# Exercises from
# ***Abstract Algebra***
# by I. N. Herstein

**Exercise 2.1.18** If $G$ is a finite group of even order, show that there must be an element $a \neq e$ such that $a = a^{-1}$.

*Proof.* First note that $a = a^{-1}$ is the same as saying $a^2 = e$, where $e$ is the identity. I.e. the statement is that there exists at least one element of order 2 in $G$. Every element $a$ of $G$ of order at least 3 has an inverse $a^{-1}$ that is not itself – that is, $a \neq a^{-1}$. So the subset of all such elements has an even cardinality (/size). There's exactly one element with order 1 : the identity $e^1 = e$. So $G$ contains an even number of elements -call it $2k$– of which an even number are elements of order 3 or above – call that $2n$ where $n < k$– and exactly one element of order 1 . Hence the number of elements of order 2 is

$$2k - 2n - 1 = 2(k - n) - 1$$

This cannot equal 0 as $2(k - n)$ is even and 1 is odd. Hence there's at least one element of order 2 in $G$, which concludes the proof. □

**Exercise 2.1.21** Show that a group of order 5 must be abelian.

*Proof.* Suppose $G$ is a group of order 5 which is not abelian. Then there exist two non-identity elements $a, b \in G$ such that $a * b \neq b * a$. Further we see that $G$ must equal $\{e, a, b, a * b, b * a\}$. To see why $a * b$ must be distinct from all the others, not that if $a *\ b = e$, then $a$ and $b$ are inverses and hence $a * b = b * a$. Contradiction. If $a * b = a$ (or $= b$ ), then $b = e$ (or $a = e$ ) and $e$ commutes with everything. Contradiction. We know by supposition that $a * b \neq b * a$. Hence all the elements $\{e, a, b, a * b, b * a\}$ are distinct.

Now consider $a^2$. It can't equal $a$ as then $a = e$ and it can't equal $a * b$ or $b * a$ as then $b = a$. Hence either $a^2 = e$ or $a^2 = b$. Now consider $a * b * a$. It can't equal $a$ as then $b * a = e$ and hence $a * b = b * a$. Similarly it can't equal $b$. It also can't equal $a * b$ or $b * a$ as then $a = e$. Hence $a * b * a = e$.

So then we additionally see that $a^2 \neq e$ because then $a^2 = e = a * b * a$ and consequently $a = b * a$ (and hence $b = e$ ). So $a^2 = b$. But then $a * b = a * a^2 = a^2 * a = b * a$. Contradiction. Hence starting with the assumption that there exists an order 5 abelian group $G$ leads to a contradiction. Thus there is no such group. □

**Exercise 2.1.26** If $G$ is a finite group, prove that, given $a \in G$, there is a positive integer $n$, depending on $a$, such that $a^n = e$.

*Proof.* Because there are only a finite number of elements of $G$, it's clear that the set $\{a, a^2, a^3, \dots\}$ must be a finite set and in particular, there should exist some $i$ and $j$ such that $i \neq j$ and $a^i = a^j$. WLOG suppose further that $i > j$ (just reverse the roles of $i$ and $j$ otherwise). Then multiply both sides by $\left(a^j\right)^{-1} = a^{-j}$ to get

$$a^i * a^{-j} = a^{i-j} = e$$

Thus the $n = i - j$ is a positive integer such that $a^n = e$. □

**Exercise 2.1.27** If $G$ is a finite group, prove that there is an integer $m > 0$ such that $a^m = e$ for all $a \in G$.

*Proof.* Let $n_1, n_2, \dots, n_k$ be the orders of all $k$ elements of $G = \{a_1, a_2, \dots, a_k\}$. Let $m = \operatorname{lcm}(n_1, n_2, \dots, n_k)$. Then, for any $i = 1, \dots, k$, there exists an integer $c$ such that $m = n_i c$. Thus

$$a_i^m = a_i^{n_i c} = (a_i^{n_i})^c = e^c = e$$

Hence $m$ is a positive integer such that $a^m = e$ for all $a \in G$. □

**Exercise 2.2.3** If $G$ is a group in which $(ab)^i = a^i b^i$ for three consecutive integers $i$, prove that $G$ is abelian.

*Proof.* Let $G$ be a group, $a, b \in G$ and $i$ be any integer. Then from given condition,

$$\begin{aligned} (ab)^i &= a^i b^i \\ (ab)^{i+1} &= a^{i+1} b^{i+1} \\ (ab)^{i+2} &= a^{i+2} b^{i+2} \end{aligned}$$

From first and second, we get

$$a^{i+1} b^{i+1} = (ab)^i (ab) = a^i b^i ab \Longrightarrow b^i a = a b^i$$

From first and third, we get

$$a^{i+2} b^{i+2} = (ab)^i (ab)^2 = a^i b^i abab \Longrightarrow a^2 b^{i+1} = b^i aba$$

This gives

$$a^2 b^{i+1} = a\left(ab^i\right) b = ab^i ab = b^i a^2 b$$

Finally, we get

$$b^i aba = b^i a^2 b \Longrightarrow ba = ab$$

This shows that $G$ is Abelian. □

**Exercise 2.2.5** Let $G$ be a group in which $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$. Show that $G$ is abelian.

