Solution of Some Homework Problems

Section 2.2 Permutations

(2.1) Find $\text{sgn}(\alpha)$ and $\alpha^{-1}$, where

\[
\alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{pmatrix}.
\]

Solution: Since $\alpha = (19)(28)(37)(46)(5)$, $\text{sgn}(\alpha) = (-1)^{9-5} = -1$ and that $\alpha^{-1} = (5)(46)(37)(28)(19)$.

(2.2) If $\alpha \in S_n$, prove that $\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha)$.

Proof: Since $\alpha \alpha^{-1} = e$, we have $\text{sign}(\alpha \alpha^{-1}) = \text{sign}(e)$. That is $\text{sign}(\alpha) \text{sign}(\alpha^{-1}) = 1$ and so $\text{sign}(\alpha) = \text{sign}(\alpha^{-1}) = 1$ or $-1$.

(2.8) Define $f : \{0, 1, 2, \cdots, 10\} \mapsto \{0, 1, 2, \cdots, 10\}$ by

\[f(n) = \text{the remainder after dividing} 4n^2 - 3n^7 \text{ by } 11.\]

(i) Show that $f$ is a permutation.

(ii) Compute the parity of $f$.

(iii) Compute the inverse of $f$.

Proof: (i) Easy to get $f(0) = 0$, $f(1) = 1$ and $f(10) \equiv f(-1) \equiv 4 + 3 \equiv 7 \pmod{11}$. We perform the following computation in $\mathbb{Z}_{11}$.

\[
\begin{align*}
f(2) & = 4(2^2) - 3(2^7) = 16(1 - 3 \cdot 8) \equiv 5(-1) \equiv 6 \pmod{11} \\
f(9) & \equiv f(-2) \equiv 16(1 + 24) \equiv 5 \cdot 3 \equiv 15 \equiv 4 \pmod{11} \\
f(3) & = 4(3^2) - 3^8 = 9(4 - 3^6) \equiv 9(4 - (-2)^3) \equiv 9(12) \equiv 9 \pmod{11} \\
f(8) & \equiv f(-3) \equiv (-3)^2(4 + (-3)^6) \equiv 9(4 + (-2)^3) \equiv (-2)(-4) \equiv 8 \pmod{11} \\
f(4) & = 4(4^2) - 3(4^7) = 4^3(1 - 3(4^4)) \equiv 9(1 - 3 \cdot 25) \equiv 9(1 - 3(3)) \equiv 9(-8) \equiv 5 \pmod{11} \\
f(7) & \equiv f(-4) \equiv 4^3 + 3(4^7) = 4^3(1 + 3(4^4)) \equiv 9(1 + 3 \cdot 25) \equiv 9(1 + 9) \equiv 2 \pmod{11} \\
f(5) & = 4(5^2) - 3(5^7) = 5^2(4 - 15(5^4)) \equiv 3(4 - 4 \cdot 9) \equiv 12(1 - 9) \equiv -8 \equiv 3 \pmod{11} \\
f(6) & \equiv f(-5) \equiv 4(5^2) + 3(5^7) = 5^2(4 + 15(5^4)) \equiv 3(4 + 4 \cdot 9) \equiv 12(1 + 9) \equiv 10 \pmod{11}
\end{align*}
\]

Thus $f = (26107)(3945)(0)(1)(8) = (26107)(3945)$.

(ii) $\text{sgn}(f) = (-1)^{11-5} = 1$, and so $f$ is an even permutation.
(iii) $f^{-1} = (3\ 9\ 4\ 5)^{-1}(2\ 6\ 10\ 7)^{-1} = (3\ 5\ 4\ 9)(2\ 7\ 10\ 6)$.

(2.10) (i) Prove that if $\alpha$ and $\beta$ are (not necessary disjoint) permutations that commute, then $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 1$.

(ii) Give an example of two permutations and for which $(\alpha\beta)^2 \neq \alpha^2\beta^2$.

**Proof:** (i) First we prove, by induction, the statement $L(k)$ that for any $k \geq 1$, $\alpha\beta^k = \beta^k\alpha$.

Since $\alpha\beta = \beta\alpha$, $L(1)$ holds.

Suppose that when $k = n \geq 1$, we have $\alpha\beta^n = \beta^n\alpha$.

