11. Let G be a group and $a, b \in G$. Show that $o(a) = o(b^{-1}ab)$

Proof: Let $o(a)$ be finite and $o(a) = n$. Then $a^n = e$, e is the identity element in G. Now, $(b^{-1}ab)^n = (b^{-1}ab)(b^{-1}ab)\dots(b^{-1}ab)$ n times

$= b^{-1}a^n b$ (you can also use mathematical induction)

$= b^{-1}eb = e$

So, $o(b^{-1}ab)$ is finite. If possible, let $\exists$ a positive integer $k < n$ such that $(b^{-1}ab)^k = e$, Then $b^{-1}a^k b = e$ or, $a^k = e$, a contradiction that $o(a) = n$. So, $o(b^{-1}ab) = n$ (by definition).

Let $o(a)$ be infinite. If possible, let $o(b^{-1}ab)$ be finite and $o(b^{-1}ab) = p$. Then $(b^{-1}ab)^p = e \Rightarrow b^{-1}a^p b = e$

$\Rightarrow a^p = e$, a contradiction that $o(a)$ is infinite.

So, $o(b^{-1}ab)$ is infinite.

So, in both cases, $o(a) = o(b^{-1}ab)$

12. Find all elements of order 10 in the group $(\mathbb{Z}_{30}, +)$.

Solution: The elements of the groups are $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{29}$. Here $o(\bar{0}) = 1$ and $o(\bar{1}) = 30$. Now $o(\bar{m}) = o(m\bar{1}) = \frac{30}{\gcd(30, m)}$ [As $o(a) = n \Rightarrow o(a^m) = \frac{n}{\gcd(m,n)}$ for some positive integer m]

So, $o(\bar{m}) = 10 \Rightarrow \gcd(30, m) = 3$

So, $\frac{m}{3}$ and $\frac{30}{3} = 10$ are prime to each other

i.e., $\frac{m}{3}$ is less than 10 and prime to 10

So, $\frac{m}{3} = 1, 3, 7, 9$ or, $m = 3, 9, 21, 27$

Hence the elements of order 10 are $\bar{3}, \bar{9}, \overline{21}$, and $\overline{27}$.

13. Let G be a group and $a \in G$ be the unique element of order n and $a \neq e$ (e is the identity element in G). Then prove that $n = 2$ and $a \in Z(G)$ (the centre of the group).

Proof: Here $o(a) = n$. As a is the unique element of order n, $a = a^{-1}$ as $o(a) = o(a^{-1}) = n$. So, $a^2 = e$ and as $a \neq e$,
So, $o(a) = 2 = n$. So, $n = 2$.
Now, also $a = xax^{-1}$ (as $o(a) = o(xax^{-1})$) for any $x \in G$.
So, $ax = xa$ for each $x \in G$.
So $a \in Z(G)$

14. If a, b are any two elements in a group G. Show that ab and ba have the same order.

Proof: we first prove that $(ba)^{n+1} = b(ab)^n a$ for any positive integer n by induction.

$(ba)^2 = (ba)(ba) = b(ab)a$. So, the result is true for $n=1$. Assume the result is true for some positive integer k. i.e., $(ba)^{k+1} = b(ab)^k a$

Now, $(ba)^{k+2} = (ba)(ba)^{k+1} = (ba)(b(ab)^k a)$
$= b(ab)(ab)^k a = b(ab)^{k+1} a$

So, the result is true for $k+1$. So by the principle of mathematical induction $(ba)^{n+1} = b(ab)^n a$ for any positive integer n.
Similarly, we can prove that $(ab)^{n+1} = a(ba)^n b$ for any positive integer n.
Now, let $o(ab)$ be finite and $o(ab) = m$. Then $(ab)^m = e$, e is the identity element in G.

Now $(ba)^{m+1} = b(ab)^m a = bea = ba$
So, $(ba)^m = e$ (by Cancellation law)

If possible let there be positive integer $p < n$ such that $(ba)^p = e$. Now, $(ab)^{p+1} = a(ba)^p b = aeb = ab$
or, $(ab)^p = e$ (by Cancellation law)

which is a contradiction that $o(ab) = n$. So, $o(ba) = n$ (by definition).

Let $o(ab)$ be infinite. If possible, let $o(ba)$ is finite and $o(ba) = n$. Then $(ab)^{n+1} = a(ba)^n b = aeb = ab$ (as $(ba)^n = e$)

or, $(ab)^n = e$ (by cancellation law). So, $o(ab)$ is finite, a contradiction.

So, $o(ba)$ is infinite.

15. Show that if G is a group of even order then there are exactly an odd number of elements of order 2.

Proof: Let $x \in G$ and $x^2 \neq e$ (e is the identity in G). Then $x \neq x^{-1}$ and also $(x^{-1})^2 \neq 2$ because if $(x^{-1})^2 = e$ $x^{-2} = e$ or $x^2 = e$, a contradiction. So there are even number of elements such that $x^2 \neq e$. Hence, there are an even number of elements x such that $x^2 = e$. Because e is one of these elements, there are odd number of elements of order 2.

