 3!/2 = Ord(A_3)$.

QUESTION 2.9.5 *Let G be a finite simple group and suppose that G has two subgroups K and H such that $[G : H] = q$ and $[G : K] = p$ where q, p are prime numbers. Show that $Ord(H) = Ord(K)$.*

Solution : Since G is finite, we need only to show that $p = q$. Hence assume that $p > q$. By Theorem 1.2.56 there is a group homomorphism Φ from G into S_q such that $Ker(\Phi) = \{e\}$ (because G is simple). Hence G is isomrphic to a subgroup of S_q, which is impossible since $p > q$, p divides $Ord(G)$ and p does not divide $q!$. Thus $p = q$, and hence $Ord(H) = Ord(K)$.

QUESTION 2.9.6 *Show that A_5 cannot contain subgroups of order 30 or 20 or 15.*

Solution : Suppose that A_5 has a subgroup H of order 30 20 or 15. Then $[G : H] = 2$ or 3 or 4. Since A_5 is non-Abelian simple group (see Theorem **??**), by Theorem 1.2.57 we conclude that A_5 is isomorphic to a subgroup of A_2 or A_3 or A_4, which is impossible since G has more elements than A_2 or A_3 or A_4.

QUESTION 2.9.7 *Show that a simple group of order 60 has a subgroup of order 10 and a subgroup of order 6.*

Solution : Let G be a simple group of order 60. Write $60 = (2^2)(3)(5)$. Let n_5 be the number of Sylow-5-subgroups, n_3 be the number of Sylow-3-subgroups. By Theorem 1.2.45 we conclude that $n_5 = 6$. Let H be a Sylow-5-subgroup. Then by Theorems 1.2.49 and 1.2.54, we conclude that $6 = n_5 = [G : N(H)]$. Hence $Ord(N(H)) = 60/6 = 10$. Thus

G has a subgroup of order 10. Now by Theorem 1.2.45 we conclude that $n_3 = 4$ or 10. Let K be a Sylow-3-subgroup. Then again by Theorems 1.2.49 and 1.2.54 $n_3 = 4 = [G : N(K)]$ or $10 = n_3 = [G : N(K)]$. If $n_3 = 4 = [G : N(K)]$, then by Theorem 1.2.57 we conclude that G is isomorphic to a subgroup of A_4 which is impossible since $Ord(G) = 60$ where $Ord(A_4) = 12$. Thus $10 = n_3 = [G : N(K)]$. Hence $Ord(N(K)) = 60/10 = 6$. Thus G has a subgroup of order 6.

QUESTION 2.9.8 *Show that a simple group G of order 60 is isomorphic to A_5.*

Solution : Write $Ord(G) = (2^2)(3)(5)$. Let n_2 be the number of Sylow-2-subgroups of G. Then either $n_2 = 5$ or $n_2 = 15$ or $n_2 = 3$ by Theorem 1.2.49. By Theorem 1.2.57 it is impossible that $n_2 = 3$. Let K be a Sylow-2-subgroup. If $n_2 = 5$, then $5 = [G : N(K)]$ by Theorem 1.2.49 and 1.2.54, and hence $G \cong A_5$ by Theorem 1.2.57. Thus assume that $n_2 = 15$. Since 4 does not divide $14 = n_2 - 1$, by Theorem 1.2.51 we conclude that there are two distinct Sylow-2-subgroup H and K such that $Ord(H \cap K) = 2$ $Ord(N(H \cap K)) > Ord(HK) = Ord(H)Ord(K)/2 = 8$. Since $Ord(N(H \cap K)) > 8$ and $Ord(N(H \cap K))$ divides 60, we conclude that $m = [G : N(H \cap K)] \leq 5$. Thus G is isomorphic to a subgroup of A_m by Theorem 1.2.57. Since $Ord(G) = 60$ and $Ord(A_m) < 60$ if $m < 5$, we conclude that $m = 5$. Since G is isomorphic to a subgroup of A_5 and $Ord(G) = Ord(A_5) = 60$, we conclude that G is isomorphic to A_5.

QUESTION 2.9.9 *Let H be a subgroup of S_5 that contains a 5-cycle and a 2-cycle. Show that $H = S_5$.*

Solution : Let *alpha* be a 5-cycle in H, and let $\beta = (b_1, b_2)$ be a 2-cycle. By Question 2.4.18 we conclude that $Ord(\alpha\beta) = 4$ OR 6. If $Ord(\alpha\beta) = 4$, then $Ord(\alpha^\beta) = 6$ by Question 2.4.19. Thus H contains an element of order 6. Since H contains an element of order 5 and an element of order 6 and $gcd(5, 6) = 1$, we conclude that 30 divides $Ord(H)$. Let $D = H \cap A_5$ and $m = [A_5 : D]$. By Question 2.5.25 we conclude that $Ord(D) \geq 15$. If $D \neq A_5$, then $1 < m \leq 4$, and thus $A_5 \cong A_m$ by Theorem 1.2.57 which is impossible. Thus $D = A_5$. Since D is exactly half of H by Question 2.5.25, we conclude that $H = S_5$.

QUESTION 2.9.10 *Let H be a subgroup of A_5 that contains a 5-cycle and a 3-cycle. Show that either $H = A_5$ or $H = S_5$.*

Solution : Let $D = H \cap A_5$, α be a 5-cycle of H, and β be a 3-cycle of H. Since β and α are even permutation, we conclude that $\alpha \in D$ and $\beta \in D$. Thus 15 divides $Ord(D)$. Hence $Ord(D) \geq 15$. Suppose that $D \neq A_5$, and let $m = [A_5 : D]$. Then $1 < m \leq 4$. Thus $A_5 \cong A_m$ by Theorem 1.2.57 which is impossible. Thus $D = A_5$. If $H \neq A_5$, then $H = S_5$ because $D = A_5$ contains exactly half of the elements of H by Question 2.5.25.

QUESTION 2.9.11 *Show that S_5 contains exactly one subgroup of order 60.*

Solution : Clearly A_5 is a subgroup of S_5 of order 60. Let H be a subgroup of S_5 of order 60. We will show that $H = A_5$. Let $D = H \cap A_5$. Suppose that $H \neq A_5$. Hence D is a proper subgroup of A_5. By Question 2.5.25 we conclude that $Ord(D) = 30$. Since $[A_5 : D] = 2$, we conclude that D is normal in A_5 by Question 2.6.1, a contradiction since A_5 is simple.

QUESTION 2.9.12 *Let G be a group of order p^n where p is prime and $n \geq 2$. Show that G is not simple.*

Solution : If G is Abelian, then every subgroup of G of order p is normal in G, and thus G is not simple. Thus assume that G is not Abelian. Then By Theorem 1.2.47 $Ord(Z(G)) \geq p$, and since G is not Abelian $Z(G) \neq G$. Thus $Z(G)$ is normal in G. Since $Z(G) \neq \{e\}$ and $Z(G) \neq G$, we conclude that G is not simple.

QUESTION 2.9.13 *Let G be a group of order pqr such that $p > q > r$ and p, q, r are prime numbers. Show that G is not simple.*

Solution : Deny. Hence G is simple. Let n_p be the number of Sylow-p-subgroups of G, n_q be the number of Sylow-q-subgroups of G, and n_r be the number of Sylow-r-subgroups of G. Since G is simple, by Theorem 1.2.46 we conclude that $n_p \neq 1$, $n_q \neq 1$, and $n_r \neq 1$. Since $p > q > r$, we conclude that $n_p = qr$ by Theorem 1.2.45. Hence there are $N_p = (p-1)qr = pqr - qr$ elements of order p. Since $q > r$ and $p > q$, we conclude that the minimum value of $n_q = p$ and the minimum value of $n_r = q$. Hence there are at least $N_q = (q-1)p = pq - p$ elements of order q and at least $N_r = (r-1)q = qr - q$ elements of order r. Now $N_p + N_q + N_r \geq pqr - qr + pq - p + qr - q = pqr + pq - (p+q) > pqr = Ord(G)$ (because $p > q$ we have $pq > (p+q)$), a contradiction. Thus G is not simple.