We consider the case $k = n + 1$, $\alpha\beta^{(n+1)} = \alpha(\beta\beta^n) = (\alpha\beta)\beta^n = (\beta\alpha)\beta^n = \beta(\beta^n\alpha) = (\beta^n)\alpha = \beta^{(n+1)}\alpha$. Thus by induction $L(k)$ holds for all integers $k \geq 1$.

Now we use induction to prove the statement $S(k)$ that $(\alpha\beta)^k = \alpha^k\beta^k$, for any integer $k \geq 1$.

Since $S(1) = L(1)$, $S(1)$ holds.

Suppose that when $k = n \geq 1$, we have $(\alpha\beta)^n = \alpha^n\beta^n$.

We consider the case $k = n + 1$, $(\alpha\beta)^{(n+1)} = (\alpha\beta)^n(\alpha\beta) = (\alpha^n\beta^n)(\alpha\beta) = \alpha^n(\beta^n\alpha)\beta = (\alpha^n\alpha)(\beta^n\beta) = \alpha^{(n+1)}\beta^{(n+1)}$. Thus, $S(k)$ holds for all integers $k \geq 1$.

Next, we show that for any integer $k$, $(\alpha\beta)^k = \alpha^k\beta^k$. This has been proved for $k$ being a positive integer. If $k = 0$, then

$$(\alpha\beta)^0 = 1 = 1\cdot 1 = \alpha^0\beta^0.$$ 

It remains to show that this holds also when $k < 0$ is a negative integer. Let $k = -n$ for some positive integer $n > 0$. Note that as $\alpha\beta = \beta\alpha$,

$$\beta^{-1}\alpha^{-1} = (\alpha\beta)^{-1} = (\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}.$$ 

Therefore, by what we have proved above, $(\alpha^{-1}\beta^{-1})^n = (\alpha^{-1})^n(\beta^{-1})^n$. It follows

$$(\alpha\beta)^k = (\alpha\beta)^{-n} = ((\alpha\beta)^{-1})^n = (\alpha^{-1})^n(\beta^{-1})^n = \alpha^{-n}\beta^{-n} = \alpha^k\beta^k.$$ 

Thus the statement holds also for all integer $k$.

**An alternative proof for Part (i):** We apply induction on $n \geq 0$ for the statement:

$S(n)$: $(\alpha\beta)^n = \alpha^n\beta^n$.

$S(0)$ holds trivially and $S(1)$ is in the hypothesis. Therefore, we assume that $S(n)$ holds for $n \leq k \geq 1$ to prove that $S(k + 1)$ is also true.

$$(\alpha\beta)^{k+1} = (\alpha\beta)^{n+1} = (\alpha\beta)^n(\alpha\beta) = \alpha^n\beta^n\alpha\beta = \alpha^{n+1}\beta^{n+1}.$$
\[= \alpha^k \beta^k \alpha \beta \quad \text{induction hypothesis} \]
\[= \alpha^k \beta (\alpha^{1-k} \alpha^{k-1}) \beta^{k-1} \alpha \beta \quad \text{multiplying by an identity} \]
\[= \alpha^k \beta \alpha^{1-k} (\alpha^{k-1} \beta^{k-1}) \alpha \beta \quad \text{associative law} \]
\[= \alpha^k \beta \alpha^{1-k} (\alpha \beta)^{k-1} (\alpha \beta) \quad \text{induction hypothesis & asso. law} \]
\[= \alpha^k \beta \alpha^{1-k} (\alpha \beta)^k \quad \text{law of exponents} \]
\[= \alpha^k \beta \alpha \beta^k \quad \text{associative law} \]
\[= \alpha^k \beta \alpha \beta^k \quad S(1) \text{ is true} \]
\[= \alpha^{k+1} \beta^{k+1} \]

This proves \(S(+1)\). The rest of the proof is the same as above.

(ii) Let \(\alpha = (123), \beta = (13)\). We have \((\alpha \beta)^2 = (132)^2 = (123)\) and \(\alpha^2 \beta^2 = (12)^2 (13)^2 = 1\).

(2.13) (i) How many permutations in \(S_5\) commute with \((123)\), and how many even permutations in \(S_5\) commute with \((123)\)?

(ii) Same questions for \((12)(34)\).

