Solutions to

TOPICS IN ALGEBRA

I.N. HERSTEIN

Part II: Group Theory

Version: 1.1
Release: Jan 2013
Author: Rakesh Balhara

Preface

These solutions are meant to facilitate the deeper understanding of the book, *Topics in Algebra*, 2^{nd} edition. We have tried to stick with the notations developed in the book as far as possible. But some notations are extremely ambiguous, so to avoid confusion, we resorted to alternate commonly used notations.

The following notation changes will be found in the text:

1. a mapping T operating on an element x is represented through $T(x)$ rather than xT.
2. subgroup generated by a is represented through $\langle a \rangle$ rather than (a)

Any suggestions or errors are invited and can be mailed to: rakeshbalhara@gmail.com

Problems (Page 35)

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
(a) $G =$ set of all integers, $a \cdot b \equiv a - b$.
(b) $G =$ set of all positive integers, $a \cdot b = ab$, usual product of integers.
(c) $G = a_0, a_1, \cdots, a_6$ where

$$a_i \cdot a_j = a_{i+j} \text{ if } i + j < 7,$$
$$a_i \cdot a_j = a_{i+j} \text{ if } i + j \geq 7$$

(for instance, $a_5 \cdot a_4 = a_{5+4-7} = a_2$ since $5 + 4 = 9 > 7$).
(d) $G =$ set of all rational numbers with odd denominators, $a \cdot b \equiv a + b$, the usual addition of rational numbers.
Solution:
(a) Clearly the binary operation is well-defined. Also $a - b \in G \quad \forall a, b \in G$. So the closure property also holds good. Now $a \cdot (b \cdot c) = a \cdot (b - c) = a - (b - c) = a - b + c$. On the other hand $(a \cdot b) \cdot c = (a - b) \cdot c = (a - b) - c = a - b - c$. So $a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$. So the associativity does not hold good. Hence G is not a group.

(b) Clearly the binary operation is well-defined. Also we can check the binary operation satisfies closure and associativity too. Again 1 is the required identity as $1 \cdot a = a \cdot 1 = a$ for all positive integers a. But we can see inverse of any element except for 1 does not exist. So the existence of inverses fails. Hence G is not a group.

(c) We can easily check G is a group with a_0 as identity element and a_{7-i} as inverse element of a_i.

(d) Again we can easily check G is a group with 0 as identity and $-\frac{m}{n}$ as inverse element of $\frac{m}{n}$. ∎

2. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(a \cdot b)^n = a^n \cdot b^n$.
Solution: We resort to induction to prove that the result holds for positive integers. For $n = 1$, we have $(a \cdot b)^1 = a \cdot b = a^1 \cdot b^1$. So the result is valid for the base case. Suppose result holds for $n = k - 1$, i.e. $(a \cdot b)^{k-1} = a^{k-1} \cdot b^{k-1}$.

We need to show result also holds good for $n = k$. We have

$$\begin{aligned}(a \cdot b)^k &= (a \cdot b)^{k-1} \cdot (a \cdot b) \\ &= (a^{k-1} \cdot b^{k-1}) \cdot (a \cdot b) \\ &= (a^{k-1} \cdot b^{k-1}) \cdot (b \cdot a) \\ &= (a^{k-1} \cdot b^k) \cdot a \\ &= a \cdot (a^{k-1} \cdot b^k) \\ &= a^k \cdot b^k\end{aligned}$$

So the result holds for $n = k$ too. Therefore, result holds for all $n \in \mathbb{N}$. Next suppose $n \in \mathbb{Z}$. If $n = 0$, then $(a \cdot b)^0 = e$ where e the identity element. Therefore $(a \cdot b)^0 = e = e \cdot e = a^0 \cdot b^0$. So the result is valid for $n = 0$ too. Next suppose n is a negative integer. So $n = -m$, where m is some positive integer. We have

$$\begin{aligned}(a \cdot b)^n &= (a \cdot b)^{-m} \\ &= ((a \cdot b)^{-1})^m \text{ by definition of the notation} \\ &= (b^{-1} \cdot a^{-1})^m \\ &= ((a^{-1}) \cdot (b^{-1}))^m \\ &= (a^{-1})^m \cdot (b^{-1})^m \text{ as the result is valid for positive integers} \\ &= (a^{-m}) \cdot (b^{-m}) \\ &= a^n \cdot b^n\end{aligned}$$

So the result is valid for negative integers too. Hence the result that $(a \cdot b)^n = a^n \cdot b^n$ holds in an abelian group for all $n \in \mathbb{Z}$. ∎

3. If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$, show that G must be abelian.
Solution: We have for all $a, b \in G$

$$\begin{aligned}&(a \cdot b)^2 = a^2 \cdot b^2 \\ \Rightarrow\ &(a \cdot b) \cdot (a \cdot b) = a^2 \cdot b^2 \\ \Rightarrow\ &a \cdot ((b \cdot a) \cdot b) = a \cdot ((a \cdot b) \cdot b) \\ \Rightarrow\ &(b \cdot a) \cdot b = (a \cdot b) \cdot b \text{ as } a^{-1} \text{ exists in } G \\ \Rightarrow\ &b \cdot a = a \cdot b \text{ as } b^{-1} \text{ exists in } G\end{aligned}$$

But $b \cdot a = a \cdot b \quad \forall\ a, b \in G$ implies G is an abelian group. Hence the result. ∎

4. If G is a group in which $(a \cdot b)^i = a^i \cdot b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

Solution: Let n, $n+1$, $n+2$ be some three consecutive integers. Therefore we have

$$(a \cdot b)^n = a^n \cdot b^n \tag{1}$$
$$(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1} \tag{2}$$
$$(a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2} \tag{3}$$

Using (2) we have

$$\begin{aligned}
&(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1} \\
\Rightarrow\ &(a \cdot b)^n \cdot (a \cdot b) = a^{n+1} \cdot (b^n \cdot b) \\
\Rightarrow\ &(a^n \cdot b^n) \cdot (a \cdot b) = (a^{n+1} \cdot b^n) \cdot b, \text{ Using (1)} \\
\Rightarrow\ &((a^n \cdot b^n) \cdot a) \cdot b = (a^{n+1} \cdot b^n) \cdot b \\
\Rightarrow\ &(a^n \cdot b^n) \cdot a = (a^n \cdot a) \cdot b^n \\
\Rightarrow\ &a^n \cdot (b^n \cdot a) = a^n \cdot (a \cdot b^n) \\
\Rightarrow\ &b^n \cdot a = a \cdot b^n \qquad (4)
\end{aligned}$$

Again using (3), analogously we have

$$\begin{aligned}
&b^{n+1} \cdot a = a \cdot b^{n+1} \\
\Rightarrow\ &b \cdot (b^n \cdot a) = a \cdot b^{n+1} \\
\Rightarrow\ &b \cdot (a \cdot b^n) = a \cdot b^{n+1}, \text{ Using (4)} \\
\Rightarrow\ &(b \cdot a) \cdot b^n = (a \cdot b) \cdot b_n \\
\Rightarrow\ &b \cdot a = a \cdot b
\end{aligned}$$

So we have $a \cdot b = b \cdot a \quad \forall\ a, b \in G$. And hence G is abelian. ∎

5. Show that the conclusion of the Problem 4 does not follow if we assume the relation $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers.
Solution: Suppose $(a \cdot b)^i = a^i \cdot b^i$ for $i = n$ and $i = n+1$. We claim G is abelian if and only if $(a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2}$. Clearly, from last Problem we have $(a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2} \Rightarrow G$ is abelian. Also if G is abelian, then $(a \cdot b)^i = a^i \cdot b^i \quad \forall\ i \in \mathbb{Z}$; in particular result holds for $i = n+2$. Thus G is abelian if and only if $(a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2}$. So the result of Problem 4 might not follow if we assume $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers. ∎

6. In S_3 give an example of two elements x, y such that $(x \cdot y)^2 \neq x^2 \cdot y^2$.
Solution: We assume, as described in Example 2.2.3, $S_3 = \{e, \psi, \psi^2, \phi, \phi \cdot \psi, \psi \cdot \phi\}$ with $\psi^3 = e$, $\phi^2 = e$ and $\phi \cdot \psi^i \cdot \phi = \psi^{-i}$. We choose $x = \psi$ and $y = \phi$. We have

$$(\psi \cdot \phi)^2 = (\psi \cdot \phi) \cdot (\psi \cdot \phi) = \psi \cdot (\phi \cdot \psi \cdot \phi) = \psi \cdot \psi^{-1} = e$$