QUESTION 2.9.14 *Let G be a group of order p^2q, where p and q are distinct prime numbers. Show that G is not simple.*

Solution : Deny. Hence G is simple. Let n_p be the number of Sylow-p-subgroups of G, n_q be the number of Sylow-q-subgroups of G. Since G is simple, by Theorem 1.2.46 we conclude that $n_p \neq 1$ and $n_q \neq 1$. Thus $n_p = q$ by Theorem 1.2.45. Thus $p < q$. Hence $n_q = p^2$ again by Theorem 1.2.45. Thus p^2 does not divide $n_p - 1 = q - 1$. Hence by Theorem 1.2.51 there are two distinct Sylow-p-subgroups H and K such that $Ord(H \cap K) = p$ and $Ord(N(H \cap K)) > Ord(HK) = p^2p^2/p = p^3$. Since $Ord(N(H \cap K) > p^3$ and $Ord(N(H \cap K))$ must divide $Ord(G) = p^2q$, we conclude that $Ord(N(H \cap K)) = p^2q = Ord(G)$. Hence $N(H \cap K) = G$, and thus $H \cap K$ is normal in G a contradiction. Hence G is not simple.

2.10 Classification of Finite Abelian Groups

QUESTION 2.10.1 *What is the smallest positive integer n such that there are exactly 3 nonisomorphic Abelian group of order n.*

Solution : Let $n = 8$. Then a group of order 8 is isomorphic to one of the following three nonisomorphic groups: Z_8, $Z_2 \oplus Z_2 \oplus Z_2$, and $Z_2 \oplus Z_4$.

QUESTION 2.10.2 *How many elements of order 2 in $Z_8 \oplus Z_2$? How many elements of order 2 in $Z_4 \oplus Z_2 \oplus Z_2$?*

Solution : In $Z_8 \oplus Z_2$, there are exactly 3 elements of order 2, namely: (4, 0), (4, 1), (0, 1). In $Z_4 \oplus Z_2 \oplus Z_2$, there are exactly 6 elements of order 2, namely: (2, 0, 0), (2, 1, 0), (2, 0, 1), (0, 1, 0), (0, 1, 1), (0, 0, 1).

QUESTION 2.10.3 *Show that an (Abelian) group G of order 45 contains an element of order 15.*

By Theorem 1.2.52, G is isomorphic to one of the following : $Z_{45} \cong Z_5 \oplus Z_9$, or $Z_5 \oplus Z_3 \oplus Z_3$. In the first case, since Z_{45} is cyclic and 15 divides 45, we conclude that G contains an element of order 15. In the second case, let $a = (1, 1, 1)$. Then by Theorem 1.2.37 $Ord(a) = lcm[Ord(1), Ord(1), Ord(1)] = lcm[5, 3, 3] = 15$.

QUESTION 2.10.4 *Show that an Abelian group of order p^n for some prime p and some $n \geq 1$ is cyclic if and only if G has exactly one subgroup of order p.*

Solution : Suppose that G is cyclic. Then G has exactly subgroup of order p by Theorem 1.2.12. Conversely, suppose that G has exactly one subgroup of order p. Then G must be isomorphic to Z_{p^n} by Theorem 1.2.52, for if by Theorem 1.2.52 G is isomorphic to $Z_{p^k} \oplus Z_{p^i} \oplus ...$ for some $k, i \geq 1$, then G would have at least two subgroups of order p.

QUESTION 2.10.5 *Show that there are exactly two Abelian groups of order* 108 *that have exactly one subgroup of order* 3.

Solution : First $108 = (3)(36) = (2^2)(3^3)$. For G to have exactly one subgroup of order 3, G must have a cyclic a subgroup of order 27 (see Question 2.10.4.) Let $G_1 = Z_4 \oplus Z_{3^3}$ and $G_2 = Z_2 \oplus Z_2 \oplus Z_{3^3}$. Then clearly that G_1 and G_2 are nonisomorphic. The subgroup of G_1 generated by $(0, 9)$ is cyclic of order 3, and the subgroup of G_2 generated by $(0, 0, 9)$ is also cyclic of order 3.

QUESTION 2.10.6 *Suppose that G is an Abelian group of order* 120 *such that G has exactly three elements of order* 2. *Classify G up to isomorphism.*

Solution : Write $120 = (2^3)(3)(5)$. Since G has exactly 3 elements of order 2. G can not have a cyclic subgroup of order 8. Thus by Theorem 1.2.52 G is isomorphic to $G_1 = Z_2 \oplus Z_4 \oplus Z_{15}$ (observe that Z_{15} is isomorphic to $Z_3 \oplus Z_5$) or G is isomorphic to $G_2 = Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_{15}$. In the first case, G_1 has the following elements of order 2, namely : (1, 2, 0), (1, 0, 0), (0, 2, 0). In the second case G_2 has the following elements of order 2, namely : (1, 1, 0), (1, 0, 0), (0, 1, 0).

QUESTION 2.10.7 *Suppose that the order of a finite Abelian group G is divisible by* 10. *Show that G has an element of order* 10.

Solution : Since 2 divides $Ord(G)$, G has an element, say a, of order 2 by Theorem 1.2.31. Also, since 5 divides $Ord(G)$, G has an element, say b, of order 5 again by Theorem 1.2.31. Since $gcd(2, 5) = 1$ and $ab = ba$, we conclude that $Ord(ab) = 10$ by Question 2.1.14.

QUESTION 2.10.8 *Find an example of a finite Abelian group such that $Ord(G)$ is divisible by* 4 *but G has no elements of order* 4.

Solution : Let $G = Z_2 \oplus Z_2 \oplus Z_2$. Then G is a group of order 8 and hence $Ord(G)$ is divisible by 4, but each nonidentity element of G is of order 2.

QUESTION 2.10.9 *What is the isomorphism class of* $U(20)$*, i.e.,* $U(20) = \{a : 1 \leq a < 20$ *and* $gcd(a, 20) = 1)\}$ *is a group under multiplication module* 20*.*

Solution : First $Ord(U(20)) = \phi(20) = 8$ (see Theorem 1.2.13) by Theorem 1.2.14. Since $U(20)$ is not cyclic, by Theorem 1.2.52 we conclude that $U(20)$ is isomorphic to $G_1 = Z_2 \oplus Z_4$ or $G_2 = Z_2 \oplus Z_2 \oplus Z_2$. Since $3 \in U(20)$ and $Ord(3) = 4$, we conclude that $U(20)$ is not isomorphic to G_2 (because every nonidentity element of G_2 is of order 2). Thus $U(20)$ is isomorphic to $Z_2 \oplus Z_4$. **Another Solution** : Write $20 = (4)(5)$. Since $gcd(4, 5) = 1$, we conclude that $U(20) \cong U(4) \oplus U(5)$ by Theorem 1.2.38. But $U(4)$ is isomorphic to Z_2 by Theorem 1.2.40 and $U(5)$ is isomorphic to Z_4 again by Theorem 1.2.40. Thus $U(20) \cong Z_2 \oplus Z_4$.