Solution:  
(i) Let \(\sigma \in S_5\) be a permutation that commute with \((123)\). Then by

\[\sigma(123)(4)(5)\sigma^{-1} = (\sigma(1) \sigma(2) \sigma(3))(\sigma(4))(\sigma(5))\]

we have \(\sigma \in \{(1), (123), (132), (45), (123)(45), (132)(45)\}\), which are all permutations in \(S_5\) commuting with \((123)\). Among them \((1), (132), (123)\) are even.

(ii) With the same method, in \(S_4\), a permutation \(\sigma \in S_4\) commutes with \((12)(34)\) if and only if \(\sigma \in \{(1), (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1432)\}\). Among them, \((1), (12)(34), (13)(24), (14)(23)\) are even.

(2.14) Give an example of \(\alpha, \beta, \gamma \in S_5\), with \(\alpha \neq (1)\), such that \(\alpha \beta = \beta \alpha, \alpha \gamma = \gamma \alpha\) and \(\beta \gamma \neq \gamma \beta\).

Solution:  
Let \(\alpha = (12), \beta = (34), \gamma = (45)\). Then we have \(\alpha \beta = \beta \alpha, \alpha \gamma = \gamma \alpha\) and \(\beta \gamma \neq \gamma \beta\).

(2.15) If \(n \geq 3\), show that if \(\alpha \in S_n\) commute with every \(\beta \in S_n\), then \(\alpha = (1)\).

Proof:  
As \(\alpha\) can be expressed as a product of disjoint cycles, we may assume that
(1 2 \cdots k) is a longest cycle in the factorization of \(\alpha\) into disjoint cycles.

First, we claim that \(k \leq 2\). By contradiction, we assume that \(k \geq 3\). Pick \(\beta = (12)\). Then we must have \(\beta \alpha \beta^{-1} = \alpha\). However, \(\beta \alpha \beta^{-1}(1) = 3 \neq 2 = \alpha(1)\). Therefore, we must have \(k \leq 2\).

Next, we claim that \(\alpha\) cannot have more than one disjoint transpositions. If not, we may assume that \(\alpha = (12)(34) \cdots\). Let \(\beta = (13)\). Then we must have \(\beta \alpha \beta^{-1} = \alpha\). However, \(\beta \alpha \beta^{-1}(1) = 3 \neq 2 = \alpha(1)\). Therefore, the claim must hold.

Thus if \(\alpha\) is not the identity, it can only be a 2-cycle. We may assume that \(\alpha = (12)\). Now we pick \(\beta = (13)\) again. Then as \(\beta \alpha \beta^{-1}(1) = 3 \neq 2 = \alpha(1)\), we have a contradiction again. This implies that \(\alpha\) must be the identity.

**Section 2.3 Groups**

(2.19) (i) Compute the order, inverse, and parity of

\[\alpha = (12)(43)(13542)(15)(13)(23)\]

(ii) What are the respective orders of the permutations in Exercise 2.1 on page 49 and 2.8 on page 50?

**Solution:** (i) Since

\[\alpha = (12)(43)(13542)(15)(13)(23)\]
\[= (43)(14)(135)(135)(23)\]
\[= (43)(14)(153)(23)\]
\[= (14)(13)(15)(23)\]
\[= (14)(15)(23)\]
\[= (154)(23)\]

the order of (154) is 3 and the order of (23) is 2. Thus the order of \(\alpha\) is \(lcm(2, 3) = 6\). Direct computation yields that \(\alpha^{-1} = (23)(145)\) and \(sgn(\alpha) = (-1)^{5-2} = -1\). Therefore \(\alpha\) is odd.

(ii) For Exercise 2.1 on page 49, \(\alpha = (19)(28)(37)(46)\) is a product of 4 disjoint 2-cycles, and so the order is \(lcm(2, 2, 2, 2) = 2\).

For Exercise 2.1 on page 49, \(\alpha = (26 10 7)(39 4 5)\) is a product of two disjoint 4-cycles, and so the order is \(lcm(4, 4) = 4\).
(2.21) If $G$ is a group, prove that the only element $g \in G$ with $g^2 = g$ is 1.

**Proof:** If $g^2 = g$, then $g^{-1}g^2 = g^{-1}g$ and so $g = 1$.

(2.22) This exercise gives a shorter list of axioms defining a group. Let $H$ be a set containing an element $e$, and assume that there is an associative binary operation $\star$ on $H$ satisfying the following properties:

(1). $e \star x = x$ for all $x \in H$;
(2). for every $x \in H$, there is $x' \in H$ with $x' \star x = e$.