Whereas

$$\psi^2 \cdot \phi^2 = \psi^2 \cdot e = \psi^2$$

Thus $(\psi \cdot \phi)^2 \neq \psi^2 \cdot \phi^2$. ∎

7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.
Solution: Again, as in Problem 6, we assume $S_3 = \{e, \psi, \psi^2, \phi, \phi \cdot \psi, \psi \cdot \phi\}$ with $\psi^3 = e$, $\phi^2 = e$. We have $(e)^2 = e$; $(\psi)^2 = \psi^2$; $(\psi^2)^2 = \psi$; $(\phi)^2 = e$; $(\phi \cdot \phi)^2 = e$; $(\phi \cdot \phi)^2 = e$. Thus $e, \phi, \psi \cdot \psi, \psi \cdot \phi$ are the elements with their square equal to identity. Also we have $(e)^3 = e$; $(\psi)^3 = e$; $(\psi^2)^3 = e$; $(\phi)^3 = \phi$; $(\phi \cdot \psi)^3 = \phi \cdot \psi$; $(\psi \cdot \phi)^3 = \psi \cdot \phi$. Thus we have e, ψ, ψ^2 with their square equal to identity. Hence the result. ∎

8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.
Solution: Since G is finite, we assume $G = \{g_1, g_1, \cdots, g_m\}$ for some positive integer m. For some $g_i \in G$, consider the sequence $g_i, g_i^2, g_i^3, \cdots$. Since G is finite and closed under binary operation, so there must be repetition in the sequence, i.e. $g_i^j = g_i^k$ for some positive integers j and k with $j > k$. But that means $g_i^{j-k} = e$, where e is the identity element. Let $j - k = n_i$. Thus we have n_i corresponding to every g_i such that $g_i^{n_i} = e$. Let $N = n_1 \times n_2 \times \cdots \times n_m$. But then $g_i^N = e$ for all i, showing the existence of required positive integer N. ∎

9. (a) If the group G has three elements, show it must be abelian.
(b) Do part (a) if G has four elements.
(c) Do part (a) if G has five elements.
Solution:
(a) Let G be a group of order 3 and some $a, b \in G$ with $a \neq b$.
Case 1, Either of a or b equals to the identity element: Suppose $a = e$ then $a \cdot b = e \cdot b = b = b \cdot e = b \cdot a$. Similarly, if $b = e$, we have $a \cdot b = b \cdot a$. Thus if either a or b equals to e, we have $a \cdot b = b \cdot a$.
Case 2, Neither of a or b is identity element: Consider $a \cdot b$. We have $a \cdot b \neq a$, otherwise it would mean $b = e$. Similarly $a \cdot b \neq b$ as $a \neq e$. Also G has only three elements, so $a \cdot b$ has not option but to be equal to the identity element. Therefore $a \cdot b = e$. A similar argument will show that $b \cdot a = e$. Thus $a \cdot b = b \cdot a$ in this case too.
So we have $a \cdot b = b \cdot a \quad \forall\, a, b \in G$. Hence G is abelian for $o(G) = 3$.

(b) Again let G be the group of order 4 and let some $a, b \in G$.
Case 1, Either of a, b equals to e: In this case, clearly $a \cdot b = b \cdot a$.
Case 2, Neither of a, b equals to e. Consider $a \cdot b$. Clearly, $a \cdot b \neq a$ and $a \cdot b \neq b$. But since G has four elements, let $c \neq e$ be the fourth element. So $a \cdot b$ has two

options, either equals to e or equals to c.

- If $a \cdot b = e$, then $a = b^{-1} \Rightarrow b \cdot a = b \cdot b^{-1} \Rightarrow b \cdot a = e$. Thus $a \cdot b = b \cdot a = e$.
- If $a \cdot b = c$, then consider $b \cdot a$. Clearly, $b \cdot a \neq a$ and $b \cdot a \neq b$. So $b \cdot a$ has only two options, either $b \cdot a = e$ or $b \cdot a = c$. But if $b \cdot a = e$, then it would imply $a \cdot b = e$, which is not true. So $b \cdot a = c$ too. Thus $a \cdot b = b \cdot a = c$.

Thus we have $a \cdot b = b \cdot a$ for all $a, b \in G$. Hence G is abelian for $o(G) = 4$.

(c) For this part, we have to make use of the material not presented till now in the book. Since the order of G is prime, therefore it is cyclic. But a cyclic group is abelian, so G must be abelian for order 5. ∎

10. Show that if every element of the group G has its own inverse, then G is abelian.
Solution: Let some $a, b \in G$. So we have $a^{-1} = a$ and $b^{-1} = b$. Also $a \cdot b \in G$, therefore $a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$. So we have $a \cdot b = b \cdot a$, showing G is abelian. ∎

11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.
Solution: We prove the result by contradiction. Note that G is a finite group. Suppose there is no element x satisfying $x^2 = e$ except for $x = e$. Thus if some $g \neq e$ belongs to G, then $g^2 \neq e$, i.e. $g \neq g^{-1}$. It means every non-identity element g has another element g^{-1} associated with it. So the non-identity elements can be paired into mutually disjoint subsets of order 2. We can assume the count of these subsets equals to some positive integer n as G is a finite group. But then counting the number of elements of G, we have $o(G) = 2n + 1$, where 1 is added for the identity element. So G is a group of odd order, which is not true. Hence there must exist an element $a \neq e$ such that $a^2 = e$ for G is a group of even order. ∎

12. Let G be a nonempty set closed under the an associative product, which in addition satisfies:
(a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
(b) Give $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$.
Prove that G must be a group under this product.
Solution: In order to show G is a group, we need to show

1. $e \cdot a = a \quad \forall\, a \in G$, and
2. If $a \cdot y(a) = e$, then $y(a) \cdot a = e$.

Suppose some $a \in G$, therefore there exists $y(a) \in G$ such that $a \cdot y(a) = e$. Again $y(a) \in G$ implies there exists $y(y(a)) \in G$ such that $y(a) \cdot y(y(a)) = e$.

So we have

$$\begin{aligned} y(a)\cdot a &= (y(a)\cdot a)\cdot e \\ &= (y(a)\cdot a)\cdot (y(a)\cdot y(y(a))) \\ &= ((y(a)\cdot a)\cdot y(a))\cdot y(y(a)) \\ &= (y(a)\cdot (a\cdot y(a)))\cdot y(y(a)) \\ &= (y(a)\cdot e)\cdot y(y(a)) \\ &= y(a)\cdot y(y(a)) \\ &= e \end{aligned}$$

Thus

$$y(a)\cdot a = e \tag{1}$$

Now using (1), we have $e\cdot a = (a\cdot y(a))\cdot a = a\cdot (y(a)\cdot a) = a\cdot e = a$. Thus

$$e\cdot a = a \tag{2}$$

Form (1) and (2), we conclude G is a group. ∎

13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead:
(a′) There exists an $e \in G$ such that $a\cdot e = a$ for all $a \in G$.
(b′) Given $a \in G$, there exists $y(a) \in G$ such that $y(a)\cdot a = e$

Solution: Consider $G = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \mid a, b \in \mathbb{Q}^+ \right\}$ with usual matrix multiplication as binary operation '$\cdot$', where $\mathbb{Q}^+$ denotes the positive rational numbers. We define $e = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Also for $M = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$, we define $y(M) = \frac{1}{a+b}e$. One can easily see that $M\cdot e = M$ and $y(M)\cdot M = e$. Also G is not a group as inverses do not exist. ∎

14. Suppose a *finite* set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.
Solution: Since G is a finite group, so we can assume $G = \{g_1, g_2, \ldots, g_n\}$, for some positive integer n. Let some $a \in G$. Consider $S = \{a\cdot g_1, a\cdot g_2, \cdots, a\cdot g_n\}$. We assert each element of S is distinct as if $a\cdot g_i = a\cdot g_j$ with $g_i \neq g_j$, then left-cancellation implies $g_i = g_j$. Therefore, $o(S) = o(G)$, combining with the fact that $S \subset G$, we conclude $S = G$. So if $a \in G$, therefore $a \in S$. But that means $a = a\cdot g_k$, for some $g_k \in G$. We claim g_k is the right-identity. For establishing our claim, we consider $S' = \{g_1\cdot a, g_2\cdot a, \cdots, g_n\cdot a\}$. Again since right-cancellation too holds good, proceeding in an analogous way, we can see $S' = G$. Let some $x \in G$. So $x \in S'$, therefore $x = g_i\cdot a$ for some $g_i \in G$. Now $x\cdot g_k = (g_i\cdot a)\cdot g_k = g_i\cdot (a\cdot g_k) = g_i\cdot a = x$. Thus we have shown, $x\cdot g_k = x \quad \forall\, x \in G$. So g_k is the right-identity. Now, since $g_k \in G$, therefore

$g_k \in S$. So $g_k = a \cdot g_l$, for some $g_l \in G$. But that shows the existence of right-inverse g_l, for an arbitrarily chosen element $a \in G$. Thus right-inverse exists for each element in G. With the existence of right-identity and right-inverses, we concluded that G is group. ∎