QUESTION 2.10.10 *What is the isomorphism class of* $U(100)$*. How many elements of order* 20 *does* $U(100)$ *have?*

Solution : First $100 = (2^2)(5^2)$. By Theorems 1.2.38 and 1.2.40 we conclude that $U(100) = U(2^2) \oplus U(5^2) = Z_2 \oplus Z_{20}$. If $b \in Z_{20}$ such that $Ord(b) = 20$, then $20(a, b) = (0, 0)$ for every $a \in Z_2$. By Theorem 1.2.14, there are $\phi(20) = 8$ elements in Z_{20} of order 20. Since (a, b) has order 20 if and only if b has order 20 and a has two choices, namely: 0, 1, we conclude that there $8 \times 2 = 16$ elements in $Z_2 \oplus Z_{20}$ of order 20. Since $U(100) \cong Z_2 \oplus Z_{20}$, we conclude that $U(100)$ has exactly 16 elements of order 20.

QUESTION 2.10.11 *Let* G *be a finite Abelian group and* $b \in G$ *has maximal order. Show that if* $a \in G$*, then* $Ord(a)$ *divides* $Ord(b)$*.*

Solution : Let $n = Ord(b)$ and let $a \in G$ such that $m = Ord(a)$. We need to show that m divides n. Let $k = gcd(m, n)$. Then $1 = gcd(m, n/k)$. Since $Ord(b) = n$, we conclude that $Ord(b^k) = n/k$. Since G is Abelian and $gcd(m, n/k) = 1$, we conclude that $Ord(ab^k) = mn/k$ by Question 2.1.14. Now since $k = gcd(m, n)$, we conclude that $nm/k \geq n$. Since $Ord(b) = n$ is of maximal order, we conclude that $mn/k = n$. Since k divides m and $mn/k = n$, we conclude that $k = m$. Since $k = m = gcd(m, n)$, we conclude that m divides n.

QUESTION 2.10.12 *Let* G *be a finite Abelian group of order* 2^n*. Show that* G *has an odd number of elements of order* 2*.*

Solution : If G is cyclic, then $G \cong Z_{2^n}$, and hence G has exactly one element of order 2 because G has exactly one subgroup of order 2. Thus suppose that G is not cyclic. Then by Theorem 1.2.52 we conclude that $G \cong G_1 = Z_{2^{m_1}} \oplus Z_{2^{m_2}} \oplus Z_{2^{m_3}} \oplus \cdots \oplus Z_{2^{m_i}}$ where $m_1 + m_2 + \cdots + m_i = n$, and $1 \leq m_k < n$. Let $a = (a_1, a_2, ..., a_i) \in G_1$ of order 2. Then not all a_k's are zeros, and for each a_k we have either $a_k = 0$ or $Ord(a_k) = 2$. Since each $Z_{2^{m_k}}$ has exactly one subgroup of order 2, we conclude that there are exactly $2^i - 1$ elements of order 2. Since $2^i - 1$ is an odd number, the proof is completed.

QUESTION 2.10.13 *Let G be a finite Abelian group such that for each divisor k of $Ord(G)$ there is exactly one subgroup of G of order k. Show that G is cyclic.*

Solution : Write $Ord(G) = (p_1^{n_1})(p_2^{n_2}) \cdots (p_m^{n_m})$ where the p_i's are distinct prime numbers and each $n_i \geq 1$. We need to show that $G \cong G_1 = Z_{p_1^{n_1}} \oplus \cdots Z_{p_m^{n_m}}$. Deny. Then by Theorem 1.2.52 and Theorem 1.2.53 there is a p_i a prime divisor of G and a subgroup H of G such that $H \cong Z_{p_i} \oplus Z_{p_i}$. Thus H has two distinct subgroups of order p_i, and thus G has two distinct subgroups of order p_i, a contradiction. Hence G is cyclic.

2.11 General Questions on Groups

QUESTION 2.11.1 *Give an example of a group G that contains two elements, say a, b, such that $Ord(a^2) = Ord(b^2)$ but $Ord(a) \neq Ord(b)$.*

Solution : Let $G = Z_6$, under addition module 6, let $a = 1$ and $b = 2$. Then $a^2 = 1 + 1 = 2$ and $b^2 = 2 + 2 = 4$. Hence $ord(a^2) = Ord(b^2) = 3$. But $Ord(a) = 6$ and $Ord(b) = 3$.

QUESTION 2.11.2 *let* $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$ *Write β as disjoint cycles, then find $Ord(\beta)$ and β^{-1}.*

Solution : $\beta = (1)(2, 3, 8, 4, 7)(5, 6)$. Hence by Theorem 1.2.20 $Ord(\beta) = LCM(4, 2) = 4$. Now $\beta^{-1} = (6, 5)(7, 4, 8, 3, 2) = (7, 4, 8, 3, 2)(6, 5)$.

QUESTION 2.11.3 *Let $\beta \in S_7$ and suppose that $\beta = (2, 1, 4, 3)(5, 6, 7)$. Find the least positive integer n such that $\beta^n = \beta^{-3}$.*

Solution : The idea is to find the order of β. So, we write β as disjoint cycles. But β is already written in disjoint cycles. Hence $Ord(\beta) = lcm[4, 3] = 12$. Now $\beta^n = \beta^{-3}$ implis $\beta^{n+3} = e$ (the isentity). Hence $n + 3 = 12$. Thus $n = 9$.

QUESTION 2.11.4 *Let* $\beta = (1, 2, 3)(1, 4, 5)$. *Write* β^{99} *in cycle form.*

Solution : First, write β as disjoint cycles. Hence $\beta = (1, 4, 5, 2, 3)$. Thus $Ord(\beta) = 5$. Since 5 divides 100, we have $\beta^{100} = \beta\beta^{99} = e$. Thus $\beta^{99} = b^{-1} = (3, 2, 5, 4, 1)$.

QUESTION 2.11.5 *Let* $\beta = (1, 5, 3, 2, 6)(7, 8, 9)(4, 10) \in S_{10}$. *Given* β^n *is a 5-cycle. What can you say about* n.

Solution : Since β^n is a 5-cycle, we conclude that $Ord(\beta^n) = 5$. Now since *beta* is in disjoint cycles, we conclude that $Ord(\beta) = lcm[5, 3, 2] = 30$. Hence by Question 2.1.12 we have $Ord(\beta^n) = 30/gcd(n, 30) = 5$. Thus $gcd(n, 30) = 6$. Thus $n = 6m$ for some $m \geq 1$ such that $gcd(m, 5) = 1$. So, n = 6, 12, 18, 24, 36,... so all n such that $gcd(n, 30) = 6$.

QUESTION 2.11.6 *Let* $G = U(8) \oplus Z_{12} \oplus S_7$. *Find the order of* $a = (3, 3, (1, 2, 4)(5, 7))$.

Solution: By Theorem 1.2.37, $Ord(a) = lcm(Ord(3), Ord(3), Ord((1, 2, 4)(5, 7))) = (2, 4, 6) = 12$.

QUESTION 2.11.7 *Suppose that* H *and* K *are two distinct normal subgroups of a finite group* G *such that* $[G : H] = [G : K] = p$, *where* p *is a prime number. Show that there is a group homomorphism from* G *ONTO* $G/H \oplus G/K$. *Also, show that* G *has a normal subgroup* D *such that* $[G : D] = p^2$. *In particular, show that* $D = H \cap K$ *is a normal subgroup of* G *such that* $[G : D] = p^2$.

Solution : First observe that since H and K are distinct and G is finite, $[G : H \cap K] > p$. Now let Φ be a map from G into $G/H \oplus G/K$ such that $\Phi(g) = (gH, gK)$. It is clear that Φ is a group homomorphism from G into $G/H \oplus G/K$ and $Ker(\Phi) = H \cap K$. Hence $G/Ker(\Phi) = G/(H \cap K)$ *cong* to a subgroup F of $G/H \oplus G/K$. Since $Ord(G/H \oplus G/K) = p^2$ and p is prime, we conclude that $Ord(F) = 1$, or p, or p^2.