(i) Prove that if $h \in H$ satisfies $h \star h = h$, then $h = e$.
(ii) For all $x \in H$, prove that $x \star x' = e$.
(iii) For all $x \in H$, prove that $x \star e = x$.
(iv) Prove that if $e' \in H$ satisfies $e' \star x = x$ for all $x \in H$, then $e' = e$.
(v) Prove that $H$ is a group.

(2.23) Let $x \in H$. Prove that if $x'' \in H$ satisfies $x''x = e$, then $x'' = x'$.

**Proof:**
(i) Let $h \in H$ satisfies $h \star h = h$. By (2), $\forall h, \exists h' \in H$ with $h' \star h = e$. We have $h' \star (h \star h) = h' \star h$ and then $(h' \star h \star h = h' \star h$, that is $e \star h = h$. Thus, $h = e$.
(ii) Since $(x \star x')^2 = (x \star x')(x \star x') = x \star (x' \star x'x') = x \star x'$, by (i), $x \star x' = e$.
(iii) $x \star e = x \star (x' \star x) = (x \star x')\star x = e \star x = x$.
(iv) Since $(e')^2 = e'e' = e'$, by (i), $e' = e$.
(v) Since $x' \star x \star x'' = e \star x'' = x''$ and $x' \star x \star x'' = x' \star (x \star x') \star x'' \star x' = x' \star x = x'$, we have $x'' = x'$.
(vi) From above, we have the following observations:
(A) $\star$ is an associative binary operation;
(B) there is a unique identity $e$ in $H$;
(C) for any element $x$ in $H$, there is a unique $x'$ in $H$ such that $xx' = x'x = e$.

By the group axioms, $H$ is a group.

(2.24) Let $G$ be a group and let $a \in G$ have order $k$. If $p$ is a prime divisor of $k$, and if there is $x \in G$ with $x^p = a$, prove that $x$ has order $p^k$.

**Proof:** Let the order of $x$ be $n$. Since $x^{pk} = (x^p)^k = a^k = 1$, $n|pk$. Since $p$ is a prime, we have either $(n, p) = 1$ or $(n, p) = p$.

Suppose first assume that $(n, p) = 1$. Since $n|pk$ and since $(n, p) = 1$, by the Euclid Lemma, $n|k$. Since $1 = x^{np} = (x^p)^n = a^n$, $k|n$ and so $n = k$. But $p|k$ and so $(n, p) = p$, a contradiction.
Thus we must have \((n, p) = p\). Then \(p | n\) and so for some integer \(n_1, n = pm_1\). It follows that \(1 = x^n = (x^p)^{n_1} = a^{n_1}\). Thus \(k | n_1\), and so for some integer \(n_2, n_1 = kn_2\). Multiplying both sides by \(p\) to get \(n = pm_1 = pkn_2\). This implies that \((pk) | n\), and so we have \(n = pk\).

(2.25) Let \(G = GL(2, R)\), and let
\[
\begin{bmatrix}
0 & -1 \\
1 & 0 \\
\end{bmatrix}
\quad \text{and} \quad 
\begin{bmatrix}
0 & 1 \\
-1 & 1 \\
\end{bmatrix}
\].

Show that \(A^4 = I = B^6\), but that \((AB)^n \neq I\) for all \(n > 0\), where \(I = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}\) is the 2 \(\times\) 2 identity matrix. Conclude that \(AB\) can have infinite order even though both factors \(A\) and \(B\) have finite order.

Proof:
\[
A^4 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = I \\
B^6 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}^6 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} = I
\]

Arguing by induction on \(n\), we can prove that
\[
(AB)^n = \left( \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \right)^n = \left( \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} \right)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \neq I.
\]

Section 2.4 Lagrange’s Theorem

(2.30) (i) Define the special linear group by \(SL(2, R) = \{ A \in GL(2, R); \det(A) = 1 \}\). Prove that \(SL(2, R)\) is a subgroup of \(GL(2, R)\).

(ii) Prove that \(GL(2, Q)\) is a subgroup of \(GL(2, R)\).

Proof: (i) (1) \(I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, R)\), so \(SL(2, R) \neq \emptyset\).