15. (a) Using the result of Problem 14, prove that the nonzero integers modulo p, p a prime number, form a group under multiplication mod p.
(b) Do part (a) for the nonzero integers relatively prime to n under multiplication mod n.
Solution:
(a) Let G be the set consists of non-zero integers modulo p. We noticed that G is a finite set with multiplication mod p as well-defined binary operation. Using Problem 14, G would be a group if we show that the multiplication mod p is associative and the both cancellation laws hold good. One can easily see that $a \otimes (b \otimes c) = (a \otimes b) \otimes c = abc \bmod p$. So associativity is not an issue. Next suppose $a \otimes b = a \otimes c$, we need to show that it would imply $b = c$. But $a \otimes b = a \otimes c \Rightarrow ab = ac \bmod p \Rightarrow a(b-c) = 0 \bmod p \Rightarrow p \mid a(b-c)$. But p being prime, so either $p \mid a$ or $p \mid b-c$. Since $p \nmid a$, so $p \mid (b-c)$. Also $p \nmid b$ and $p \nmid c$, so $p \mid (b-c)$ implies $b - c = 0$, or $b = c$. Thus left-cancellation law holds good. Similarly we can see right-cancellation also holds good. Using previous problem, we conclude G is a group.
(b) Let G be the set consists of non-zero integers relatively prime to n. Clearly G is a finite set. Also multiplication mod n is well-defined binary operation over G. To show G is a group under multiplication mod n, we need to show that associativity and both cancellation laws hold good. It is easy to see that $a \otimes (b \otimes c) = (a \otimes b) \otimes c = abc \bmod n$. So associativity holds good. Next suppose $a \otimes b = a \otimes c$. But that means $ab = ac \bmod n \Rightarrow a(b-c) = 0 \bmod n \Rightarrow n \mid a(b-c)$. But $\gcd(a, n) = 1$, therefore $n \mid a(b-c)$ implies $n \mid (b-c)$. Also $\gcd(b, n) = \gcd(c, n) = 1$, therefore $n \mid (b-c)$ implies $b = c$. Thus we see left-cancellation holds good. Similarly, we can check right-cancellation too holds good. And so G is a group. ∎

16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.
Solution: We construct a set G with $n \geq 2$ elements, equipped with a binary operation $\cdot : G \times G \longrightarrow G$ such that $x \cdot y = y$. Clearly the binary operation $\cdot$ is well-defined. Next, we see $x \cdot (y \cdot z) = y \cdot z = z$. Also $(x \cdot y) \cdot z = z$. Thus the binary operation is associative. Next we check left-cancellation. Suppose we have $x \cdot y = x \cdot z$. But $x \cdot y = y$ and $x \cdot z = z$. Thus $x \cdot y = x \cdot z \Rightarrow y = z$, showing left-cancellation holds good. On the other hand, if we have $x \cdot y = z \cdot y$, we cannot conclude $x = z$ as $x \cdot y = z \cdot y = y \quad \forall x, z \in G$. Thus right-cancellation does not hold good. Finally, we prove G is not a group. Suppose G is group, therefore it must have the identity element. Let e be the identity element. But then $x \cdot e = e \quad \forall x \in G$, showing all elements are identity elements. Thus we get

$G = \{e\}$, but we have assumed G has n elements with $n \geq 2$, hence a contradiction. Thus G has no identity element. Hence G is not a group. So if a finite set with well-defined binary operation is satisfying associativity and one sided cancellation law, it need not to be a group under that binary operation. ∎

17. Prove that in Problem 14 infinite examples exist, satisfying the conditions, which are not groups.
Solution: We define $A_n = \{in \mid i \in \mathbb{Z}^+\}$, where n is a positive integer greater than 1. Clearly A_n with usual multiplication as binary operation satisfies all conditions of Problem 14, but is not a group as inverses do not exist for all elements. Also since there are infinite positive integers greater than 1, so we have infinite examples satisfying the conditions of Problem 14 but are not groups. ∎

18. For any $n > 2$, construct a non-abelian group of order $2n$. (*Hint:* imitate the relation in S_3)
Solution: Let G be the group that we are going to construct. Let $\cdot$ denotes its binary operation and let e be its identity element. Thus we have constructed an element of G, which is e. Next we construct an element $a \neq e$ with order $n \geq 3$. Thus we have constructed n element, which are $e, a, a^2, \cdots, a^{n-1}$. Finally we construct an element other than already constructed, b, with order 2, i.e. $b^2 = e$. We interconnect a, b with the rule: $b \cdot a \cdot b^{-1} = a^{-1}$. We claim we have got $2n$ elements, i.e. $G = \{e, a, a^2, \cdots, a^{n-1}, b, b \cdot b, \cdots, b \cdot a^{n-1}\}$. To establish our claim, we first notice that $b \cdot a^i \cdot b = a^{-i}$. With this rule at hand, one can easily check any expression resulting from the product of a^i and b^j will belongs to those $2n$ elements. To give readers more insight, suppose we have some expression $a^i \cdot b^j \cdot a^k$. Now either $j = 0$ or $j = 1$. If $j = 0$, then expression equals to a^{i+k}, and thus belong to G. Whereas if $j = 1$, then let $x = a^i \cdot b \cdot a^k$. We have $b \cdot x = (b \cdot a^i \cdot b) \cdot a^k = a^{-i} \cdot a^k = a^{k-i}$. Left-multiplying by b, we get $x = b \cdot a^{k-i}$. Thus $x \in G$. Also $a \cdot b = b \cdot a^{-1}$; since $n \neq 2$, therefore $a \cdot b \neq b \cdot a$. Thus we have got G, a non-abelian group of order $2n$. ∎

19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1 a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4))$; use induction on n)
Solution: Let X_n denote a expression we get by bracketing the n elements, keeping the order of elements same. We need to show all expressions X_n are same for all n. We will use induction over n. For $n = 1$ and $n = 2$, we have only one expression possible, so trivially all expressions are same. For $n = 3$, we have two ways of bracketing $a_1 a_2 a_3$, i.e $a_1 \cdot (a_2 \cdot a_3)$ and $(a_1 \cdot a_2) \cdot a_3$. Since the binary operation $\cdot$ is satisfying associativity, therefore both expression are same. Next suppose the result is true for $n \leq i-1$. We need to show that the result is equally true for $n = i$. Let X_i be some expression. Then it must be product of some two shorter expressions, i.e $X_i = Y_\alpha \cdot Z_{i-\alpha}$, where $\alpha < i$. But all expressions

with number of elements less than i are same. So $Y_\alpha = a_1 \cdot Y_{\alpha-1}^{'}$, where $Y_{\alpha-1}^{'}$ is some expression consists of $\alpha - 1$ elements. Similarly, $Z_{i-\alpha} = a_{\alpha+1} \cdot Z_{i-\alpha-1}^{'}$. Thus we have

$$\begin{aligned} X_i &= Y_\alpha \cdot Z_{i-\alpha} \\ &= (a_1 \cdot Y_{\alpha-1}^{'}) \cdot (a_{\alpha+1} \cdot Z_{i-\alpha-1}^{'}) \\ &= a_1 \cdot X_{i-1}^{'}, \end{aligned}$$

where $X_{i-1}{}'$ is some expression of $i-1$ terms. But all expressions containing $i-1$ terms are same (order of elements is assumed to remain same). But then all expression having i elements turns out to be equal to $a_1 \cdot X_{i-1}^{'}$. Thus all expressions having i elements are same. The induction hypothesis implies result is valid for all n. Hence the result. ∎

20. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that the G forms a group under matrix multiplication.
Solution: It is easy to check that G is a group under matrix multiplication, with $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as identity element and $\frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ as inverse element of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Note that $ad - bc \neq 0$ is given and of the inverses exist for all elements. ∎

21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?
Solution: We have G closed under multiplication as $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \in G$. Now since $ad \neq 0$, therefore G forms a group under matrix multiplication with $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as identity element and $\begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix}$ as inverse element of $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Finally we have $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ implies $ab' + bd' = a'b + b'd$. Since $ab' + bd' \neq a'b + b'd$ for all values of a, b, d, a', b', d', so G is not an abelian. ∎

22. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.