Since $Ord(G/(H \cap K)) = [G : H \cap K] = Ord(F)$ and $[G : H \cap K] > p$, we conclude that $Ord(G/(H \cap K)) = Ord(F) = [G : H \cap K] = p^2$. Hence Φ is ONTO and $H \cap K$ is normal in G such that $[G : H \cap K] = p^2$.

QUESTION 2.11.8 *Suppose that H and K are two distinct subgroups of a finite group G such that $[G : H] = [G : K] = 2$. Show that there is a group homomorphism from G ONTO $G/H \oplus G/K$. Also, show that G has a normal subgroup D such that $[G : D] = 4$. In particular, show that $D = H \cap K$ is a normal subgroup of G such that $[G : D] = 4$.*

Solution : Since $[G : H] = [G : K] = 2$, we conclude that H and K are both normal in G by Question 2.6.1. Hence replace p in Question 2.11.7 with 2 and use the same argument.

QUESTION 2.11.9 *Let G be a finite group with an odd number of elements. Suppose that G has a normal subgroup H of order 5. Show that $H \subset Z(G)$.*

Solution : Since H is normal in G, we conclude that $Ord(G/C(H))$ divides $Ord(Aut(H))$ by Question 2.7.56. But $H \cong Z_5$ because H is cyclic with 5 elements. Thus $Ord(G/C(H))$ divides $Ord(Aut(Z_5))$. Hence $Ord(G/C(H))$ divides $Ord(U(5)) = 4$ because $Ord(Aut(Z_5)) = Ord(U(5)) = 4$ by Theorem 1.2.41. Let $n = Ord(G/C(H)) = [G : C(H]$. Since G has an odd order, n must be an odd number. Since n divides 4 and n is odd, we conclude that $n = 1$. Hence $[G : C(H)] = 1$, and thus $C(H) = G$. Since every element of H commute with every element of G, we conclude that $H \subset Z(G)$.

QUESTION 2.11.10 *Let G be a finite group with an odd number of elements such that G has no subgroup K with $[G : K] = 3$. If H is a normal subgroup of G with 7 elements, then show that $H \subset Z(G)$.*

Solution : Since H is normal in G, we conclude that $Ord(G/C(H))$ divides $Ord(Aut(H))$ by Question 2.7.56. But $H \cong Z_7$ because H is cyclic with 7 elements. Thus $Ord(G/C(H))$ divides $Ord(Aut(Z_7))$. Hence $Ord(G/C(H))$ divides $Ord(U(7)) = 6$ because $Ord(Aut(Z_7)) = Ord(U(7)) = 6$ by Theorem 1.2.41. Let $n = Ord(G/C(H)) = [G : C(H]$. Since G has an odd order, n must be an odd number. Since G has no subgroups of index 3, we conclude that $n \neq 3$. Since n divides 6 and n is odd and $n \neq 3$, we conclude that $n = 1$. Hence $[G : C(H)] = 1$, and thus $C(H) = G$. Since every element of H commute with every element of G, we conclude that $H \subset Z(G)$.

QUESTION 2.11.11 *Show that* $G = \mathcal{Q}/\mathcal{Z}$ *is an infinite group such that each element of* G *is of finite order.*

Solution: Deny. Then G has a finite order, say n. Thus $n = [\mathcal{Q} : \mathcal{Z}]$, and thus $ng = \mathcal{Z}$ for every $g \in G$. Now let $x = 1/(n+1)\mathcal{Z} \in G$. Then $nx = n/(n+1)\mathcal{Z} \neq \mathcal{Z}$, a contradiction. Thus G is an infinite group. Let $y \in G$. Then $y = a/m\mathcal{Z}$ for some $a \in \mathcal{Z}$ and for some nonzero nonnegative $m \in \mathcal{Z}$. Thus $my = a\mathcal{Z} = \mathcal{Z}$. Thus $Ord(y)$ divides m, and hence y is of finite order.

QUESTION 2.11.12 *For each* $n \geq 2$*, show that* $G = \mathcal{Q}/\mathcal{Z}$ *has a unique subgroup of order* n*.*

Solution : let $n \geq 2$ and $H_n = \{a/n\mathcal{Z} : 0 \leq a < n\}$. It is easy to see that H_n is a subgroup of G of order n. Suppose that D is a subgroup of G of order n. We will show that $D = H_n$. let $d \in D$. Then $d = g\mathcal{Z}$. Since $nd = ng\mathcal{Z} = \mathcal{Z}$, we conclude that $ng = b \in \mathcal{Z}$. Thus $g = b/n \in \mathcal{Q}$, and hence $d = c/n\mathcal{Z}$ for some $0 \leq c < n$. Thus $d \in H_n$, and hence $D \subset H_n$. Since $Ord(H_n) = Ord(D) = n$ and $D \subset H_n$, we conclude that $D = H_n$.

QUESTION 2.11.13 *Is there a group homomorphism from* $G = Z_8 \oplus Z_2 \oplus Z_2$ *ONTO* $D = Z_4 \oplus Z_4$*.*

Solution : No. For suppose that Φ is a group homomorphism from G ONTO D. Since $F = G/Ker(\Phi) \cong D$ and $Ord(G) = 32$ and $Ord(D) = 16$, we conclude that $Ord(Ker(\Phi)) = 2$. Hence $Ker(\Phi) = \{(0,0,0), (a_1, a_2, a_3)\}$. Suppose that $a_1 = 0$. Then $Ord((1,0,0)Ker(\Phi)) = 8$, a contradiction since D has no elements of order 8. Thus assume that $a_1 \neq 0$. Since $Ord((a_1, a_2, a_3)) = 2$, we conclude that $a_1 = 4$. Now $(2,0,0)Ker(\Phi), (2,0,1)Ker(\Phi), (2,1,0)Ker(\Phi), (2,1,1)Ker(\Phi), (0,1,1)Ker(\Phi)$ are all distinct elements of $F = G/Ker(\Phi)$ and each is of order 2. Now D has exactly 3 elements of order 3, namely: $(2,2), (2,0), (0,2)$. Thus $F \ncong D$ because F has at least 4 elements of order 2, where D has exactly 3 elements of order 2. A contradiction. Hence there is no group homomorphism from $G = Z_8 \oplus Z_2 \oplus Z_2$ ONTO $D = Z_4 \oplus Z_4$.

QUESTION 2.11.14 *Let* $G = \mathcal{Z} \oplus \mathcal{Z}$ *and let* $H = \{(a,b) : a, b$ *are even integers* $\}$*. Show that* H *is a subgroup of* G*. Describe the group* G/H*.*

Let $x = (a_1, b_1), y = (a_2, b_2) \in H$. Then $y^{-1}x = (-a_2, -b_2) + (a_1, b_1) = (a_1 - a_2, b_1 - b_2) \in H$ because $a_1 - a_2, b_1 - b_2$ are even integers. Thus H is a subgroup of G by Theorem 1.2.7. Observe that $H = 2\mathcal{Z} \oplus 2\mathcal{Z}$. Now let $K = \mathcal{Z}/2\mathcal{Z}$ and let Φ be the group homomorphism from G ONTO $K \oplus K$ defined by $\Phi(a, b) = (a2\mathcal{Z}, b2\mathcal{Z})$. Then $Ker(\Phi) = 2\mathcal{Z} \oplus 2\mathcal{Z} = H$. Hence $G/H \cong K \oplus K = Z_2 \oplus Z_2$. Thus G/H has exactly 4 elements.

For two elements x, y in a group G, [xy] denotes the element $x^{-1}y^{-1}xy$ (such element is called the commutator of x and y).