(2) For any \(A, B \in SL(2, R)\), \(\det(AB) = \det(A) \det(B) = 1\), so \(AB \in SL(2, R)\).

(3) For any \(A \in SL(2, R)\), as \(AA^{-1} = I\), \(\det(A) \det(A^{-1}) = \det(I) = 1\). It follows that \(\det(A^{-1}) = \frac{1}{\det(A)} = 1\) and so \(A^{-1} \in SL(2, R)\).

Combining (1), (2), (3), we conclude that \(SL(2, R)\) is a subgroup of \(GL(2, R)\).

(ii) (1) \(I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, Q)\), so \(GL(2, Q) \neq \emptyset\).
(2) For any \( A, B \in GL(2, Q) \), \((\det)(AB) = (\det)(A)(\det)(B) \neq 0 \) and by the multiplication, \((AB)_{ij} = \sum_k a_{ik}b_{kj}\) is a rational number, so \( AB \in GL(2, Q) \).

(3) For any \( A \in GL(2, Q), A_{-1} = \frac{1}{\det(A)}A^* \). \((\det)(A)(A^{-1}) = (\det)(I) = 1 \). By the knowledge of linear algebra, every element of matrix of \( A^* \) is rational and \((\det)(A)\) is rational. So \( A^{-1} \in GL(2, Q) \).

Combing (1),(2),(3), we get \( GL(2, Q) \) is a subgroup of \( GL(2, R) \).

(2.31) (i) Give an example of two subgroups \( H \) and \( K \) of a group \( G \) whose union \( H \cup K \) is not a subgroup of \( G \).

(ii) Prove that the union \( H \cup K \) of two subgroups is itself a subgroup if and only if either \( H \) is a subset of \( K \) or \( K \) is a subset of \( H \).

**Proof:** (i) Let \( G = \mathbb{Z}, H = 2\mathbb{Z}, K = 3\mathbb{Z} \). Then as \( 2 \in 2\mathbb{Z} \) and \( 3 \in 3\mathbb{Z} \) but \( 2 + 3 = 5 \notin H \cup K \), \( H \cup K \nsubseteq \mathbb{Z} \).

(ii) If \( H \subseteq K \) or \( K \subseteq H \), then \( H \cup K \) is either \( H \) or \( K \), and so a subgroup of \( G \). Conversely, suppose, to the contrary, that there is \( a \in H - K \) and \( b \in K - H \) such that \( ab \in H \cup K \). If \( ab \in H \), then \( b = a^{-1}(ab) \in H \), a contradiction. If \( ab \in K \), then \( a = (ab)b^{-1} \in H \), a contradiction. Thus if \( H \cup K \subseteq G \), we must have either \( H - K = \emptyset \) or \( K - H = \emptyset \).

(2.32) Let \( G \) be a finite group with subgroups \( H \) and \( K \). If \( H \leq K \), prove that \([G : H] = [G : K][K : H]\).

**Proof:** By Lagrange, \([G : H] = \frac{|G|}{|H|}, [G : K] = \frac{|G|}{|K|}\) and \([K : H] = \frac{|K|}{|H|}\). Thus \([G : H] = [G : K][K : H]\).

(2.34) Prove that every subgroup \( S \) of a cyclic group \( G = \langle a \rangle \) is itself cyclic.

**Proof:** Let \( a^k \) be the element of \( S \) such that \( k = \min \{ i > 0 : a^i \in S \} \). Since \( G = \langle a \rangle \), any \( b \in S \) can be expressed as \( b = a^l \) for some integer \( l \). Write \( l = ks + t, 0 \leq t < k \). If \( t > 0 \), then \( a^t = a^{ks+t} = a^{ks}a^t \) and so \( a^t = a^l a^{-ks} \in H \), contradicting the choice of \( k \). Thus \( t = 0 \) and \( k|l \). Hence \( S = \langle a^k \rangle \).

(2.37) If \( H \) is a subgroup of a group \( G \), prove that the number of left closers of \( H \) in \( G \) is equal to the number of right closers of \( H \) in \( G \).

**Proof:** Let \( L \) and \( R \) denote the set of left cosets and right cosets of \( H \) in \( G \), respectively. Define a function \( f : L \mapsto R \) by \( f(aH) = Ha^{-1} \).