Solution: Easy to check G is a group under multiplication. Also we have

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a' & 0 \\ 0 & a'^{-1} \end{pmatrix} = \begin{pmatrix} a' & 0 \\ 0 & a'^{-1} \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ 0 & a^{-1}a'^{-1} \end{pmatrix}$$

Hence G is abelian too. ∎

23. Construct in the G of Problem 21 a subgroup of order 4.
Solution: Let $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Clearly $a^2 = I$ and $b^2 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Also $ab = ba = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Thus $H = \{I, a, b, ab\}$ forms a subgroup of G. ∎

24. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplication as the operation in G, prove that G is a group of order 6.
Solution: Its trivial to check that

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Hence $o(G) = 6$ ∎

25. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3, relative to matrix multiplication. Show $o(G) = 48$.
(b) If we modify the example of G in part (a) by insisting that $ad - bc = 1$, then what is $o(G)$?
Solution: See Problem 26, which is general case of this problem. ∎

*26. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are the integers modulo p, p being a prime number, such that $ad - bc \neq 0$. G forms group relative to matrix multiplication. What is $o(G)$?
(b) Let H be the subgroup of the G of part (a) defined by

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}.$$

What is $o(H)$?
Solution:
(a) We will first count the number of ways in which $ad - bc = 0$. We separate

this counting into two cases. In first case we count the ways when $ad = bc = 0$. In second case, we will count the number of ways in which $ad = bc \neq 0$.
Case 1: $ad = bc = 0$: When $a = 0$, we can choose d in p ways; and when $d = 0$, we can choose a in p ways. But in this $a = d = 0$ has been counted twice. Therefore there are $2p - 1$ ways in which $ad = 0$. Similarly, $bc = 0$ in $2p - 1$ ways. Thus there are $(2p - 1)^2$ ways in which $ad = bc = 0$.
Case 2: $ad = bc \neq 0$: Since $ad \neq 0$, therefore $a \neq 0$ and $d \neq 0$. Similarly, $b \neq 0$ and $c \neq 0$. We chose some value of $a \neq 0$ in $p - 1$ ways; some value of $d \neq 0$ in $p - 1$ ways; some value of b in $p - 1$ ways; then find the value of c with these chosen values of a, d, b. Since $ad = bc \bmod p$ has unique solution in c for non-zero values of a, d, b; thus we get unique value of c. Thus $ad = bc \neq 0$ can be chosen in $(p - 1)^3$ ways.
Finally, the number ways of choosing a, b, c, d with $ad - bc \neq 0$ equals number ways of choosing a, b, c, d without any restriction minus the number of ways of choosing a, b, c, d with $ad - bc = 0$. Thus the number of ways of choosing a, b, c, d with $ad - bc \neq 0$ is $p^4 - (p - 1)^3 - (2p - 1)^2$. On simplification, we get

$$o(G) = p^4 - p^3 - p^2 + p$$

(b) We separate our counting of a, b, c, d for which $ad - bc = 1$ in three separate cases.
Case 1: $ad = 0$: This restrict $bc = -1$. The number ways of choosing a, d for which $ad = 0$ is: $2p - 1$. On the other hand, the number of ways of choosing b, c for which $bc = -1$ is: $p - 1$. Thus when $ad = 0$, we can choose a, b, c, d in $(2p - 1)(p - 1)$
Case 2: $bc = 0$: Analogous to previous case, we get number of ways of choosing a, b, c, d as $(2p - 1)(p - 1)$.
Case 3: $ad \neq 0$ and $bc \neq 0$: In this case we get number of ways of choosing a, b, c, d as $(p - 1)(p - 1)$
Thus total number of ways of choosing a, b, c, d for which $ad - bc = 1$ is: $2(2p - 1)(p - 1) + \sum_{p-2} (p - 1)^2$. On simplifying we get

$$o(G) = p^3 - p \quad \blacksquare$$

Problems (Page 46)

1. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite of infinite, is again a subgroup of G?)
Solution: Let some $x, y \in H \cap K$. Therefore $x \in H$ and $y \in H$. But H being a subgroup, so $xy^{-1} \in H$. Again $x \in K$ and $y \in K$. K being subgroup implies $xy^{-1} \in K$. But $xy^{-1} \in H$ and $xy^{-1} \in K$ implies $xy^{-1} \in H \cap K$. Thus we have for all $x, y \in H \cap K$, $xy^{-1} \in H \cap K$. Hence $H \cap K$ is a subgroup of G.

Problems (Page 70)

1. Are the following mappings automorphisms of their respective groups?
(a) G group of integers under addition, $T : x \to -x$.
(b) G group of positive reals under multiplication, $T : x \to x^2$.
(c) G cyclic group of order 12, $T : x \to x^3$.
(d) G is the group S_3, $T : x \to x^{-1}$
Solution:
(a) Yes, as G is an abelian group.

(b) No, as mapping is not a homomorphism.

(c) No, as if $G = \langle a \rangle$, then $o(a) = 12$, while $o(T(a)) = 4$, showing T is not an automorphism. Note that an isomorphism preserve the order of elements.

(d) No, as G is a non-abelian group, so the mapping $T : x \longrightarrow x^{-1}$ fails to be a homomorphism. ∎

2. Let G be a group, H a subgroup of G, T an automorphism of G. Let $T(H) = \{T(h) \mid h \in H\}$. Prove $T(H)$ is a subgroup of G.
Solution: We need to show $T(H)$ is a subgroup of G. Let $x, y \in T(H)$, therefore $x = T(h_1)$ and $y = T(h_2)$ for some $h_1, h_2 \in H$. But then $xy^{-1} = T(h_1)(T(h_2))^{-1} = T(h_1)T(h_2^{-1}) = T(h_1 h_2^{-1}) = T(h_3)$ for some $h_3 \in H$ as H is a subgroup of G. So $xy^{-1} \in T(H) \quad \forall\, x, y \in H$. This shows $T(H)$ is a subgroup of G. ∎

3. Let G be a group, T an automorphism of G, N a normal subgroup of G. Prove that $T(N)$ is a normal subgroup of G.
Solution: We need to show $T(N)$ is a normal subgroup of G. Clearly by last Problem, $T(N)$ is a subgroup of G. Let some $g \in G$, therefore $g = T(g')$ for some $g' \in G$ as T is an onto mapping. But then $gT(N)g^{-1} = T(g')T(N)T(g')^{-1} = T(g')T(N)T(g'^{-1}) = T(g'Ng'^{-1}) = T(N)$ as N is normal in G. Thus we have $gT(N)g^{-1} = T(N) \quad \forall\, g \in G$. Hence $T(N)$ is normal in G. ∎

4. For $G = S_3$ prove that $G \approx \mathscr{I}(G)$.
Solution: We have, from Lemma 2.8.2

$$\frac{G}{Z} \approx \mathscr{I}(G) \tag{1}$$

Also we claim for S_n with $n \geq 3$, we have $Z = \{I\}$, where I is the identity mapping. We assume $A = \{x_1, x_2, \cdots, x_n\}$ is the set of elements on which mappings from S_n operate. Suppose some $T \in S_n$ with $T \neq I$, therefore there is some x_i such that $T(x_i) \neq x_i$. Let $T(x_i) = x_j$, where $i \neq j$. Since $n \geq 3$, therefore we

can have x_k with $k \neq i$ and $k \neq j$. Define $T' : A \longrightarrow A$ such that $T'(x_i) = x_i$; $T'(x_j) = x_k$; $T'(x_k) = x_j$; and $T'(x_l) = x_l$ for the rest of $x_l \in A$. But then $TT'(x_i) = T(T'(x_i)) = T(x_i) = x_j$; and $T'T(x_i) = T'(T(x_i)) = T'(x_j) = x_k$, showing $TT' \neq T'T$. So if some $T \neq I$, then $TT' \neq T'T$ for some $T' \in S_n$. Thus $T \notin Z \quad \forall\ T \neq I$; implying $Z = \{I\}$. Finally, using (1), we have $S_n \approx \mathscr{I}(S_n) \quad \forall\ n \geq 3$ ∎

5. For any group G prove that $\mathscr{I}(G)$ is a normal subgroup of $\mathscr{A}(G)$ (the group $\mathscr{A}(G)/\mathscr{I}(G)$ is called the *group of outer automorphisms* of G).
Solution: We have some change of notations, so we prefer to give detailed solution of this problem. We define $T_g : G \longrightarrow G$ such that $T_g(x) = gxg^{-1}$ (Note that this is different from what is given in the book). Clearly $T_g \in \mathscr{A}(G)$ for all $g \in G$. Next, we define $\mathscr{I}(G) = \{T_g \mid g \in G\}$. Let some some T_{g_1}, $T_{g_2} \in \mathscr{I}(G)$. But then for all $x \in G$, we have $T_{g_1}T_{g_2}(x) = T_{g_1}(T_{g_2}(x)) = T_{g_1}(g_2xg_2^{-1}) = g_1(g_2xg_2^{-1})g_1^{-1} = (g_1g_2)x(g_1g_2)^{-1} = T_{g_1g_2}(x)$. Thus $T_{g_1}T_{g_2} = T_{g_1g_2}$. But $T_{g_1g_2} \in \mathscr{I}(G)$, therefore $T_{g_1}T_{g_2} \in \mathscr{I}(G)$. Again let some $T_g \in \mathscr{I}(G)$, therefore for all $x \in G$, we have $T_g(x) = gxg^{-1}$. So we have, for all $x \in G$

$$\begin{aligned}
& T_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} \\
\Rightarrow\ & T_g(g^{-1}xg) = x \\
\Rightarrow\ & T_g^{-1}(T_g(g^{-1}xg)) = T_g^{-1}(x) \\
\Rightarrow\ & g^{-1}xg = T_g^{-1}(x) \\
\Rightarrow\ & T_g^{-1}(x) = (g^{-1})x(g^{-1})^{-1} \\
\Rightarrow\ & T_g^{-1}(x) = T_{g^{-1}}(x)
\end{aligned}$$