16. Let S be a non-empty subset of a group G, and let $C(S) = \{x \in G : xs = sx, \text{ for all } s \in S\}$. Show that $C(S)$ is a subgroup of G. What is $C(G)$?

Proof: As, $es = se = s$ for all $s \in S$, e is the identity in G, so, $e \in C(S)$. So, $C(S)$ is non-empty

Now let $x, y \in C(S) \Rightarrow xs = sx$ and $ys = sy$, for all $s \in S$

Now $xys = xsy = sxy$, for all $s \in S$. So $xy \in C(S)$

Let $y \in C(S)$. Then $ys = sy$ for all $s \in S$

So, $y^{-1}s = sy^{-1}$, for all $s \in S$.

Hence $y^{-1} \in C(S)$. So, $C(S)$ is a subgroup of G.

$C(G)$ is the centre of the group G which we denote by $Z(G)$.

17. Prove that an infinite cyclic group has exactly two generators.

Proof: Let $G = \langle a \rangle$ be an infinite cyclic group generated by a. Let $b \in G$ be another generator of G, so that $G = \langle b \rangle$. Since $b \in G$, we have $b = a^m$, for some integer m, and similarly, since $a \in G$, we have $a = b^n$ for some integer n

So, $a = b^n = (a^m)^n = a^{mn}$ or, $a^{mn-1} = e = a^0$. Since, all the powers of a are distinct in an infinite cyclic group, we have $mn - 1 = 0$ or ~~m~~ $mn = 1$. Hence $m = \pm 1$, showing $b = a^{-1}$ is the only other generator of G.

18. Give an example of a nonabelian group each of whose subgroups ~~are~~ is normal.

Solution: Consider the quaternion group Q_8 (Example 4 in Page-6) Here the only subgroup of order 2 is $\{I, -I\}$ which is trivially normal. All the subgroups of order 4 have index 2, and hence (by worked out exercise 1 of Page-34) are normal in G. Hence Q_8 is the desired group.

19. If G is a group with centre $Z(G)$ and if $G/Z(G)$ is cyclic, then prove that G must be abelian.

Proof: Let $G/Z(G) = \langle xZ(G) \rangle$, $x \in G$. Let $a, b \in G$ Then $aZ(G)$ is an element of $G/Z(G)$. So, $aZ(G) = (xZ(G))^m$
$= x^m Z(G)$ for some integer m

So, $a = x^m y$ for some $y \in Z(G)$. Similarly, $b = x^n z$, for some $z \in Z(G)$ and some integer n, so that

$ab = (x^m y)(x^n z) = x^m y x^n z = x^m x^n y z = x^{m+n} y z$, as $y \in Z(G)$

Also $ba = (x^n z)(x^m y) = x^n z x^m y = x^n x^m z y = x^{n+m} z y = x^{m+n} y z$ as $m+n = n+m$, and $y, z \in Z(G)$

So, $ab = ba$. Hence G is abelian.

20. If N and M are normal subgroups of G. Prove that NM is also a normal subgroups of G.

Proof: Let $h \in NM$ Then $h = nm$, $n \in N$, $m \in M$

As N is normal, $xnx^{-1} \in N$, for all $x \in G$. As M is normal, $xmx^{-1} \in M$, for all $x \in G$.

Now, $xhx^{-1} = xnmx^{-1} = (xnx^{-1})(xmx^{-1}) \in NM$ for all $x \in G$

So, NM is a normal subgroup

[As, N, M are normal subgroups of G, $NM = MN$, so NM is a subgroup of G].

21. Show that the order of each element of the Quotient group $\mathbb{Q}/\mathbb{Z}$ is finite

Proof: Let $\frac{a}{b} \in \mathbb{Q}$ such that a is an integer and b is a positive integer. Consider $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$

Now $b\left(\frac{a}{b} + \mathbb{Z}\right) = a + \mathbb{Z} = \mathbb{Z}$ Hence order of $\frac{a}{b} + \mathbb{Z}$ is finite. So, ~~each element~~ order of each element of $\mathbb{Q}/\mathbb{Z}$ is finite.

22. Show that there does not exist any group G such that $o\left(G/Z(G)\right) = 37$

Proof: If possible, let there be a group G such that $o\left(G/Z(G)\right) = 37$

As 37 is prime, so $G/Z(G)$ is cyclic. As $G/Z(G)$ is cyclic then G is abelian (by ex. 19 of Page-62)

But G is abelian $Z(G) = G$. So, $o\left(G/Z(G)\right) \neq 37$, a contradiction. So, there does not exist such a group.