QUESTION 2.11.15 *Let x, y be two elements in a group G such that y commutes with the element $[xy]$. Prove that $y^n x = xy^n[yx]^n$ for every positive integer $n \geq 1$.*

Solution: First observe that [yx] is the inverse of [xy]. Since y commutes with $[xy]$, we conclude that y commutes with [yx] by Question 2.2.6. We prove the claim by induction. Let $n = 1$. Then $yx = xy[yx] = xyy^{-1}x^{-1}yx = yx$. Assume the claim is valid for a positive integer $n \geq 1$, i.e., $y^n x = xy^n[yx]^n$. We prove the claim for $n+1$. Now $y^{n+1}x = yy^n x = yxy^n[yx]^n$. But $yx = xy[yx]$ and y^m commutes with [yx] for every positive integer m (since y commute with [yx]). Hence $y^{n+1}x = yy^n x = yxy^n[yx]^n = xy[yx]y^n[yx]^n = xy^{n+1}[yx]^{n+1}$.

QUESTION 2.11.16 *Let x, y be two elements in a group G such that X and y commute with the element $[xy]$. Prove that $(xy)^n = x^n y^n [yx]^{n(n-1)/2}$ for every positive integer $n \geq 1$.*

Solution: Once again, observe that [yx] is the inverse of [xy]. Since x and y commute with $[xy]$, we conclude that x and y commute with [yx] by Question 2.2.6. We prove the claim by induction. Let $n = 1$. Then $xy = xy[yx]^0 = xy$. Assume the claim is valid for a positive integer $n \geq 1$, i.e., $(xy)^n = x^n y^n [yx]^{n(n-1)/2}$. We prove the claim for $n+1$, i. e., we need to show that $(xy)^{n+1} = x^{n+1}y^{n+1}[yx]^{(n+1)n/2}$. Now $(xy)^{n+1} = (xy)^n(xy) = x^n y^n [yx]^{n(n-1)/2}(xy) = x^n y^n xy[yx]^{n(n-1)/2}$ (since x and y commute with $[xy]$). But $y^n x = xy^n[yx]^n$ by Question 2.11.15. Hence $(xy)^{n+1} = (xy)^n(xy) = x^n y^n [yx]^{n(n-1)/2}(xy) = x^n y^n xy[yx]^{n(n-1)/2} = x^n xy^n y[yx]^n[yx]^{n(n-1)/2} = x^{n+1}y^{n+1}[yx]^{n+(n(n-1)/2)} = x^{n+1}y^{n+1}[yx]^{(n+1)n/2}$.

QUESTION 2.11.17 *Let G be a non-cyclic group of order p^3 for some odd prime number p. Then :*

1. *If G is non-Abelian, then show that $Z(G)$ (the center of G) contains exactly p elements. Also, show that $(xy)^p = x^p y^p$ for every $x, y \in G$.*

2. *Let L be a subgroup of $Z(G)$ of order p. Show that the map $\alpha : G \longrightarrow L$ such that $\alpha(g) = g^p$ is a ring homomorphism from G into L.*

3. *Show that G contains a normal subgroup H that is isomorphic to $Z_p \oplus Z_p$.*

Solution (1). By Theorem 1.2.47, $Ord(Z(G)) = p$ or p^2 or p^3. Since G is non-Abelian, we conclude that $Ord(Z(G)) \neq p^3$. Suppose that $Ord(Z(G)) = p^2$. Since $Z(G)$ is a normal subgroup of G and $Ord(G/Z(G)) = p$, we conclude that $G/Z(G)$ is a cyclic group, and hence G is Abelian by Question 2.6.6, a contradiction. Thus $Ord(Z(G)) = p$ (observe that p is an odd number not needed here.) Now since $Ord(G/Z(G)) = p^2$, we conclude that $G/Z(G)$ is abelian by Question 2.8.3. Hence $xyZ(G) = yxZ(G)$ for every $x, y \in G$, and thus $[xy] = x^{-1}y^{-1}xy = z \in Z(G)$ for every $x, y \in G$. Since $[xy] \in Z(G)$ for every $x, y \in G$, we conclude that $(xy)^p = x^p y^p [yx]^{p(p-1)/2}$ for every $x, y \in G$ by Question 2.11.16. Since $Ord(Z(G)) = p$ and 2 divides $p-1$ (because p is odd), we conclude that $[yx]^{p(p-1)/2} = 1$. Thus $(xy)^p = x^p y^p [yx]^{p(p-1)/2} = x^p y^p$.

(2) Since $L \subset Z(G)$, we conclude that L is normal in G. Since $Ord(L) = p$ $Ord(G/L) = p^2$. Since G is non-cyclic, we conclude that G/L is not cyclic. Since $Ord(G/L) = p^2$ and G/L is not cyclic, we conclude that each non-identity element of G/L has order p, i.e., $g^p \in L$ for every $g \in G$. Now let $x, y \in G$. Since $\alpha(xy) = (xy)^p = x^p y^p$ by (1) and $x^p \in L$ for each $x \in G$, we conclude that α is a group homomorphism from G into L.

(3) Assume that G is Abelian. Since G is non-cyclic, we conclude that $G \cong Z_{p^2} \oplus Z_p$ OR $G \cong Z_p \oplus Z_p \oplus Z_p$ by Theorem 1.2.52, and thus in either case G contains a normal subgroup isomorphic to $Z_p \oplus Z_p$. Now suppose that G is non-Abelian. By Theorem 1.2.43, we conclude that G has a subgroup H of order p^2. Since $[G : H] = p$, we conclude that there is a group homomorphism from G into S_p such that $Ker(\Phi)$ is contained in H by Theorem 1.2.56. Hence $Ord(Ker(\Phi)) = 1$ OR p Or

p^2. Thus, $Ord(G/Ker(\Phi)) = p^3$ or p^2 or p. Since $G/Ker(\Phi)$ is group-isomorphic to a subgroup of S_p and neither p^3 divides $Ord(S_p) = p!$, nor p^2 divides $p!$, we conclude that $Ord(G/Ker(\Phi)) = p$, and thus $Ker(\Phi) = H$ (since $Ker(\Phi)$ is contained in H). Thus H is a normal subgroup of G. Now since $Ord(H) = p^2$, we conclude that H is Abelian by Question 2.8.3. Hence $H \cong Z_{p^2}$ or $H \cong Z_p \oplus Z_p$ by Theorem 1.2.52. If $H \cong Z_p \oplus Z_p$, then we are done. Hence assume that $H \cong Z_{p^2}$. Thus H is cyclic and hence G contains an element of order p^2. Now let α as in (2). Since Ord(Z(G)) = p and α is a group homomorphism from G into $Z(G)$ and G contains an element of order p^2, we conclude that $\alpha(G) = Z(G)$. Thus, $G/Ker(alpha) \cong Z(G)$, and hence $Ord(G/Ker(\alpha)) = p$. Thus, $Ord(Ker(\alpha)) = p^2$, and therefore $Ker(\alpha)$ is Abelian by Question 2.8.3. Now let $x \in Ker(\alpha)$. Then $\alpha(x) = x^p = 1 \in Z(G)$. Hence $Ord(x) = 1$ or $Ord(x) = p$. Since $ker(\alpha)$ is Abelian and each nonidentity element of $Ker(\alpha)$ has order p, we conclude that $Ker(\alpha) \cong Z_p \oplus Z_p$.