*Proof.* We have

$$\begin{aligned}
&(ab)^3 = a^3b^3, \text{ for all } a, b \in G \\
\Longrightarrow &(ab)(ab)(ab) = a\left(a^2b^2\right)b \\
\Longrightarrow &a(ba)(ba)b = a\left(a^2b^2\right)b \\
\Longrightarrow &(ba)^2 = a^2b^2, \text{ by cancellation law.}
\end{aligned}$$

Again,

$$\begin{aligned}
&(ab)^5 = a^5b^5, \text{ for all } a, b \in G \\
\Longrightarrow &(ab)(ab)(ab)(ab)(ab) = a\left(a^4b^4\right)b \\
\Longrightarrow &a(ba)(ba)(ba)(ba)b = a\left(a^4b^4\right)b \\
\Longrightarrow &(ba)^4 = a^4b^4, \text{ by cancellation law.}
\end{aligned}$$

Now by combining two cases we have

$$\begin{aligned}
&(ba)^4 = a^4b^4 \\
\Longrightarrow &\left((ba)^2\right)^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &\left(a^2b^2\right)^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &\left(a^2b^2\right)\left(a^2b^2\right) = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &a^2\left(b^2a^2\right)b^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &b^2a^2 = a^2b^2, \text{ by cancellation law.} \\
\Longrightarrow &b^2a^2 = (ba)^2, \text{ since } (ba)^2 = a^2b^2 \\
\Longrightarrow &b(ba)a = (ba)(ba) \\
\Longrightarrow &b(ba)a = b(ab)a \\
\Longrightarrow &ba = ab, \text{ by cancellation law.}
\end{aligned}$$

It follows that, $ab = ba$ for all $a, b \in G$. Hence $G$ is abelian □

**Exercise 2.2.6c** Let $G$ be a group in which $(ab)^n = a^nb^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that $\left(aba^{-1}b^{-1}\right)^{n(n-1)} = e$.

*Proof.* We start with the following two intermediate results. (1) $(ab)^{n-1} = b^{n-1}a^{n-1}$. (2) $a^nb^{n-1} = b^{n-1}a^n$. To prove (1), notice by the given condition for all $a, b \in G$ $(ba)^n = b^na^n$, for some fixed integers $n > 1$. Then, $(ba)^n = b^na^n \Longrightarrow b.(ab)(ab)\ldots.(ab).a = b\left(b^{n-1}a^{n-1}\right)a$, where $(ab)$ occurs $n-1$ times $\Longrightarrow (ab)^{n-1} = b^{n-1}a^{n-1}$, by cancellation law. Hence, for all $a, b \in G$

$$(ab)^{n-1} = b^{n-1}a^{n-1}.$$

To prove (2), notice by the given condition for all $a, b \in G$ $(ba)^n = b^n a^n$, for some fixed integers $n > 1$. Then we have

$$\begin{aligned}
&(ba)^n = b^n a^n \\
\Longrightarrow & b \cdot (ab)(ab) \ldots (ab) \cdot a = b\left(b^{n-1}a^{n-1}\right)a, \text{ where } (ab) \text{ occurs } n-1 \text{ times} \\
\Longrightarrow & (ab)^{n-1} = b^{n-1}a^{n-1}, \text{ by cancellation law} \\
\Longrightarrow & (ab)^{n-1}(ab) = \left(b^{n-1}a^{n-1}\right)(ab) \\
\Longrightarrow & (ab)^n = b^{n-1}a^n b \\
\Longrightarrow & a^n b^n = b^{n-1}a^n b, \text{ given condition} \\
\Longrightarrow & a^n b^{n-1} = b^{n-1}a^n, \text{ by cancellation law.}
\end{aligned}$$

Therefore for all $a, b \in G$ we have

$$a^n b^{n-1} = b^{n-1} a^n$$

In order to show that

$$\left(aba^{-1}b^{-1}\right)^{n(n-1)} = e, \text{ for all } a, b \in G$$

it is enough to show that

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \quad \forall x, y \in G.$$

Step 3 This is because of

$$\begin{aligned}
(ab)^{n(n-1)} = (ba)^{n(n-1)} &\Longrightarrow (ba)^{-1}\big)^{n(n-1)} (ab)^{n(n-1)} = e \\
&\Longrightarrow \left(a^{-1}b^{-1}\right)^{n(n-1)} (ab)^{n(n-1)} = e \\
&\Longrightarrow \left(\left(a^{-1}b^{-1}\right)^n\right)^{n-1} \left((ab)^n\right)(n-1) = e \\
&\Longrightarrow \left((ab)^n \left(a^{-1}b^{-1}\right)^n\right)^{n-1} = e, \text{ by (1)} \\
&\Longrightarrow \left(aba^{-1}b^{-1}\right)^{n(n-1)} = e, \text{ ( given condition)}
\end{aligned}$$