Since \( L \) is a set of equivalence classes, we must show that \( f \) is a well-defined map. In
other words, the value of \( f(aH) \) does not depend on the choice of representatives of the left coset \( aH \). To see that, let \( a, a_1 \in aH \) be two representatives of the left coset \( aH \). Then \( aH = a_1H \), and so \( aa_1^{-1} \in H \). It follows that \( Ha^{-1} = Ha_1^{-1} \) and so \( f(aH) = f(a_1H) \). Hence \( f \) is well-defined.

We shall show that \( f : L \mapsto R \) is injective. Suppose that \( f(a_1H) = f(a_2H) \). Then \( Ha_1^{-1} = Ha_2^{-1} \), and so \( a_1a_2^{-1} \in H \). This implies that \( a_1H = a_2H \). Hence \( f \) is injective.

It remains to show that \( f : L \mapsto R \) is surjective. For any \( Ha \in R, a^{-1} \in G \), and so \( f(a^{-1}H) = H(a^{-1})^{-1} = Ha \). Hence \( f \) is surjective.

Summing up, \( f : L \mapsto R \) is a bijective map.

Section 2.5 Homomorphisms

(2.40) (i) Show that the composite of homomorphisms is itself a homomorphism.

(ii) Show that the inverse of an isomorphism is an isomorphism.

(iii) Show that two groups that are isomorphic to a third group are isomorphic to each other.

(iv) Prove that isomorphism is an equivalence relation on any set of groups.

Proof:  
(i) Let \( f : G_1 \mapsto G_2, h : G_2 \mapsto G_3 \) be homomorphisms. For any \( g_1, g_2 \in G_1, f(g_1g_2) = f(g_1)f(g_2) \). Since \( f(g_1), f(g_2), f(g_1)f(g_2) \in G_2 \) and since \( h \) is a group homomorphism, \( h(f(g_1)f(g_2)) = h(f(g_1))h(f(g_2)) = (hf)(g_1)(hf)(g_2) \). That is \( (hf)(g_1g_2) = (hf)(g_1)(hf)(g_2) \), and so \( hf : G_1 \mapsto G_3 \) is also a group homomorphism.

(ii) Let \( f \) be an isomorphism from \( G_1 \) to \( G_2 \). Then \( f \) is a bijection and for any \( g_1, g_2 \in G_1 \), \( f(g_1g_2) = f(g_1)f(g_2) \). And so \( f^{-1} \) is a bijection from \( G_2 \) to \( G_1 \) and for any \( h_1, h_2 \in G_2 \), there are \( g_1, g_2 \in G_1 \) such that \( f(g_1) = h_1, f(g_2) = h_2 \). It follows that \( f^{-1}(h_1h_2) = f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2) \). Thus \( f^{-1} : G_2 \mapsto G_1 \) is also a group isomorphism.

(iii) Let \( f : G_1 \mapsto G_2 \) and \( h : G_3 \mapsto G_2 \) be group isomorphisms. By (ii), \( h^{-1} : G_2 \mapsto G_3 \) is an isomorphism. Thus by (i), \( g^{-1}f : G_1 \mapsto G_3 \) is a homomorphism. As the composition of two bijections is also a bijection, \( g^{-1}f : G_1 \mapsto G_3 \) is an isomorphism.

(iv) Define, for groups \( G \) and \( H \), that \( G \sim H \) if \( G \) is isomorphic to \( H \).

For any group \( G \), the identity map \( i : G \mapsto G \) is an isomorphism, and so \( G \sim G \). Thus \( \sim \) is reflexive.

By (ii), if \( f : G \mapsto H \) is an isomorphism, then \( f^{-1} : H \mapsto G \) is also an isomorphism. Thus \( \sim \) is symmetric.

Suppose that \( f : G_1 \mapsto G_2 \) and \( h : G_2 \mapsto G_3 \) are isomorphisms. Then by (iii), \( (hf) : G_1 \mapsto G_3 \) is also an isomorphism, and so \( \sim \) is transitive.
(2.42) This exercise gives some invariants of a group $G$. Let $f : G \rightarrow H$ be an isomorphism.

(i) Prove that if $a \in G$ has infinite order, then so does $f(a)$, and if $a$ has finite order $n$, then so does $f(a)$. Conclude that if $G$ has an element of some order $n$ and $H$ does not, then $G \not\cong H$.