QUESTION 2.11.18 *Suppose that a non-cyclic group G has order p^n for some odd prime number p and $n \geq 3$. Show that G contains a normal subgroup isomorphic to $Z_p \oplus Z_p$.*

Solution : Suppose that G is a non-cyclic Abelian. Then $G \cong Z_{p^i} \oplus D$ for some Abelian group D of order p^{n-i} for some i, $1 \leq i < n$ by Theorem 1.2.52. Thus G contains a normal subgroup isomorphic to $Z_p \oplus Z_p$. Thus assume that G is non-Abelian. We prove it by induction on n. If $n = 3$, then by (3) in Question 2.11.17 we are done. Hence assume that the claim is valid for $3 \leq m < n$ and we will prove the claim when $m = n$. Since $Ord(Z(G)) = p^k$ for some $1 \leq k < n$ by Theorem 1.2.47, let $F = G/L$ for some subgroup L of order p contained in $Z(G)$. Thus $Ord(F) = p^{n-1}$. Now suppose that F is cyclic. Then G is Abelian by Question 2.6.6, a contradiction. Hence F is not cyclic. Thus F contains a normal subgroup J (of order p^2) isomorphic to $Z_p \oplus Z_p$ by the assumption. Since $Ord(J \cap Z(F)) \geq p$ by Theorem 1.2.59, let M be a subgroup $J \cap Z(F)$ of order p. Then M is a normal subgroup of F. Let Φ be the of group homomrphism from G ONTO $F = G/L$ defined by $\Phi(g) = gL$. Thus $H = \Phi^{-1}(J)$ is a normal subgroup of G which contains L and $Ord(H) = p^3$; also $\Phi^{-1}(M) = N$ is a normal subgroup of G such that $Ord(N) = p^2$ and $N \subset H$. Thus, N is Abelian by Question 2.8.3. Thus either $N \cong Z_{p^2}$ OR $N \cong Z_p \oplus Z_p$ by Theorem 1.2.52. If $N \cong Z_p \oplus Z_p$, then we are done (since N is normal in G). Thus assume that $N \cong Z_{p^2}$, and hence H contains an element of

order p^2 (Since $N \subset H$ and $N \cong Z_{p^2}$). Observe that H is a non-cyclic normal subgroup of G because $\Phi(H) = J$ is a non-cyclic subgroup of F. Since L is a subgroup of H of order p and it is normal being a subset of $Z(G)$, let $\alpha : H \longrightarrow L$ such that $\alpha(h) = h^p$ for every $h \in H$. Hence α is a group homomorphism from H into L by (2) in Question 2.11.17. Since H contains an element of order p^2, we conclude that $\alpha(H) = L$. Since $H/Ker(\alpha) \cong \alpha(H) = L$, we conclude that $Ord(Ker(\alpha)) = p^2$ and $Ker(\alpha) = \{h \in H : \alpha(h) = h^p = e$ (the identity of H (G)$\}$. It is clear that $Ker(\alpha)$ is normal in H. Now let $g \in G$. Since H is normal in G and $Ker(\alpha) \subset H$, we conclude that $g^{-1}Ker(\alpha)g \subset H$. Let $a \in Ker(\alpha)$. Then $(g^{-1}ag)^p = g^{-1}a^pg = e$. Hence $g^{-1}ag \in Ker(\alpha)$. Thus $g^{-1}Ker(\alpha)g \subset Ker(\alpha)$ for every $g \in G$. Hence $Ker(\alpha)$ is a normal subgroup of G by Question 2.6.29. Since $Ord(Ker(\alpha)) = p^2$ and every nonidentity element of $Ker(\alpha)$ has order p, we conclude that $Ker(\alpha) \cong Z_p \oplus Z_p$ is a normal subgroup of G. [**LONG PROOF BUT I TRIED TO GIVE ALL THE DETAILS, SO DO NOT GET DISCOURAGED**]

QUESTION 2.11.19 *(compare with Question 2.8.22) Let G be a group of order p^n where $n \geq 1$ and p is an odd prime number. If G contains exactly one subgroup of order p, then show that G is cyclic.*

Solution : If $n = 1$ OR $n = 2$, then the claim is clear. Hence assume that $n \geq 3$. Deny. Then by Question 2.11.18, G contains a subgroup that is isomorphic to $Z_p \oplus Z_p$. Thus G contains at least two distinct subgroups of order p, a contradiction. Thus G must be cyclic.

QUESTION 2.11.20 *Let H, K be normal subgroups of a group G such that G/H and G/K are Abelian groups. Prove that $G/(H \cap K)$ is Abelian group.*

Solution Let Φ be the group homomorphism from G into $G/H \oplus G/K$ defined by $\Phi(g) = (gH, gK)$. Then $Ker(\Phi) = H \cap K$. Thus, $G/(H \cap K) \cong$ to a subgroup of $G/H \oplus G/K$. Hence $G/(H \cap K)$ is an Abelian group.

QUESTION 2.11.21 *Let G be a group of order p^n where $n \geq 1$ and p is an odd prime number. If every subgroup of G is normal in G, then show that G is Abelian.*

Solution If n = 1 OR $n = 2$, then there is nothing to prove. Hence assume that $n \geq 3$. Assume the claim is valid for all $2 \leq m < n$. Then by Question 2.11.18, G contains a normal subgroup isomorphic to $Z_p \oplus Z_p$. Hence G contains two distinct normal subgroups, say H and K, each is of order p. Hence G/H and G/K are Abelian by assumption. Thus $G/(H \cap K)$ is Abelian by Question **??**. But $H \cap K = \{e\}$ (e = the identity of G). Thus G is Abelian.

QUESTION 2.11.22 *(A generalization of Question 2.6.1) let G be a group of order n and let H be a subgroup of G such that $[G : H] = p$ where p is the smallest prime divisor of n. Prove that H is normal in G.*

Solution : By Theorem 1.2.56, there is a group homomorphism Φ from G into S_p such that $Ker(\Phi)$ is a normal subgroup of H. We will show that $Ker(\Phi) = H$, and hence H is normal in G. Suppose that $Ker(\Phi)$ is properly contained in H. Since $[G : H] = p$, we conclude that $Ord(G/Ker(\Phi)) = d$ for some integer $d > 2$. Since p is the smallest positive prime divisor of n, we conclude that either p^2 divides d or there is a prime number $q > p$ such that q divides d. Since $G/Ker(\Phi)$ is isomorphic to a subgroup of S_p and $Ord(S_p) = p! = p(p-1)(p-2)...(1)$, we conclude that p is the largest prime number that may divide the order of $G/Ker(\Phi) = d$ and if p divides d, then p^2 does not divide d. Hence neither p^2 divides d nor q divides d, a contradiction. Thus $Ker(\Phi) = H$ is a normal subgroup of G.

QUESTION 2.11.23 *Let G be a group of order p^n where $n \geq 1$ and p is a prime number. Prove that for every m, $1 \leq m < n$, there is a normal subgroup of G of order p^m.*

Solution : If $n = 1$ OR $n = 2$, then the claim is clear. Hence assume that $n \geq 3$. First it is clear that for every m, $1 \leq m < n$, there is a subgroup of order p^m. Hence let H be a subgroup of G of order $n-1$. Then $[G : H] = p$ is the smallest prime divisor of the order of G. Thus H is normal in G by Question 2.11.22. Also, since $Ord(Z(G)) \geq p$ by Theorem 1.2.47, we conclude that G has a normal subgroup of order p. We prove the claim by induction. For $n = 3$, then the claim is clear by the previous argument. Hence assume that the claim is correct for all groups of order p^k where $3 \leq k < n$. Let L be a subgroup of $Z(G)$ of order p. Set $F = G/L$ and let Phi be the group homomorphism from G ONTO F defined by $\Phi(g) = gL$ for every $g \in G$. Then

$Ord(G/L) = p^{n-1}$. Thus , by assumption, for every $2 \leq mleqn-1$, there is a normal subgroup D of F of order p^{m-1}, and hence $J = \Phi^{-1}(D)$ is a normal subgroup of G of order p^m.