Thus $T_g^{-1} = T_{g^{-1}}$. But $T_{g^{-1}} \in \mathscr{I}(G)$, therefore $T_g^{-1} \in \mathscr{I}(G)$. Hence $\mathscr{I}(G)$ is a subgroup of $\mathscr{A}(G)$. Finally, suppose some $T \in \mathscr{A}(G)$ and some $T_g \in \mathscr{I}(G)$, then we have for all $x \in G$

$$\begin{aligned}
TT_gT^{-1}(x) &= T(T_g(T^{-1}(x))) \\
&= T(g(T^{-1}(x))g^{-1}) \\
&= T(g)T(T^{-1}(x))T(g^{-1}) \\
&= T(g)x(T(g))^{-1} \\
&= T_{T(g)}(x)
\end{aligned}$$

Thus $TT_gT^{-1} = T_{T(g)}$. But $T_{T(g)} \in \mathscr{I}(G)$. Thus $TT_gT^{-1} \in \mathscr{I}(G) \quad \forall\ T \in \mathscr{A}(G)$. Hence $\mathscr{I}(G)$ is a normal subgroup in $\mathscr{A}(G)$. ∎

6. Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. Determine $\mathscr{A}(G)$.

Solution: The possible proper subgroups of G are $\{e, a\}$, $\{e, b\}$, $\{e, ab\}$. We aim at finding a mapping T which is an automorphism. Since T is homomorphism, therefore $T(e) = e$. Also once we have found $T(a)$ and $T(b)$, the value of $T(ab)$ get decided by itself as $T(ab) = T(a)T(b)$. Now what could be the possible values of $T(a)$ so that T is an automorphism. Since $o(a) = 2$, so $o(T(a))$ must be 2. The elements with order 2 are a, b, ab, so $T(a)$ has three choices namely a, b, ab. Once $T(a)$ is decided, what could be the possible values for $T(b)$. Again order of b is 2, so the order of $T(b)$ must be 2. Again we have three possible candidates, a, b, ab, out of which one has already been fixed to $T(a)$. So $T(b)$ has two choices. Thus we have $3 \times 2 = 6$ possible automorphisms. Thus

$$\mathscr{A}(G) = \left\{ \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & b & a & ab \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & b & ab & a \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & a & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & b & a \end{pmatrix} \right\} \quad \blacksquare$$

7. (a) A subgroup C of G is said to be a *characteristic subgroup* of G if $T(C) \subset C$ for all automorphisms T of G. Prove a characteristic subgroup of G must be a normal subgroup of G.
(b) Prove that the converse of (a) is false.
Solution:
(a) We, for some $g \in G$, define $T_g : G \longrightarrow G$ such that $T_g(x) = gxg^{-1}$. It is routine to check T_g is an automorphism of G for all $g \in G$. But it is given that $T(C) \subset C$ for all automorphisms T. So $T_g(C) \subset C \quad \forall\, g \in G$. But that means $gCg^{-1} \subset C$, or $gcg^{-1} \in C \quad \forall\, g \in G \;\&\; \forall\, c \in C$. Thus C is normal in G.

(b) We simply give an example to show that converse of part(a) need not be true. For $G = \{e, a, b, ab\}$ with $a^2 = e$, $b^2 = e$ and $ab = ba$; and $C = \{e, a\}$; and $T = \begin{pmatrix} e & a & b & ab \\ e & b & a & ab \end{pmatrix}$, we have C is a normal subgroup of G but $T(C) \nsubseteq C$. Note that T defined above is an automorphism of G. $\blacksquare$

8. For any group G, prove that the commutator subgroup G' is a characteristic subgroup of G. (See Problem 5, Section 2.7)
Solution: Let $U = \{xyx^{-1}y^{-1} \mid x, y \in G\}$. So $G' = \langle U \rangle$. Also if some $u \in U$, then $u^{-1} \in U$ too. So if some $a \in G'$, then $a = \prod_{i \in \Lambda} x_i y_i x_i^{-1} y_i^{-1}$, where Λ is

some finite index set. But then

$$\begin{aligned} T(a) &= T(\prod_{i\in\Lambda} x_i y_i x_i^{-1} y_i^{-1}) \\ &= \prod_{i\in\Lambda} T(x_i y_i x_i^{-1} y_i^{-1}) \\ &= \prod_{i\in\Lambda} T(x_i)T(y_i)T(x_i^{-1})T(y_i^{-1}) \\ &= \prod_{i\in\Lambda} T(x_i)T(y_i)(T(x_i))^{-1}(T(y_i))^{-1} \\ &= \prod_{i\in\Lambda} x_i' y_i' x_i'^{-1} y_i'^{-1} \end{aligned}$$

So $T(a) \in G' \quad \forall\ a \in G'$. Thus $T(G') \subset G'$. Hence G' is a characteristic subgroup of G. ∎

9. If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.
Solution: Let some $g \in G$. We define $T_g : G \longrightarrow G$ such that $T_g(x) = gxg^{-1}$. Clearly T_g is an automorphism of G. Also $T_g(N) = N$ as N is given to be normal in G. Now consider $T_g : N \longrightarrow N$. Since $T_g(N) = N$, one can easily see T_g is an automorphism of N too. But then $T_g(M) \subset M$ as M is given to be a characteristic subgroup of N. So $gMg^{-1} \subset M \quad \forall g \in G$, or $gmg^{-1} \in M \quad \forall\ g \in G\ \&\ \forall m \in M$. Hence M is normal in G. ∎

10. Let G be a finite group, T an automorphism of G with the property that $T(x) = x$ for $x \in G$ if and only if $x = e$. Prove that every $g \in G$ can be represented as $g = x^{-1}T(x)$ for some $x \in G$.
Solution: First note that G is given to be a finite group. We define mapping $\phi : G \longrightarrow G$ such that $\phi(x) = x^{-1}T(x)$. Clearly mapping so defined is well-defined. Also

$$\begin{aligned} \phi(a) = \phi(b) &\Rightarrow a^{-1}T(a) = b^{-1}T(b) \\ &\Rightarrow T(a)(T(b))^{-1} = ab^{-1} \\ &\Rightarrow T(ab^{-1}) = ab^{-1} \end{aligned}$$

But $T(x) = x$ implies $x = e$, so $\phi(a) = \phi(b)$ implies $ab^{-1} = e$, i.e. $a = b$. Thus mapping ϕ is one-to-one. But since G is finite, therefore ϕ being one-to-one implies ϕ is onto too. But onto implies that if some $g \in G$, then it has its pre-image in G, i.e. $g = x^{-1}T(x)$ for some $x \in G$. Hence every element g of G can be represented as $x^{-1}T(x)$ for some $x \in G$. ∎

11. Let G be a finite group, T an automorphism of G with the property that $T(x) = x$ if and only if $x = e$. Suppose further that $T^2 = I$. Prove that G must be abelian.

Solution: Using previous problem, if some $g \in G$, then $g = x^{-1}T(x)$ for some $x \in G$. So we have $T(g) = T(x^{-1}T(x)) = T(x^{-1})T(T(x)) = (T(x))^{-1}T^2(x) = (T(x))^{-1}x = (x^{-1}T(x))^{-1} = g^{-1}$. Thus $T(g) = g^{-1} \quad \forall\ g \in G$. Now let $a, b \in G$. So we have

$$T(ab) = (ab)^{-1} = b^{-1}a^{-1} \tag{1}$$

Also

$$T(ab) = T(a)T(b) = a^{-1}b^{-1} \tag{2}$$

Using (1) and (2), we have

$$b^{-1}a^{-1} = a^{-1}b^{-1} \Rightarrow ab = ba$$

So we have $ab = ba \quad \forall\ a, b \in G$. Hence G is an abelian group. ∎

*12. Let G be a finite group and suppose the automorphism T sends more than three-quarters of the elements of G onto their inverses. Prove that $T(x) = x^{-1}$ for all $a \in G$ and that G is abelian.