Now, it suffices to show that

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \quad \forall x, y \in G.$$

Now, we have

$$\begin{aligned}
(ab)^{n(n-1)} &= (a^n b^n)^{n-1}, \text{ by the given condition} \\
&= \left(a^n b^{n-1} b\right)^{n-1} \\
&= \left(b^{n-1} a^n b\right)^{n-1}, \text{ by (2)} \\
&= (a^n b)^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (1)} \\
&= b^{n-1} (a^n)^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (1)} \\
&= \left(b^{n-1} \left(a^{n-1}\right)^n\right) \left(b^{n-1}\right)^{n-1} \\
&= \left(a^{n-1}\right)^n b^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (2)} \\
&= \left(a^{n-1}\right)^n \left(b^{n-1}\right)^n \\
&= \left(a^{n-1} b^{n-1}\right)^n, \text{ by (1)} \\
&= (ba)^{n(n-1)}, \text{ by (1).}
\end{aligned}$$

This completes our proof. □

**Exercise 2.3.17** If $G$ is a group and $a, x \in G$, prove that $C\left(x^{-1}ax\right) = x^{-1}C(a)x$

*Proof.* Note that

$$C(a) := \{x \in G \mid xa = ax\}.$$

Let us assume $p \in C\left(x^{-1}ax\right)$. Then,

$$\begin{aligned}
& p\left(x^{-1}ax\right) = \left(x^{-1}ax\right)p \\
\Longrightarrow & \left(px^{-1}a\right)x = x^{-1}(axp) \\
\Longrightarrow & x\left(px^{-1}a\right) = (axp)x^{-1} \\
\Longrightarrow & \left(xpx^{-1}\right)a = a\left(xpx^{-1}\right) \\
\Longrightarrow & xpx^{-1} \in C(a).
\end{aligned}$$

Therefore,

$$p \in C\left(x^{-1}ax\right) \Longrightarrow xpx^{-1} \in C(a).$$

Thus,

$$C\left(x^{-1}ax\right) \subset x^{-1}C(a)x.$$

Let us assume

$$q \in x^{-1}C(a)x.$$

Then there exists an element $y$ in $C(a)$ such that

$$q = x^{-1}yx$$

Now,

$$y \in C(a) \Longrightarrow ya = ay.$$

Also,

$$q\left(x^{-1} a x\right)=\left(x^{-1} y x\right)\left(x^{-1} a x\right)=x^{-1}(y a) x=x^{-1}(y a) x=\left(x^{-1} y x\right)\left(x^{-1} a x\right)=\left(x^{-1} y x\right) q .$$

Therefore,

$$q\left(x^{-1} a x\right)=\left(x^{-1} y x\right) q$$

So,

$$q \in C\left(x^{-1} a x\right) .$$

Consequently we have

$$x^{-1} C(a) x \subset C\left(x^{-1} a x\right) .$$

It follows from the aforesaid argument

$$C\left(x^{-1} a x\right)=x^{-1} C(a) x .$$

This completes the proof. □

**Exercise 2.3.19** If $M$ is a subgroup of $G$ such that $x^{-1} M x \subset M$ for all $x \in G$, prove that actually $x^{-1} M x=M$.

**Exercise 2.3.16** If a group $G$ has no proper subgroups, prove that $G$ is cyclic of order $p$, where $p$ is a prime number.

*Proof.* Case-1: $G=(e), e$ being the identity element in $G$. Then trivially $G$ is cyclic. Case-2: $G \neq(e)$. Then there exists an non-identity element in $G$. Let us consider an non-identity element in $G$, say $a \neq(e)$. Now look at the cyclic subgroup generated by $a$, that is, $\langle a\rangle$. Since $a \neq(e) \in G,\langle a\rangle$ is a subgroup of $G$. If $G \neq\langle a\rangle$ then $\langle a\rangle$ is a proper non-trivial subgroup of $G$, which is an impossibility. Therfore we must have

$$G=\langle a\rangle .$$

This implies, $G$ is a cyclic group generated by $a$. Then it follows that every non-identity element of $G$ is a generator of $G$. Now we claim that $G$ is finite. □

**Exercise 2.3.21** If $A, B$ are subgroups of $G$ such that $b^{-1} A b \subset A$ for all $b \in B$, show that $A B$ is a subgroup of $G$.