QUESTION 2.11.24 *Let L be a normal subgroup of a group G, Φ be the group homomorphism from G ONTO $F = G/L$ defined by $\Phi(g) = gL$ for every $g \in G$, H be a subgroup of F, $N_F(H)$ be the normalizer of H in F, $K = \Phi^{-1}(H)$. Then $N(K) = \Phi^{-1}(N_F(H))$, where $N(K)$ is the normalizer of K in G.*

Solution : First observe that L is a subgroup of K. Let $g \in N(K)$. Since $gKg^{-1} = K$ and $\Phi(K) = H$, $gLHg^{-1}L = H$ in F. Thus $gL \in N_F(H)$, and hence $g \in \Phi^{-1}(N_F(H))$. Now let $g \in \Phi^{-1}(N_F(H))$ and let $kinK$. Then $\Phi(k) = kL \in H$. Thus $gLkLg^{-1}L = gkg^{-1}L \in H$. Since $\Phi(K) = H$, we conclude that $gLkLg^{-1}L = gkg^{-1}L = k_1L$ for some $k_1 \in K$. Thus $gkg^{-1} = k_1z \in K$ for some $z \in L \subset K$. Thus $g \in N(K)$. Hence $N(K) = \Phi^{-1}(N_F(H))$

QUESTION 2.11.25 *Let G be a group of order p^n where $n \geq 1$ and p is a prime number. Prove that H is properly contained in $N(H)$ for every proper subgroup H of G.*

Solution: If $n = 1$ or $n = 2$, then the claim is clear. Also if G is Abelian, then there is nothing to prove. Hence assume that $n \geq 3$ and G is non-Abelian. Now let H be a subgroup of G. If $Z(G)$ *not* $\subset H$, then $Ord(Z(G)H) > Ord(H)$ by Theorem 1.2.48 and it is clear that $H \subset Z(G)H$. But is is easily verified that $Z(G)H \subset N(H)$. Thus $H \neq N(H)$. So we prove the claim for all proper subgroups of G that contain $Z(G)$. Now Let $n = 3$. Then every subgroup of G of order p^2 is normal in G by Question 2.11.22 and if H is subgroup of G of order p containing $Z(G)$, then $H = Z(G)$ and thus $N(H) = N(Z(G)) = G$. We proceed by induction on n. For $n = 3$, then the claim is clear by the previous argument. Hence assume that the claim is correct for all groups of order p^k where $3 \leq k < n$. Set $F = G/Z(G)$ and let Phi be the group homomorphism from G ONTO F defined by $\Phi(g) = gZ(G)$ for every $g \in G$. Then $Ord(F = G/Z(G)) < p^n$ and there is one to one correspondence between the subgroups of G containing $Z(G)$ and the subgroups of F. Let H be a subgroup of F,and $K = \Phi^{-1}(H)$. Then $N(K) = \Phi^{-1}(N_F(H))$ by Question 2.11.24, where $N_F(H)$ is the normalizer of H in F. Since $H \neq N_F(H)$ by assumption, we conclude that $K \neq N(K)$, and thus K is properly contained in $N(K)$.

QUESTION 2.11.26 *Show that* A_4 *does not contain a subgroup of order* 6*,*

Solution : Deny. Let H be a subgroup of A_4 of order 6. Since $[A_4 : H] = 2$, by Question 2.6.1 we conclude that H is normal in A_4. Now since $Ord(H) = 6 = (3)(2)$, let K be a Sylow-3-subgroup of H (observe that K is also a Sylow-3-subgroup of A_4). Then by Theorem 1.2.50 we conclude that $A_4 = HN_{A_4}(K)$ (note that $N_{A_4}(K)$ is the normalizer of K in A_4). Since $[H : K] = 2$, once again K is normal in H. Thus $H \subset N_{A_4}(K)$. Hence by Theorem 1.2.48 we have $Ord(A_4) = Ord(H)Ord(N_{A_4}(K))/Ord(H \cap N_{A_4}(K) = 6Ord(N_{A_4}(K)/6 = Ord(N_{A_4}(K)$. Hence $N_{A_4}(K) = A_4$. Thus K is normal in A_4. Hence K is unique by Theorem 1.2.46. Thus there are exactly two elements of order 3 in A_4. But $(1, 2, 3), (1, 3, 2), (1, 2, 4)$ are elements in A_4 and each is of order 3. Thus A_4 has at least 3 elements of order 3, a contradiction. Hence A_4 does not contain a subgroup of order 6.

QUESTION 2.11.27 *Let* G *be a group of order* $105 = (7)(5)(3)$*. Show that if* G *has a subgroup* H *of order* $35 = (7)(5)$*, then* G *has exactly subgroup, say* K*, of order* 7*, and hence show that* K *is normal in* G*.*

Solution : Since $[G : H] = 3$, we conclude that H is normal in G by Question 2.11.22. By Theorem 1.2.43, we conclude that H has a Sylow-7-subgroup, say K (observe that K is a Sylow-7-subgroup of G). Since $[H : K] = 5$, we conclude that K is normal in H again by Question 2.11.22. Thus $H \subset N_G(K)$. But by Theorem 1.2.50, we conclude that $[G : H] = 3$ divides $N_G(K)$. Since $H \subset N_G(K)$, we conclude that 35 divides $Ord(N_G(K))$. Since 35 divides $Ord(N_G(K))$ and 3 divides $Ord(N_G(K))$ and gcd(35, 3) = 1, we conclude that $(35)(3) = 105$ divides $Ord(N_G(K))$. Thus $N_G(K) = G$. Hence K is normal in G. Now G is unique by Theorem 1.2.46.

QUESTION 2.11.28 *(***a generalization of Question 2.11.27***) Suppose that* G *is a group of order* pqr *such that* $p > q > r$*, where* p, q, r *are prime numbers. Show that* G *has a subgroup of order* pq *if and only if* G *has exactly one subgroup of order* p*, i.e., if and only if* G *has a normal subgroup of* G *of order* p*.*

Solution : Suppose that G has a subgroup H of order pq. Since $[G : H] = r$, we conclude that H is normal in G by Question 2.11.22.

Let K be a Sylow-p-subgroup of H. Since $[H : K] = q$ and $q < p$, we conclude that K is normal in H again by Question 2.11.22. Hence $H \subset N_G(K)$, and thus pq divides $Ord(N_G(K))$. Now by Theorem 1.2.50 we conclude that r divides $Ord(N_G(K))$. Since $gcd(pq, r) = 1$ and pq divides $Ord(N_G(K))$ and r divides $Ord(N_G(K))$, we conclude that pqr divides $Ord(N_G(K))$. Thus $N_G(K) = G$. Hence K is normal in G, and thus K is unique by Theorem 1.2.46.

For the converse, suppose that G has exactly one subgroup, say K, of order p. Then K is normal in G by Theorem 1.2.46. Let D be a Sylow-q-subgroup of G. Then KD is a subgroup of G by Question 2.6.16. Now since $K \cap D = \{e\}$, we conclude that $Ord(KD) = pq$ by Theorem 1.2.48.

QUESTION 2.11.29 *Let G be an infinite group and suppose that G has a a proper subgroup H such that $[G : H] = n < \infty$. Show that G has a normal subgroup K such that neither $K = G$ nor $K = \{e\}$.*

Solution : By Theorem 1.2.56, there is a group homomorphism Φ from G into S_n such that $Ker(\Phi) \subset H$. Now $K = Ker(\Phi)$ is a normal subgroup of G. Since G is infinite and S_n is finite and $G/K \cong$ to a subgroup of S_n, we conclude that $K \neq \{e\}$. Also, since $K \subset H$ and $H \neq G$, we conclude that $K \neq G$.