Solution: Define a set $H = \{x \in G \mid T(x) = x^{-1}\}$. So we have $o(H) > \frac{3}{4}n$. Let some $h \in H$. Consider the set Hh. Clearly $o(Hh) > \frac{3}{4}n$. Therefore $o(H \cap Hh) > \frac{n}{2}$. Let some $x \in H \cap Hh$. Therefore $x = h_1$ and $x = h_2h$, for some $h_1, h_2 \in H$. Also since $x \in H \cap Hh \subset H$, therefore $T(x) = x^{-1}$. So

$$T(x) = x^{-1} = h_1^{-1} \tag{1}$$

$$T(x) = x^{-1} = (h_2h)^{-1} = h^{-1}h_2^{-1} \tag{2}$$

$$T(x) = T(h_2h) = T(h_2)T(h) = h_2^{-1}h^{-1} \tag{3}$$

Using (2) and (3), we get $h^{-1}h2^{-1} = h2^{-1}h^{-1}$, or $hh_2 = h_2h$. Also $h_2 = xh^{-1}$, so $hh_2 = h_2h \Rightarrow hxh^{-1} = xh^{-1}h \Rightarrow hx = xh$. Thus we have

$$hx = xh \quad \forall\ x \in H \cap Hh \tag{4}$$

Now consider $N(h)$, i.e. normalizer subgroup of h. The equation (4) implies $H \cap Hh \subset N(h)$. So $o(N(h)) > \frac{n}{2}$. But $N(h)$ being a subgroup of G, therefore $o(N(h)) \mid o(G)$, forcing $N(h) = G$. But that means $hg = gh \quad \forall\ g \in G$. So $h \in Z \quad \forall\ h \in H$, where Z is the center subgroup of G. So $o(Z) > \frac{3}{4}n$. Again Z being a subgroup of G, so $o(Z) \mid o(G)$, forcing $Z = G$. But $Z = G$ implies G is abelian. Also if G is abelian, then if some $x, y \in H$, we have $T(xy^{-1}) = T(x)T(y^{-1}) = x^{-1}(y^{-1})^{-1} = x^{-1}y = (y^{-1}x)^{-1} = (xy^{-1})^{-1}$, showing xy^{-1} too belongs to H. Hence with G abelian, H becomes a subgroup of G. But then $o(H) \mid o(G)$, therefore $H = G$ as $o(H) > \frac{3}{4}n$. But $H = G$ implies

$T(x) = x^{-1} \quad \forall\, x \in G$, what we need to show. ∎

13. In Problem 12, can you find an example of a finite group which is non-abelian and which has an automorphism which maps exactly three-quarters of the elements of G onto their inverses?
Solution: Consider the Quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Let $T = \begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ 1 & -1 & -i & i & -j & j & k & -k \end{pmatrix}$. We left it to the reader to check T is an automorphism of Q which transfer exactly $\frac{3}{4}$ elements of Q into their inverses. ∎

*14. Prove that every finite group having more than two elements has a non-trivial automorphism.
Solution: Let G be some group with order greater than 2. Now either G is non-abelian, or G is abelian. If G is non-abelian, then we have $Z \neq G$, where Z is the center subgroup of G. So there is some $g \in G$ such that $g \notin Z$. We define for some $g \notin Z$, mapping $T : G \longrightarrow G$ such that $T(x) = gxg^{-1}$. We claim T so defined is an automorphism which is not equal to identity mapping. T is an automorphism of G is easy to check. Also if $T = I$, then $T(x) = x \quad \forall\, x \in G$. But that means $gxg^{-1} = x \Rightarrow gx = xg \quad \forall\, x \in G$, i.e. $g \in Z$ which is not the case. So $T \neq I$. So for non-abelian groups, we have found a non-trivial automorphism.

When G is abelian, either $x^2 = e$ for all $x \in G$ or there is some $x_0 \in G$ such that $x_0^2 \neq e$. If there is some $x_0 \in G$ such that $x_0^2 \neq e$, then we claim that the mapping $T : G \longrightarrow G$ such that $T(x) = x^{-1}$ is a non-trivial automorphism of G. Since G is abelian, T surely is an automorphism. Also if $T = I$, then we have $x^{-1} = x \quad \forall\, x \in G$, i.e $x^2 = e \quad \forall\, x \in G$, which is not the case. So T is a non-trivial automorphism of G.

On the other hand, if G is abelian, with $x^2 = e \quad \forall\, x \in G$, then for some positive integer m

$$G \approx \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{m \text{ times}}$$

Note that here we have assumed G to be finite. But then there exist m independent symbols, $a_1, a_2, \cdots, a_m$ with $o(a_i) = 2 \quad \forall\, i$. By independent we mean $a_i \neq \prod_{j \in \Lambda} a_j$ for any index set Λ. So

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_m \rangle$$

Also $o(G) \geq 3$ guarantees us the existence of atleast two such independent symbols, say a_1 and a_2. We define a mapping $T : G \longrightarrow G$ such that $T(a_1) = a_2$, $T(a_2) = a_1$ and for the rest of independent symbols a_i, $T(a_i) = a_i$. Once defined

for independent symbols, we extend it for all elements of G using:

$$T(\prod_{j\in\Lambda} a_j) = \prod_{j\in\Lambda} T(a_j)$$

Clearly extending T this way for all elements of G makes T a homomorphism. Also we can check T is onto. Thus we have found an automorphism of G which is not equal to an identity mapping. Hence every finite group with order greater than 2 has a non-trivial automorphism. ∎

*15. Let G be a group of order $2n$. Suppose that half of the elements of G are of order 2, and the other half form a subgroup H of order n. Prove that H is of odd order and is an abelian subgroup of G.

Solution: Let K denotes the set of all elements with order 2. Therefore $G = H \cup K$. Also the index of H in G is 2, so H is a normal subgroup of G (See problem 2, page 53). Let some $k \in K$, therefore $k^{-1} = k$. Also H being normal in G implies $kHk^{-1} = H$. Let some $h \in H$, therefore $h = kh_1k^{-1}$ for some $h_1 \in H$. So we have $h = kh_1k^{-1} \Rightarrow hk = kh_1$; but $hk \in K$ (Why), so $hk = (hk)^{-1}$. Thus $kh_1 = hk = (hk)^{-1} = k^{-1}h^{-1} = kh^{-1} \Rightarrow h_1 = h^{-1}$. Thus we have $h = kh^{-1}k \quad \forall\ h \in H$. Now let some $x, y \in H$, therefore $x = kx^{-1}k$, and $y = ky^{-1}k$. So

$$xy = (kx^{-1}k)(ky^{-1}k) = kx^{-1}kky^{-1}k = kx^{-1}y^{-1}k \tag{1}$$

Also

$$xy = k(xy)^{-1}k = ky^{-1}x^{-1}k \tag{2}$$

Using (1) and (2), we have

$$\begin{aligned} kx^{-1}y^{-1}k = ky^{-1}x^{-1}k &\Rightarrow x^{-1}y^{-1} = y^{-1}x^{-1} \\ &\Rightarrow yx = xy \end{aligned}$$

So $xy = yx \quad \forall x, y \in H$. Hence H is an abelian subgroup of G Also since there is no element with order 2, so order of H is odd (See Problem 11, page 35). ∎

*16. Let $\phi(n)$ be the Euler ϕ-function. If $a > 1$ is an integer, prove that $n \mid \phi(a^n - 1)$.

Solution: Let G be a cyclic group of order $a^n - 1$. The existence of such G is guaranteed (Why). Therefore $G = \langle x \rangle$ for some $x \in G$. Define mapping $T : G \longrightarrow G$ such that $T(y) = y^a$. Now since $\gcd(a, a^n - 1) = 1$, therefore T is an automorphism of G, i.e $T \in \mathscr{A}(G)$. Also $T^2(y) = TT(y) = T(y^a) = y^{a^2}$. So we have $T^n(y) = y^{a^n}$. But $y^{a^n - 1} = e$, where e is the identity element of G, therefore $y^{a^n} = y$. So $T^n(y) = y \quad \forall\ y \in G$. Therefore $T^n = I$, where I is the identity mapping. Next suppose for some positive integer $m < n$, we have $T^m = I$. Then we have $T^m(y) = y \quad \forall\ y \in G$, in particular, we have $T^m(x) = x$. But

$T^m(x) = x \Rightarrow x^{a^m} = x \Rightarrow x^{a^m-1} = e \Rightarrow o(x) < a^n - 1$, which is not true. Thus n is the smallest possible integer for which $T^n = I$. Thus $o(T) = n$ in $\mathscr{A}(G)$. Also G being finite cyclic group, therefore $o(\mathscr{A}(G)) = \phi(o(G)) = \phi(a^n - 1)$. So by Lagrange Theorem, we get $n \mid \phi(a^n - 1)$. ∎

17. Let G be a group and Z the center of G. If T is any automorphism of G, prove that $Z(T) \subset Z$.
Solution: We need to show that Z is a characteristic subgroup of G. For some automorphism mapping T, we need to show $T(Z) \subset Z$. Let some $z \in T(Z)$, therefore there exist some $x \in Z$ such that $T(x) = z$. But $x \in Z$ implies $xg = gx \quad \forall\ g \in G$. Since mapping T is one-to-one, therefore we have $T(xg) = T(gx) \quad \forall\ g \in G$. But $T(xg) = T(gx) \Rightarrow T(x)T(g) = T(g)T(x) \Rightarrow zT(g) = T(g)z \quad \forall\ g \in G$. But since T is onto, therefore $zT(g) = T(g)z \quad \forall\ g \in G \Rightarrow zg' = g'z \quad \forall\ g' \in G$, which says $z \in Z$. Therefore $z \in T(Z) \Rightarrow z \in Z$. So $T(Z) \subset Z$. ∎