(ii) Prove that if $G \cong H$, then for every divisor $d$ of $|G|$, both $G$ and $H$ have the same number of elements of order $d$.

**Proof:** Let $a \in G$ be an element with order $n$ and let $f(a) \in H$ have order $m$. If $n < \infty$, then $(f(a))^n = f(a^n) = f(1_G) = 1_H$ and so $m|n$. Thus $m$ is also finite. Applying the same argument to the isomorphism $f^{-1} : H \rightarrow G$, we conclude that if $m < \infty$, then $n|m$ and so $n$ must also be finite.

Moreover, this also shows that if one of $n$ or $m$ is finite, then $n|m$ and $m|n$, which imply that $n = m$.

(ii) Let $a_1, a_2, \cdots, a_k \in G$ be all the elements in $G$ that are of order $d$. Then as shown in (i), $f(a_1), f(a_2), \cdots, f(a_k) \in H$ are $k$ elements in $H$ that are of order $d$. If $y \in H - \{f(a_1), \cdots, f(a_k)\}$ has order $d$, then since $f$ is an isomorphism, $\exists x \in G - \{a_1, \cdots, a_k\}$ such that $f(x) = y$ and such that $x$ also has order $d$, contrary to the assumption that $\{a_1, a_2, \cdots, a_k\}$ is the set of all order $d$ elements in $G$. Thus both $G$ and $H$ have the same number of elements of order $d$.

(2.43) Prove that $A_4$ and $D_{12}$ are nonisomorphic groups of order 12.

**Proof:** Since the elements of $A_4$ has orders 1,2,or 3 but in $D_{12}$ there are elements of order 6, By Exercise 2.42(ii), $A_4$ and $D_{12}$ are not isomorphic.

(2.45) Show that every group $G$ with $|G| < 6$ is abelian.

**Proof:** We first prove the following claims for a finite group $G$.

Claim 1: Let $H$ be a subgroup of $G$, then $|H|$ divides $|G|$. This follows from the Lagrange Theorem.

Claim 2: If $|G|$ is prime, then $G$ must be cyclic. For any $g \in G$ with $g \neq 1$, $H = \langle a \rangle \leq G$.

Since $|G|$ is a prime and since $|H > 1$, by Claim 1, $|H| = |G|$, and so $G = H$ is cyclic.

By Claim 2, if $|G| \in \{2,3,5\}$, then $G$ is cyclic and so abelian. It remains to show the case when $|G| = 4$.

If $G$ has an element $a$ of order 4, then $G = \langle a \rangle$ is cyclic, and so abelian.

Hence by Claim 1, we conclude that every $g \in G - \{1\}$ must have order 2. Thus it
suffices to show that if a group $G$ in which every element $a \in G$, $a^2 = 1$, then $G$ is abelian.

Let $G$ be such a group. $\forall a, b \in G$, we have $(ab)^2 = 1 = a^2b^2$. This implies that $abab = aabb$. Cancelling $a$ from left and $b$ from right, we have $ba = ab$, and so $G$ is abelian.

(2.47) (i) If $f : G \rightarrow H$ is a homomorphism and $x \in G$ has order $k$, prove that $f(x) \in H$ has order $m$, where $m|k$.

(ii) If $f : G \rightarrow H$ is a homomorphism and if $|G|, |H| = 1$, prove that $f(x) = 1$ for all $x \in G$.

Proof: Since $f : G \rightarrow H$ is a homomorphism, for $x \in G$ of order $k$ in $G$, $(f(x))^k = f(x^k) = f(1_G) = 1_H$. If $f(x)$ has order $m$, then $m|k$.

(ii) The problem assumes that both $|G|$ and $|H|$ are finite. By contradiction, suppose there exists $x \in G$ with order $k$ but $f(x) \neq 1$. Let the order of $f(x)$ be $m > 1$. By (i), $m|k$. By Lagrange, $k$ divides $|G|$, and $m$ divides $|H|$. It follows by $m|k$ that $m > 1$ is a common divisor of both $|G|$ and $|H|$, contrary to the assumption that $|G|, |H| = 1$.

(2.50) (i) Show that if $H$ is a subgraph with $bH = Hb = \{hb : h \in H\}$ for every $b \in G$, then $H$ must be a normal subgroup.