*Proof.* Proof: Let us consider any two elements $p$ and $q$ in $A B$. Then there exist elements $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that

$$p=a_1 b_1 \text { and } q=a_2 b_2 .$$

Now,

$$\begin{aligned}
p q^{-1} & =\left(a_1 b_1\right)\left(a_2 b_2\right)^{-1} \\
& =\left(a_1 b_1\right)\left(b_2^{-1} a_2^{-1}\right) \\
& =a_1\left(b_1 b_2^{-1} a_2^{-1} b_2 b_1^{-1}\right) b_1 b_2^{-1} .
\end{aligned}$$

Since $b^{-1}Ab \subset A$, for all $b \in B$, we have

$$b_1 {b_2}^{-1} {a_2}^{-1} b_2 b_1^{-1} \in A.$$

$\square$

**Exercise 2.3.22** If $A$ and $B$ are finite subgroups, of orders $m$ and $n$, respectively, of the abelian group $G$, prove that $AB$ is a subgroup of order $mn$ if $m$ and $n$ are relatively prime.

*Proof.* Proof: Firstly we show that $AB$ forms a subgroup of the abelian group $G$. Let us consider $p \in AB, q \in AB$ and $p = a_1 b_1, q = a_2 b_2$, for some $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then,

$$\begin{aligned} pq &= (a_1 b_1)(a_2 b_2) \\ &= a_1 (b_1 a_2) b_2 \\ &= a_1 (a_2 b_1) b_2, \text{ since } G \text{ is abelian} \\ &= (a_1 a_2)(b_1 b_2) \in AB. \end{aligned}$$

Therefore,

$$p, q \in AB \Longrightarrow pq \in AB.$$

Also,

$$p^{-1} = (a_1 b_1)^{-1} = (b_1)^{-1} (a_1)^{-1} = (a_1)^{-1} (b_1)^{-1} \in AB.$$

So $AB$ is a subgroup of $G$. $\square$

**Exercise 2.3.28** Let $M, N$ be subgroups of $G$ such that $x^{-1}Mx \subset M$ and $x^{-1}Nx \subset N$ for all $x \in G$. Prove that $MN$ is a subgroup of $G$ and that $x^{-1}(MN)x \subset MN$ for all $x \in G$.

*Proof.* Proof: First we assert that $MN$ is a subgroup of $G$. Let us consider two elements

$$x, y \in MN.$$

Then, there exists $m_1, m_2 \in M$ and $n_1, n_2 \in N$ such that

$$x = m_1 n_1 \text{ and } y = m_2 n_2.$$

Now we need to show that $xy^{-1} \in MN$. Now,

$$\begin{aligned} xy^{-1} &= m_1 n_1 (m_2 n_2)^{-1} \\ &= m_1 n_1 n_2^{-1} m_2^{-1} \\ &= m_1 m_2^{-1} \left( m_2 n_1 n_2^{-1} m_2^{-1} \right). \end{aligned}$$

Since, $n_1, n_2 \in N$, then $n_1 n_2^{-1} \in N$ and this implies $m_2 n_1 n_2^{-1} m_2^{-1} \in N$. Consequently,

$$xy^{-1} = m_1 m_2^{-1} \left( m_2 n_1 n_2^{-1} m_2^{-1} \right) \in MN.$$

Thus,

$$x, y \in MN \Longrightarrow xy \in MN.$$

Hence, $MN$ is a subgroup of $G$. $\square$

**Exercise 2.3.29** If $M$ is a subgroup of $G$ such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.

*Proof.* Proof: To prove $x^{-1}Mx = M$, it suffices to show that

$$M \subset x^{-1}Mx$$

Let us consider an element $m$ in $M$. Then,

$$m = x^{-1}\left(xmx^{-1}\right)x, \text{ for any } x \in G.$$

Since $G$ is a group,

$$x \in G \Longrightarrow x^{-1} \in G.$$

So,

$$xmx^{-1} = \left(x^{-1}\right)^{-1}mx^{-1} \in x^{-1}Mx(\subset M) \Longrightarrow xmx^{-1} \in M$$

It follows that

$$m = x^{-1}\left(xmx^{-1}\right)x \in x^{-1}Mx.$$

Thus,

$$m \in M \Longrightarrow m \in x^{-1}Mx.$$

Consequently,

$$M \subset x^{-1}Mx$$

Thence,

$$M = x^{-1}Mx$$

This completes the proof. □

**Exercise 2.4.8** If every right coset of $H$ in $G$ is a left coset of $H$ in $G$, prove that $aHa^{-1} = H$ for all $a \in G$.