QUESTION 2.11.30 *Let G be a finite group of odd order. Prove that if a is a nonidentity elements of G, then a is not a conjugate of a^{-1}, i.e., show that $a \neq g^{-1}a^{-1}g$ for every $g \in G$.*

Solution First observe that since $ord(G)$ is an odd number, $a \neq a^{-1}$ for every nonidentity element $a \in G$ (for if $a = a^{-1}$ and a is nonidentity, then $Ord(a) = 2$ which is impossible since $Ord(G)$ is an odd number). Now assume that $a = g^{-1}a^{-1}g$ for some $g \in G$, where a is nonidentity. Then a and a^{-1} are two distinct elements of G. Now let $b \in CL(a)$ (recall that CL(a) is the conjugacy class of a, see Theorem 1.2.54), Since b is a conjugate of a , b^{-1} is a conjugate of a^{-1}. Thus b^{-1} is a conjugate of a. Hence $b^{-1} \in CL(a)$. Since $b^{-1} \in CL(a)$ for every $b \in CL(a)$ and $b^{-1} \neq b$ for every $b \in CL(a)$, we conclude that $Ord(CL(a))$ is an even number. But $Ord(CL(a)) = Ord(G)/Ord(C(a))$ by Theorem 1.2.54 and $Ord(G)/Ord(C(a))$ is an odd number since $Ord(G)$ is an odd number. Thus $Ord(CL(a))$ is an odd number which is contradiction. Thus, a is not a conjugate of a^{-1} for every nonidentity element a of G.

QUESTION 2.11.31 *Let G be a group and Φ be a map from G ONTO G given by $\Phi(g) = g^{-1}$. Show that Φ is a group isomorphism if and only if G is an Abelian group.*

Solution : If G is Abelian, then it is clear that Φ is an isomorphism. Hence assume that Φ is an isomorphism. Let $g_1, g_2 \in G$. Then $\Phi(g_1g_2) = (g_1g_2)^{-1} = g_1^{-1}g_2^{-1}$. But $(g_1g_2)^{-1} = g_2^{-1}g_1{-}1$. Thus $g_2^{-1}g_1{-}1 = g_1^{-1}g_2^{-1}$. Hence $(g_2^{-1}g_1{-}1)^{-1} = (g_1^{-1}g_2^{-1})^{-1}$. Hence $g_1g_2 = g_2g_1$.

QUESTION 2.11.32 *Let G be a finite a group and Φ be an isomorphism from G ONTO G such that $\Phi(g) = g$ if and only if $g = e$ and Φ^2 is the identity map (Φ^2 means the composition of Φ with Φ). Show that G is Abelian.*

Solution : Let $K = \{g_1^{-1}\Phi(g_1) : g_1 \in G\}$. First we show that $G = K$. Suppose that $g_1^{-1}\Phi(g_1) = g_2^{-1}\Phi(g_2)$ for some $g_1, g_2 \in G$. Then $\Phi(g_1)\Phi(g_2)^{-1} = \Phi(g_1g_2{-}1) = g_1g_2{-}1$. Thus $g_1g_2^{-1} = e$ by hypothesis. Hence $g_1 = g_2$. Since G is finite and for every $g_1, g_2 \in G$ $g_1^{-1}\Phi(g_1) \neq g_2^{-1}\Phi(g_2)$, we conclude that $K = G$. Now let $x \in G$. Then $x = g^{-1}\Phi(g)$ for some $g \in G$. Thus $\Phi(x) = \Phi(g^{-1}\Phi(g)) = \Phi(g^{-1})\Phi(\Phi(g)) = \Phi(g)^{-1}g = (g^{-1}\Phi(g))^{-1} = x^{-}1$. Since $\Phi(x) = x^{-1}$ is an isomorphism, we conclude that G is Abelian by Question 2.11.31.

QUESTION 2.11.33 *Let G be a group and Φ be a group isomorphism from G Onto G such that $\Phi(g) = g^2$ for every $g \in G$. Suppose that Φ^2 is the identity map on G. Show that G is Abelian such that $Ord(g) = 3$ for every nonidentity $g \in G$. In particular, if G is finite, then show that $Ord(G) = 3^n$ for some $n \geq 1$ and $G \cong Z_3 \oplus Z_3 \cdots \oplus Z_3$ (n copies of Z_3).*

Solution : Let $g \in G$. Since $\Phi(g) = g^2$ and $\Phi(\Phi(g)) = g$, we conclude that $g = \Phi(\Phi(g)) = \Phi(g^2) = g^4$. Thus $g^3 = e$. Hence $Ord(g) = 3$ for every nonidentity $g \in G$ and $g^2 = g^{-1}$. Thus $\Phi(g) = g^2 = g^{-1}$ for every $g \in G$. Since ϕ is an isomorphism, we conclude that G is Abelian by Question 2.11.31. Suppose G is finite. Since every nonidentity element of G has order 3, we conclude that $Ord(G) = 3^n$ for some $n \geq 1$. Also, by Theorem 1.2.52, we conclude that $G \cong Z_3 \oplus Z_3 \cdots \oplus Z_3$ (n copies of Z_3).

QUESTION 2.11.34 *Show that* $G = \{\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in Z_3\}$ *is a non-Abelian group of order* 27*, under matrix multiplication such that each nonidentity element of* G *has order* 3*.*

Solution : A straight forward calculation will show that G is a group with 27 elements. Now let $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Then the entry in the first row and third column of AB is 2. But the entry in the first row and third column of BA is 1. Hence $AB \neq BA$. Thus G is non-Abelian. Let $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $a, b, c \in Z_3$. Thus $A^3 = \begin{bmatrix} 1 & 3a & 3ac+3b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}$. but $3a = 3ac + 3b = 3c = 0$ in Z_3. Hence $A^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

QUESTION 2.11.35 *Let* $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $a, b, c \in Z_n$. *Show that Thus* $A^m = \begin{bmatrix} 1 & ma & m(m-1)/2ac + mb \\ 0 & 1 & mc \\ 0 & 0 & 1 \end{bmatrix}$.

Solution : For $m = 1$, the claim is clear. Hence assume that the claim is valid for $m = k \geq 1$. We prove it for $m = k + 1$. Now $A^{k+1} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} A^k = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & ka & k(k-1)/2ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{bmatrix} =$
$\begin{bmatrix} 1 & (k+1)a & (k(k-1)/2 + k)ac & (k+1)b \\ 0 & 1 & (k+1)c & \\ 0 & 0 & 1 & \end{bmatrix} = \begin{bmatrix} 1 & (k+1)a & k(k+1)/2ac & (k+1)b \\ 0 & 1 & (k+1)c & \\ 0 & 0 & 1 & \end{bmatrix}$

QUESTION 2.11.36 *(* **a generalization of Question 2.11.34***) Let* p *be an odd prime number. Show that* $G = \{\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in Z_p\}$ *is*

a non-Abelian group of order p^3*, under matrix multiplication, such that each nonidentity element of* G *has order* p*.*

Solution :A straight forward calculation will show that G is a group with p^3 elements. Now let $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Then the entry in the first row and third column of AB is 2. But the entry in the first row and third column of BA is 1. Hence $AB \neq BA$. Thus G is non-Abelian. Let $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $a, b, c \in Z_p$. Then by Question 2.11.35, we have $A^p = \begin{bmatrix} 1 & pa & p(p-1)/2ac + pb \\ 0 & 1 & pc \\ 0 & 0 & 1 \end{bmatrix}$. but $pa = p(p-1)/2ac + pb = pc = 0$ in Z_p. Hence $A^p = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

QUESTION 2.11.37 *Give an example of a a non-Abelian group* H *of order* 3^5 *such that each element of* G *is of order* 3*. Also, give an example of a non-Abelian group* H *of order* 54 *such that* H *has an element of order* 12*.*

Solution : Let $H = Z_3 \oplus Z_3 \oplus G$, where G is the group in Question 2.11.34. Since G is non-Abelian, we conclude that H is non-Abelian. It is clear that each element of H is of order 3.

For the second part, let $H = Z_4 \oplus G$, where G is the group in Question 2.11.34. Then H a non-Abelian group and $Ord(H) = 54$. Let $a = (1, B)$, where B is a nonidentity element of G. Then by Theorem 1.2.37 $Ord(a) = lcm[Ord(1), Ord(B)] = lcm[4, 3] = 12$.