18. Let G be a group and T an automorphism of G. If, for $a \in G$, $N(a) = \{x \in G \mid xa = ax\}$, prove that $N(T(a)) = T(N(a))$.
Solution: We need to show $N(T(a)) = T(N(a)) \quad \forall\ a \in G\ \&\ T \in \mathscr{A}(G)$. We have $N(T(a)) = \{x \in G \mid xT(a) = T(a)x\}$. But since T is an onto mapping, therefore

$$\begin{aligned} N(T(a)) &= \{T(x') \mid x' \in G\ \&\ T(x')T(a) = T(a)T(x')\} \\ &= \{T(x') \mid x' \in G\ \&\ T(x'a) = T(ax')\} \\ &= \{T(x') \mid x' \in G\ \&\ x'a = ax'\}; \text{ since mapping is one-to-one} \\ &= \{T(x') \mid x' \in N(a)\} \\ &= T(N(a)) \quad \blacksquare \end{aligned}$$

19. Let G be a group and T an automorphism of G. If N is normal subgroup of G such that $T(N) \subset N$, show how you could use T to define an automorphism of G/N.
Solution:
20. Use the discussion following Lemma 2.8.3 to construct
(a) a non-abelian group of order 55.
(b) a non-abelian group of order 203.
Solution:
21. Let G be the group of order 9 generated by elements a, b, where $a^3 = b^3 = e$. Find all automorphisms of G.
Solution: Again, as in Problem 6, we are going to exploit the fact that an automorphism leaves the order of elements unchanged. G has four non-trivial subgroups, which are $\{e, a, a^2\}$; $\{e, b, b^2\}$; $\{e, a^2b, ab^2\}$; $\{e, ab, a^2b^2\}$. Now the element e has not choice but has to map to itself, so only 1 choice. The element

a has 8 choices for being get mapped as all elements other than e has same order as a has. Once image of a is fixed, the image of a^2 get fixed by itself as $T(a^2) = T(a)T(a)$. So a^2 has no choice. Next after fixing image of e, a, a^2, the element b has only 6 choices left. But fixing the image of a and$b$ fixes the image of remaining elements. So $b^2, ab, a^2b^2, a^2b, ab^2$ have no choices. Thus the total automorphisms of G are $8 \times 6 = 48$. So $o(\mathscr{A}(G)) = 48$. ∎

Problems (Page 74)

1. Let G be a group; consider the mappings of G into itself, λ_g, defined for $g \in G$ by $\lambda_g(x) = xg$ for all $x \in G$. Prove that λ_g is one-to-one and onto, and that $\lambda_{gh} = \lambda_h\lambda_g$.
Solution: We start with one-to-one. Suppose $\lambda_g(x) = \lambda_g(y)$. But $\lambda_g(x) = \lambda_g(y) \Rightarrow xg = yg \Rightarrow x = y$. So $\lambda_g(x) = \lambda_g(y)$ implies $x = y$, showing λ_g is one-to-one mapping. Next we tackle onto. Suppose some $y \in G$. But then for $x = yg^{-1} \in G$, we have $\lambda_g(x) = (yg^{-1})g = y$. This shows x is the inverse-image of y. Thus λ_g is onto too. Finally, we have $\lambda_{gh}(x) = xgh = (\lambda_g(x))h = \lambda_h(\lambda_g(x)) = \lambda_h\lambda_g(x)$ for all $x \in G$. Thus $\lambda_{gh} = \lambda_h\lambda_g$. ∎

2. Let λ_g be defined as in Problem 1, τ_g as in the proof of Theorem 2.9.1. Prove that for any $g, h \in G$, the mappings λ_g, τ_h satisfy $\lambda_g\tau_h = \tau_h\lambda_g$. (*Hint:* For $x \in G$ consider $\lambda_g\tau_h(x)$ and $\tau_h\lambda_g(x)$.)
Solution: We recap our notation, mapping $\lambda_g : x \longrightarrow xg$ and $\tau_h : x \longrightarrow hx$. Now we have for all $x \in G$, $\lambda_g\tau_h(x) = \lambda_g(\tau_h(x)) = \lambda_g(hx) = hxg = \tau_h(xg) = \tau_h(\lambda_g(x)) = \tau_h\lambda_g(x)$. Thus $\lambda_g\tau_h = \tau_h\lambda_g$. ∎

3.If θ is one-to-one mapping of G onto itself such that $\lambda_g\theta = \theta\lambda_g$ for all $g \in G$, prove that $\theta = \tau_h$ for some $h \in G$.
Solution: We are given θ is an one-to-one and onto mapping with $\lambda_g\theta = \theta\lambda_g \quad \forall\, g \in G$. So we have $\lambda_g\theta(x) = \theta\lambda_g(x) \quad \forall\, g, x \in G \Rightarrow \theta(x)g = \theta(xg) \quad \forall\, g$, $x \in G$. Since it holds for all $x \in G$, in particular must hold for $x = e$. Thus we have $\theta(e)g = \theta(g)$. Since $\theta(e) \in G$, so we let $\theta(e) = h$ for some $h \in G$. Thus we have $\theta(g) = hg \quad \forall\, g \in G$. But that means $\theta = \tau_h$, hence the result. ∎

4. (a) If H is a subgroup of G show that for every $g \in G$, gHg^{-1} is a subgroup of G.
(b) Prove that $W =$ intersection of all gHg^{-1} is a normal subgroup of G.
Solution:
(a) Consider gHg^{-1} for some $g \in G$. Let $x, y \in gHg^{-1}$, therefore $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. But then $xy^{-1} = gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} = gh_3g^{-1}$ for some $h_3 \in H$. Thus $xy^{-1} \in gHg^{-1} \quad \forall\, x, y \in gHg^{-1}$. Hence gHg^{-1} is a subgroup of G for all $g \in G$.

(b) We have $W = \bigcap_{g\in G} gHg^{-1}$. Let some $x \in G$. Consider xWx^{-1}. We have $xWx^{-1} = x(\bigcap_{g\in G} gHg^{-1})x^{-1} = \bigcap_{g\in G} x(gHg^{-1})x^{-1} = \bigcap_{g\in G} xgHg^{-1}x^{-1} = \bigcap_{g\in G} (xg)H(xg)^{-1}$. But since the mapping $\phi : G \longrightarrow G$ such that $\phi(g) = xg$ is an onto mapping, so $xWx^{-1} = \bigcap_{g\in G} (xg)H(xg)^{-1} = \bigcap_{g'\in G} g'Hg'^{-1} = W$. But

$xWx^{-1} = W \quad \forall\, x \in G$ implies W is normal in G. ∎

5. Using Lemma 2.9.1 prove that a group of order p^2, where p is a prime number, must have a normal subgroup of order p.
Solution: Let G be a group with order p^2. Since $p \mid o(G)$ and p is a prime number, therefore the Cauchy's Theorem guarantees us existence of an element a of order p. Let $H = \langle a \rangle$. Therefore H is a subgroup of order p. Now since $p^2 \nmid p!$, therefore we have $o(G) \nmid i_G(H)!$. So using Lemma 2.9.1, we have $K_\theta \neq \{e\}$, along with $K_\theta \subset H$ and K_θ normal in G. But then $o(H) = p$, a prime number, forces $K_\theta = H$. Thus H is normal in G. ∎

6. Show that in a group G of order p^2 any normal subgroup of order p must lie in the center of G.
Solution: Let H be the normal subgroup of G. Let some $h \in H$ and some $g \in G$. We have $ghg^{-1} \in H$ as H is normal in G. If $h = e$, then we have $ghg^{-1} = h$, or $gh = hg \quad \forall\, g \in G$. Next we assume $h \neq e$, so $H = \langle h \rangle$. Now since the $o(g) \mid o(G)$, therefore $o(g) = 1, p, p^2$. When $o(g) = 1$, then we have $g = e$, and so $ghg^{-1} = g$, or $hg = hg$. When $o(g) = p$, we have $ghg^{-1} \in H$. Since $H = \langle h \rangle$, therefore $ghg^{-1} = h^i$ for some positive integer $i < p$. With this have $h = g^p h g^{-p} = g^{p-1}(ghg^{-1})g^{-(p-1)} = g^{p-1}(h^i)g^{-(p-1)} = \cdots = h^{i^p}$. So $h^{i^p - 1} = e$, but $o(h) = p$, therefore $p \mid i^p - 1$, or $i^p = 1 \bmod p$. But we have, from Fermat theorem $i^p = i \ mod\ p$. From these two equations, we conclude $i = 1 \bmod p$, or $i = 1$. Thus we have $ghg^{-1} = h$, or $gh = hg$, for all $h \in H$ and for all g of order p. Finally, when $o(g) = p^2$, we have $G = \langle g \rangle$, therefore G is abelian and we have $gh = hg$ in this case too. Thus we concluded $gh = hg$ for all $h \in H$ and for all $g \in G$. And so $h \in Z \quad \forall\, h \in H$, where Z is the center subgroup of G. Hence $H \subset Z$. ∎