*Proof.* Proof: We have

$$Ha = bH, \text{ for } a, b \in G.$$

Then there exist $h_1, h_2 \in H$ such that

$$h_1a = bh_2.$$

Hence,

$$\begin{aligned} h_1a = bh_2 &\Longrightarrow b = h_1ah_2^{-1} \\ &\Longrightarrow bH = h_1ah_2^{-1}H \\ &\Longrightarrow Ha = h_1ah_2^{-1}H \\ &\Longrightarrow Ha = h_1aH \\ &\Longrightarrow h_1^{-1}Ha = aH \\ &\Longrightarrow Ha = aH \end{aligned}$$

Therefore,

$$\begin{aligned} &Ha = aH, \text{ for all } a \in G \\ \Longrightarrow &H = aHa^{-1}. \end{aligned}$$

This completes the proof. □

**Exercise 2.4.26** Let $G$ be a group, $H$ a subgroup of $G$, and let $S$ be the set of all distinct right cosets of $H$ in $G$, $T$ the set of all left cosets of $H$ in $G$. Prove that there is a 1-1 mapping of $S$ onto $T$.

*Proof.* It suffices to show that there is a bijection betwwen the set of all distinct left cosets of $H$ in $G$ and the set of all distinct right cosets of $H$ in $G$ Let us consider an element $a$ in $G$. Let us define a mapping

$$f : S \to T$$

by the assignment

$$f(Ha) = a^{-1}H, Ha \in S.$$

First we show that the mapping $f$ is well defined in the sense that if

$$Hx = Ha \text{ then } x^{-1}H = a^{-1}H.$$

Now

$$\begin{aligned} Hx = Ha &\Longrightarrow x \in Ha \\ &\Longrightarrow xa^{-1} \in H \\ &\Longrightarrow \left(x^{-1}\right)^{-1} a^{-1} \in H \\ &\Longrightarrow a^{-1} \in x^{-1}H \\ &\Longrightarrow a^{-1}H = x^{-1}H. \end{aligned}$$

Therefore $f$ assigns a unique coset in $T$ to a unique coset in $S$. We now prove that $f$ is one-one. Let $Ha, Hb \in S$ and $Ha \neq Hb$. Then,

$$\begin{aligned} f(Ha) = f(Hb) &\Longrightarrow a^{-1}H = b^{-1}H \\ &\Longrightarrow a^{-1} \in b^{-1}H \\ &\Longrightarrow \left(b^{-1}\right)^{-1} a^{-1} \in H \\ &\Longrightarrow ba^{-1} \in H \\ &\Longrightarrow b \in Ha \Longrightarrow Hb = Ha. \end{aligned}$$

So,

$$Ha \neq Hb \Longrightarrow f(Ha) \neq f(Hb).$$

This proves that $f$ is one-one. In order to prove the $f$ is onto, let us take an element $aH$ in $T$. The pre-image of $aH$ is $Ha^{-1}$ in $S$, since

$$f\left(Ha^{-1}\right) = \left(a^{-1}\right)^{-1} H = aH.$$

Therefore, $f$ is onto. Consequently, $f$ is a bijection from $S$ to $T$. Hence we get an one-one mapping $S$ onto $T$. This completes the proof. $\square$

**Exercise 2.4.32** Let $G$ be a finite group, $H$ a subgroup of $G$. Let $f(a)$ be the least positive $m$ such that $a^m \in H$. Prove that $f(a) \mid o(a)$, where $o(a)$ is an order of $a$.

*Proof.* Let us assume that

$$o(a) = n.$$

Then by Division Algorithm, there exist $q$ and $r$ such that

$$n = qf(a) + r, \text{ where } 0 \leq r < f(a).$$

Since $o(a) = n$, we have

$$\begin{aligned} a^n = &\Longrightarrow (a)^{qf(a)} \cdot a^r = e \\ &\Longrightarrow \left(a^{f(a)}\right)^q \cdot a^r = e \end{aligned}$$

Now,

$$a^{f(a)} \in H \Longrightarrow \left(a^{f(a)}\right)^q \in H \Longrightarrow a^r \in H, \text{ as } e \in H.$$

The minimality of $f(a)$ that $a^{f(a)} \in H$, forced $r = 0$. It follows that

$$n = qf(a).$$

Therefore,

$$f(a) \mid o(a)$$

This completes the proof. □

**Exercise 2.4.36** If $a > 1$ is an integer, show that $n \mid \varphi(a^n - 1)$, where $\phi$ is the Euler $\varphi$-function.

*Proof.* Proof: We have $a > 1$. First we propose to prove that

$$\operatorname{Gcd}(a, a^n - 1) = 1.$$

If possible, let us assume that $\operatorname{Gcd}(a, a^n - 1) = d$, where $d > 1$. Then $d$ divides $a$ as well as $a^n - 1$. Now, $d$ divides $a \Longrightarrow d$ divides $a^n$. This is an impossibility, since $d$ divides $a^n - 1$ by our assumption. Consequently, $d$ divides 1 , which implies $d = 1$. Hence we are contradict to the fact that $d > 1$. Therefore

$$\operatorname{Gcd}(a, a^n - 1) = 1.$$

Then $a \in U_{a^n-1}$, where $U_n$ is a group defined by

$$U_n := \{\bar{a} \in \mathbb{Z}_n \mid \operatorname{Gcd}(a, n) = 1\}.$$

We know that order of an element divides the order of the group. Here order of the group $U_{a^n-1}$ is $\phi(a^n - 1)$ and $a \in U_{a^n-1}$. This follows that o$(a)$ divides $\phi(a^n - 1)$. □

**Exercise 2.5.23** Let $G$ be a group such that all subgroups of $G$ are normal in $G$. If $a, b \in G$, prove that $ba = a^j b$ for some $j$.

*Proof.* Let $G$ be a group where each subgroup is normal in $G$. let $a, b \in G$.

$$\langle a \rangle \triangleright G \Rightarrow b \cdot \langle a \rangle = \langle a \rangle \cdot b.$$
$$\Rightarrow \quad b \cdot a = a^j \cdot b \text{ for some } j \in \mathbb{Z}.$$

(hence for $a_1 b \in G \quad a^j b = b \cdot a$ ). $\square$

**Exercise 2.5.30** Suppose that $|G| = pm$, where $p \nmid m$ and $p$ is a prime. If $H$ is a normal subgroup of order $p$ in $G$, prove that $H$ is characteristic.

*Proof.* Let $G$ be a group of order $pm$, such that $p \nmid m$. Now, Given that $H$ is a normal subgroup of order $p$. Now we want to prove that $H$ is a characterestic subgroup, that is $\phi(H) = H$ for any automorphism $\phi$ of $G$. Now consider $\phi(H)$. Clearly $|\phi(H)| = p$. Suppose $\phi(H) \neq H$, then $H \cap \phi(H) = \{e\}$. Consider $H\phi(H)$, this is a subgroup of $G$ as $H$ is normal. Also $|H\phi(H)| = p^2$. By lagrange's theorem then $p^2 \mid pm \Longrightarrow p \mid m$ - contradiction. So $\phi(H) = H$, and $H$ is characterestic subgroup of $G$ $\square$

**Exercise 2.5.31** Suppose that $G$ is an abelian group of order $p^n m$ where $p \nmid m$ is a prime. If $H$ is a subgroup of $G$ of order $p^n$, prove that $H$ is a characteristic subgroup of $G$.

*Proof.* Let $G$ be an abelian group of order $p^n m$, such that $p \nmid m$. Now, Given that $H$ is a subgroup of order $p^n$. Since $G$ is abelian $H$ is normal. Now we want to prove that $H$ is a characterestic subgroup, that is $\phi(H) = H$ for any automorphism $\phi$ of $G$. Now consider $\phi(H)$. Clearly $|\phi(H)| = p^n$. Suppose $\phi(H) \neq H$, then $|H \cap \phi(H)| = p^s$, where $s < n$. Consider $H\phi(H)$, this is a subgroup of $G$ as $H$ is normal. Also $|H\phi(H)| = \frac{|H||\phi(H)|}{|H \cap \phi(H)|} = \frac{p^{2n}}{p^s} = p^{2n-s}$, where $2n - s > n$. By lagrange's theorem then $p^{2n-s} | p^n m \Longrightarrow p^{n-s} | m \Longrightarrow p \mid m$-contradiction. So $\phi(H) = H$, and $H$ is characterestic subgroup of $G$. $\square$

**Exercise 2.5.37** If $G$ is a nonabelian group of order 6, prove that $G \simeq S_3$.

*Proof.* Suppose $G$ is a non-abelian group of order 6 . We need to prove that $G \cong S_3$. Since $G$ is non-abelian, we conclude that there is no element of order 6. Now all the nonidentity element has order either 2 or 3 . All elements cannot be order 3 .This is because except the identity elements there are 5 elements, but order 3 elements occur in pair, that is $a, a^2$, both have order 3 , and $a \neq a^2$. So, this is a contradiction, as there are only 5 elements. So, there must be an element of order 2 . All elements of order 2 will imply that $G$ is abelian, hence there is also element of order 3 . Let $a$ be an element of order 2 , and $b$ be an element of order 3 . So we have $e, a, b, b^2$, already 4 elements. Now $ab \neq e, b, b^2$. So $ab$ is another element distinct from the ones already constructed.