7. Using the result of Problem 6, prove that any group of order p^2 is abelian.
Solution: Let G be a group with order p^2. Problem 5 implies that there exist a normal subgroup H of order p. But since p is a prime number, therefore $H = \langle a \rangle$ for some $a \in H$. But since $o(G) = p^2$, therefore there exist $b \in G$ such that $b \notin H$. Let $K = \langle b \rangle$. Now order of b divides order of G, therefore $o(b) = 1$ or p or p^2. If $o(b) = 1$, then we have $b = e \in H$, which is contravene our assumption. So $o(b) \neq 1$. Next if $o(b) = p$, then since $o(G) \nmid i_G(K)!$, we have K too normal in G. Therefore, Problem 6 implies $H, K \subset Z$. And so $HK \in Z$. But $o(HK) = o(H)o(K)/o(H \cap K) = p^2$ as $H \cap K = \{e\}$. Therefore $o(Z) \geq p^2$, forcing $Z = G$, making G an abelian group. Finally if $o(b) = p^2$, then we have $G = \langle b \rangle$ and hence abelian in this case too. So we concluded G is an abelian group. ∎

8. If p is a prime number, prove that any group G of order $2p$ must have a

subgroup of order p, and that this subgroup is normal in G.
Solution: Cauchy Theorem guarantees the existence of an element $a \in G$ such that $o(a) = p$. But then $H = \langle a \rangle$ is a subgroup of G with $o(H) = p$. Also since $2p \nmid 2!$, therefore $o(G) \nmid i_G(H)!$. But then there exists a normal subgroup K of G inside H with $K \neq \{e\}$. So we have $o(K) \mid o(H)$ and with $o(H)$ being prime forces $K = H$. Thus H is normal in G. ∎

9. If $o(G)$ is pq where p and q are distinct prime numbers and if G has a normal subgroup of order p and a normal subgroup of order q, prove that G is cyclic.
Solution: We are given a group G with $o(G) = pq$, where p, q are prime numbers. Also we are given H, K normal subgroups of G with $o(H) = p$ and $o(K) = q$. So we have $H = \langle a \rangle$ for some $a \in H$; and $K = \langle b \rangle$ for some $b \in K$. Also since p and q are distinct primes, so we have $H \cap K = \{e\}$. We claim $ab = ba$. To establish our claim, consider $aba^{-1}b^{-1}$. We have $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = ah$ for some $h \in H$. Therefore $aba^{-1}b^{-1} \in H$. Again, $aba^{-1}b^{-1} = (aba^{-1})b^{-1} = kb^{-1}$ for some $k \in K$. Therefore $aba^{-1}b^{-1} \in K$. So $aba^{-1}b^{-1} \in H \cap K = \{e\}$. That is $aba^{-1}b^{-1} = e \Rightarrow ab = ba$. Next we claim $o(ab) = pq$, so that $G = \langle ab \rangle$, i.e. a cyclic group. We have $(ab)^{pq} = a^{pq}b^{pq}$, as $ab = ba$. Therefore $(ab)^{pq} = a^{pq}b^{pq} = (a^p)^q(b^q)^p = e^q e^p = e$. Therefore $pq \mid o(ab)$. Suppose for some positive integer t with $t < pq$, we have $(ab)^t = e$. But $(ab)^t = e \Rightarrow a^t b^t = e \Rightarrow a^t = b^{-t} \Rightarrow a^{tq} = (b^q)^{-t} \Rightarrow a^{tq} = e \Rightarrow o(a) \mid tq \Rightarrow p \mid tq \Rightarrow p \mid t$ as $\gcd(p, q) = 1$. Similarly, we have $q \mid t$. But then we have $pq \mid t$, implying $t > pq$ as $p \neq 0$, which is against our assumption. So we have pq as the smallest positive integer for which $(ab)^{pq} = e$, implying $o(ab) = pq$. Thus $G = \langle ab \rangle$ and is cyclic. ∎

*10. Let $o(G)$ be pq, $p > q$ are primes, prove
(a) G has a subgroup of order p and a subgroup of order q.
(b) If $q \nmid p - 1$, then G is cyclic.
(c) Given two primes $p, q, q \mid p - 1$, there exists a non-abelian group of order pq.
(d) Any two non-abelian groups of order pq are isomorphic.
Solution:
(a)

Problems (Page 80)

1. Find the orbit and cycles of the following permutations:
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$
   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

Solution:
(a) Clearly $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix} = (1,2,3,4,5)(6)(7)(8,9)$. So orbit of 1, 2, 3, 4 and 5 is the set $\{1,2,3,4,5\}$; orbit of 6 is 6; orbit of 7 is 7; orbit of 8 and 9 is the set $\{8,9\}$. Also $(1,2,3,4,5)$ and $(8,9)$ are its cycles.

(b) Again $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix} = (1,6,2,5)(3,4)$. So the orbit of 1, 2, 5 and 6 is the set $\{1,2,5,6\}$; and the orbit of 3 and 4 is the set $\{3,4\}$. Also $(1,6,2,5)$ and $(3,4)$ are its cycles. ∎

2. Write the permutation in the Problem 1 as the product of disjoint cycles.
Solution: We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix} = (1,2,3,4,5)(6)(7)(8,9)$ and $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix} = (1,6,2,5)(3,4)$. ∎

3. Express as the product of disjoint cycles:
   (a) $(1,5)(1,6,7,8,9)(4,5)(1,2,3)$.
   (b) $(1,2)(1,2,3)(1,2)$.

Solution:
(a) Let $(1,5)(1,6,7,8,9)(4,5)(1,2,3) = \tau$. So we have $\tau = \tau_1\tau_2\tau_3\tau_4$, where $\tau_1 = (1,5)$, $\tau_2 = (1,6,7,8,9)$, $\tau_3 = (4,5)$ and $\tau_4 = (1,2,3)$. Now

$$\begin{aligned} \tau(1) &= \tau_1\tau_2\tau_3\tau_4(1) \\ &= \tau_1(\tau_2(\tau_3(\tau_4(1)))) \\ &= \tau_1(\tau_2(\tau_3(2))) \\ &= \tau_1(\tau_2(2)) \\ &= \tau_1(2) \\ &= 2 \end{aligned}$$

Repeating analogously, we have $\tau(2) = 3$; $\tau(3) = 6$; $\tau(6) = 7$; $\tau(7) = 8$; $\tau(8) = 9$; $\tau(9) = 5$; $\tau(5) = 4$; and $\tau(4) = 1$. Thus we have $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 6 & 1 & 4 & 7 & 8 & 9 & 5 \end{pmatrix} = (1,2,3,6,7,8,9,5,4)$.

(b) Proceeding as in part (a), we have $(1,2)(1,2,3)(1,2) = (1,3,2)$. ∎

4. Prove that $(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$.
Solution: One can easily check $(1, 2, \ldots, n)(n, n-1, \ldots, 1) = I$, where I is the identity permutation. Hence $(1, 2, \ldots, n)^{-1} = (n, n-1, \ldots, 1)$. ∎

5. Find the cycle structure of all the powers of $(1, 2, \ldots, 8)$.
Solution: Let $(1, 2, 3, 4, 5, 6, 7, 8) = \tau$. So we have

$$\begin{aligned}
\tau^2 &= \tau\tau = (1,2,3,4,5,6,7,8)(1,2,3,4,5,6,7,8) \\
&= (1,3,5,7)(2,4,6,8) \\
\tau^3 &= \tau^2\tau = (1,3,5,7)(2,4,6,8)(1,2,3,4,5,6,7,8,9) \\
&= (1,4,7,2,5,8,3,6) \\
\tau^4 &= \tau^3\tau = (1,4,7,2,5,8,3,6)(1,2,3,4,5,6,7,8,9) \\
&= (1,5)(2,6)(3,7)(4,8) \\
\tau^5 &= \tau^4\tau = (1,5)(2,6)(3,7)(4,8)(1,2,3,4,5,6,7,8,9) \\
&= (1,6,3,8,5,2,7,4) \\
\tau^6 &= \tau^5\tau = (1,6,3,8,5,2,7,4)(1,2,3,4,5,6,7,8,9) \\
&= (1,7,5,3)(2,8,6,4) \\
\tau^7 &= \tau^6\tau = (1,7,5,3)(2,8,6,4)(1,2,3,4,5,6,7,8,9) \\
&= (1,8,7,6,5,4,3,2) \\
\tau^8 &= \tau^7\tau = (1,8,7,6,5,4,3,2)(1,2,3,4,5,6,7,8,9) \\
&= (1)(2)(3)(4)(5)(6)(7)(8) = I
\end{aligned}$$

So for $i \in \mathbb{Z}$, we have $\tau^i = \tau^{i \bmod 8}$