$ab^2 \neq e, b, ab, b^2, a$. So, we have got another element distinct from the other. So, now $G = \left\{e, a, b, b^2, ab, ab^2\right\}$. Also, ba must be equal to one of these elements. But $ba \neq e, a, b, b^2$. Also if $ba = ab$, the group will become abelian. so $ba = ab^2$. So what we finally get is $G = \left\langle a, b \mid a^2 = e = b^3, ba = ab^2\right\rangle$. Hence $G \cong S_3$. $\square$

**Exercise 2.5.43** Prove that a group of order 9 must be abelian.

*Proof.* We use the result from problem 40 which is as follows: Suppose $G$ is a group, $H$ is a subgroup and $|G| = n$ and $n \nmid (i_G(H))!$. Then there exists a normal subgroup $K\ neq { e }$ and $K \subseteq H$. So, we have now a group $G$ of order 9. Suppose that $G$ is cyclic, then $G$ is abelian and there is nothing more to prove. Suppose that $G$ s not cyclic,then there exists an element $a$ of order 3 , and $A = \langle a\rangle$. Now $i_G(A) = 3$, now $9 \nmid 3$ !, hence by the above result there is a normal subgroup $K$, non-trivial and $K \subseteq A$. But $|A| = 3$, a prime order subgroup, hence has no non-trivial subgroup, so $K = A$. So $A$ is normal subgroup. Now since $G$ is not cyclic any non-identity element is of order 3.So Let $a(\neq e) \in G$.Consider $A = \langle a\rangle$. As shown before $A$ is normal. $a$ commutes with any if its powers. Now Let $b \in G$ such that $b \notin A$. Then $bab^{-1} \in A$ and hence $bab^{-1} = a^i$.This implies $a = b^3ab^{-3} = a^{i^3} \implies a^{i^3-1} = e$. So, 3 divides $i^3 - 1$. Also by fermat's little theorem 3 divides $i^2 - 1$.So 3 divides $i - 1$. But $0 \leq i \leq 2$. So $i = 1$, is the only possibility and hence $ab = ba$. So $a \in Z(G)$ as $b$ was arbitrary. Since $a$ was arbitrary $G = Z(G)$. Hence $G$ is abelian. $\square$

**Exercise 2.5.44** Prove that a group of order $p^2$, $p$ a prime, has a normal subgroup of order $p$.

**Exercise 2.5.52** Let $G$ be a finite group and $\varphi$ an automorphism of $G$ such that $\varphi(x) = x^{-1}$ for more than three-fourths of the elements of $G$. Prove that $\varphi(y) = y^{-1}$ for all $y \in G$, and so $G$ is abelian.

**Exercise 2.6.15** If $G$ is an abelian group and if $G$ has an element of order $m$ and one of order $n$, where $m$ and $n$ are relatively prime, prove that $G$ has an element of order $mn$.

**Exercise 2.7.3** Let $G$ be the group of nonzero real numbers under multiplication and let $N = \{1, -1\}$. Prove that $G/N \simeq$ positive real numbers under multiplication.

**Exercise 2.7.7** If $\varphi$ is a homomorphism of $G$ onto $G'$ and $N \triangleleft G$, show that $\varphi(N) \triangleleft G'$.

**Exercise 2.8.7** If $G$ is a group with subgroups $A, B$ of orders $m, n$, respectively, where $m$ and $n$ are relatively prime, prove that the subset of $G$, $AB = \{ab \mid a \in A, b \in B\}$, has $mn$ distinct elements.

**Exercise 2.8.12** Prove that any two nonabelian groups of order 21 are isomorphic.

**Exercise 2.8.15** Prove that if $p > q$ are two primes such that $q \mid p - 1$, then any two nonabelian groups of order $pq$ are isomorphic.

**Exercise 2.9.2** If $G_1$ and $G_2$ are cyclic groups of orders $m$ and $n$, respectively, prove that $G_1 \times G_2$ is cyclic if and only if $m$ and $n$ are relatively prime.

**Exercise 2.10.1** Let $A$ be a normal subgroup of a group $G$, and suppose that $b \in G$ is an element of prime order $p$, and that $b \notin A$. Show that $A \cap (b) = (e)$.

**Exercise 2.11.6** If $P$ is a $p$-Sylow subgroup of $G$ and $P \triangleleft G$, prove that $P$ is the only $p$-Sylow subgroup of $G$.

**Exercise 2.11.7** If $P \triangleleft G$, $P$ a $p$-Sylow subgroup of $G$, prove that $\varphi(P) = P$ for every automorphism $\varphi$ of $G$.

**Exercise 2.11.22** Show that any subgroup of order $p^{n-1}$ in a group $G$ of order $p^n$ is normal in $G$.

**Exercise 3.2.21** If $\sigma, \tau$ are two permutations that disturb no common element and $\sigma\tau = e$, prove that $\sigma = \tau = e$.

**Exercise 3.2.23** Let $\sigma, \tau$ be two permutations such that they both have decompositions into disjoint cycles of cycles of lengths $m_1, m_2, \ldots, m_k$. Prove that for some permutation $\beta, \tau = \beta\sigma\beta^{-1}$.

**Exercise 3.3.2** If $\sigma$ is a $k$-cycle, show that $\sigma$ is an odd permutation if $k$ is even, and is an even permutation if $k$ is odd.

**Exercise 3.3.9** If $n \geq 5$ and $(e) \neq N \subset A_n$ is a normal subgroup of $A_n$, show that $N$ must contain a 3-cycle.

**Exercise 4.1.19** Show that there is an infinite number of solutions to $x^2 = -1$ in the quaternions.

**Exercise 4.1.34** Let $T$ be the group of $2 \times 2$ matrices $A$ with entries in the field $\mathbb{Z}_2$ such that $\det A$ is not equal to 0. Prove that $T$ is isomorphic to $S_3$, the symmetric group of degree 3.

**Exercise 4.2.5** Let $R$ be a ring in which $x^3 = x$ for every $x \in R$. Prove that $R$ is commutative.

**Exercise 4.2.6** If $a^2 = 0$ in $R$, show that $ax + xa$ commutes with $a$.

**Exercise 4.2.9** Let $p$ be an odd prime and let $1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b}$, where $a, b$ are integers. Show that $p \mid a$.

**Exercise 4.3.1** If $R$ is a commutative ring and $a \in R$, let $L(a) = \{x \in R \mid xa = 0\}$. Prove that $L(a)$ is an ideal of $R$.

**Exercise 4.3.25** Let $R$ be the ring of $2 \times 2$ matrices over the real numbers; suppose that $I$ is an ideal of $R$. Show that $I = (0)$ or $I = R$.

**Exercise 4.4.9** Show that $(p-1)/2$ of the numbers $1, 2, \ldots, p-1$ are quadratic residues and $(p-1)/2$ are quadratic nonresidues $\mod p$.

**Exercise 4.5.12** If $F \subset K$ are two fields and $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$, show that they are relatively prime in $K[x]$.

**Exercise 4.5.16** Let $F = \mathbb{Z}_p$ be the field of integers $\mod p$, where $p$ is a prime, and let $q(x) \in F[x]$ be irreducible of degree $n$. Show that $F[x]/(q(x))$ is a field having at exactly $p^n$ elements.

**Exercise 4.5.23** Let $F = \mathbb{Z}_7$ and let $p(x) = x^3 - 2$ and $q(x) = x^3 + 2$ be in $F[x]$. Show that $p(x)$ and $q(x)$ are irreducible in $F[x]$ and that the fields $F[x]/(p(x))$ and $F[x]/(q(x))$ are isomorphic.

**Exercise 4.5.25** If $p$ is a prime, show that $q(x) = 1 + x + x^2 + \cdots x^{p-1}$ is irreducible in $Q[x]$.

**Exercise 4.6.2** Prove that $f(x) = x^3 + 3x + 2$ is irreducible in $Q[x]$.

**Exercise 4.6.3** Show that there is an infinite number of integers a such that $f(x) = x^7 + 15x^2 - 30x + a$ is irreducible in $Q[x]$.

**Exercise 5.1.8** If $F$ is a field of characteristic $p \neq 0$, show that $(a + b)^m = a^m + b^m$, where $m = p^n$, for all $a, b \in F$ and any positive integer $n$.

**Exercise 5.2.20** Let $V$ be a vector space over an infinite field $F$. Show that $V$ cannot be the set-theoretic union of a finite number of proper subspaces of $V$.

**Exercise 5.3.7** If $a \in K$ is such that $a^2$ is algebraic over the subfield $F$ of $K$, show that a is algebraic over $F$.

**Exercise 5.3.10** Prove that $\cos 1^\circ$ is algebraic over $\mathbb{Q}$.

**Exercise 5.4.3** If $a \in C$ is such that $p(a) = 0$, where $p(x) = x^5 + \sqrt{2}x^3 + \sqrt{5}x^2 + \sqrt{7}x + \sqrt{11}$, show that $a$ is algebraic over $\mathbb{Q}$ of degree at most 80.

**Exercise 5.5.2** Prove that $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

**Exercise 5.6.3** Let $\mathbb{Q}$ be the rational field and let $p(x) = x^4 + x^3 + x^2 + x + 1$. Show that there is an extension $K$ of $Q$ with $[K : Q] = 4$ over which $p(x)$ splits into linear factors.

**Exercise 5.6.14** If $F$ is of characteristic $p \neq 0$, show that all the roots of $x^m - x$, where $m = p^n$, are distinct.