(ii) Use part (i) to give a second proof of Proposition 2.62(ii): If $H \leq G$ has index 2, then $H \trianglelefteq G$.

Proof: (i) For any for every $b \in G$, $bH = Hb = \{hb : h \in H\}$. Then for any $h \in H$, $bh = h_1b$ for some $h_1 \in H$ and so $bhd^{-1} = h_1 \in H$. Thus by definition of a normal subgroup, $H$ is a normal subgroup of $G$.

(ii) Since $\forall b \in G - H$, $bH \cap H = \emptyset$ and $[G : H] = 2$, and since $[G : H]$ counts the number of left (right) cosets of $H$ in $G$, we have $G = H \cup bH = H \cup Hb$. That means that $\forall b \in G$, $bH = Hb$ and so by (i), $H \trianglelefteq G$.

(2.53) Define $W = \langle (12)(34) \rangle$, the cyclic subgroup of $S_4$ generated by $(12)(34)$. Show that $W$ is a normal subgroup of $V$, but that $W$ is not a normal subgroup of $S_4$. Conclude that normality is not transitive: $W \leq V$ and $V \leq G$ do not imply $W \leq G$.

Proof: Since for every $g \in S_4$, $x \in V$, $g^{-1}xg \in V$, then $V \leq S_4$.

Since $V = \{(1), (12)(34), (13)(24), (14)(23)\}$, $W = \langle (12)(34) \rangle = \{(1), (12)(34)\}$ is a subgroup of $W$ of index $2$, by Exercise 2.50, $W \leq V$.

Since $(13)^{-1}(12)(34)(13) = (14)(23) \not\in W$, $W \not\trianglelefteq S_4$.

(2.55) Give an example of a group $G$, a subgroup $H \leq G$, and an element $g \in G$ with
\[ G : H \] = 3 and \( g^3 \not\in H. \)

**Proof:** Take \( G = S_3, H = \langle (12) \rangle, g = (23). \) Then \( g \in S_3. \) By Lagrange, \( [G : H] = 3. \) But \( g^3 = g \not\in H. \)

(2.60) Assume that there is a group of order 8 whose elements \( 1, i, j, k \) satisfy \( i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, \) and \( ij = -ji, ik = -ki, jk = -kj. \) Prove that \( G \cong Q \) and, conversely, that \( Q \) is such a group.

**Proof:** Define bijection \( \sigma \) by setting \( \sigma(1) = I, \sigma(i) = A, \sigma(j) = B, \sigma(k) = BA^3, \sigma(-1) = A^2, \sigma(-i) = A^3, \sigma(-j) = BA^2, \sigma(-k) = BA. \) We can verify that this bijection keep the operation and \( G \cong Q. \)

**Section 2.6 Quotient Groups**

(2.65) Prove \( U(\mathbb{Z}_9) \cong \mathbb{Z}_6 \) and \( U(\mathbb{Z}_{15}) \cong \mathbb{Z}_4 \times \mathbb{Z}_2. \)
Proof: Note that \( U(\mathbb{Z}_9) = \{ x \in \mathbb{Z}_9 : (x, 9) = 1 \} = \{ [1], [2], [4], [5], [7], [8] \} \), and the binary operation is multiplication. Direct computation yields that the order of \([2]\) in the multiplicative group \( U(\mathbb{Z}_9) \) is 6, and so \( U(\mathbb{Z}_9) = \langle [2] \rangle \cong \mathbb{Z}_6 \), as \( \mathbb{Z}_6 \) is also a cyclic group of order 6.

Note that \( G = U(\mathbb{Z}_{15}) = \{ [x] \in \mathbb{Z}_{15} : (x, 15) = 1 \} = \{ [1], [2], [4], [7], [8], [11], [13], [14] \} \), and the binary operation is multiplication. Direct computation reveals that the order of 4 elements are \([2], [7], [8], [13]\) and order 2 elements are \([4], [11], [14]\).

Let \( H = \{ [1], [2], [4], [8] \} \), and \( K = \{ [1], [11] \} \). Then \( G \) is abelian, \( H \leq G \), and \( K \cap H = \{ [1] \} \). Thus \( |HK| = |G| \) and so \( G = HK = \{ hk : h \in H, k \in K \} \). Moreover, if \( hk = h_1k_1 \) for some \( h, h_1 \in H \) and \( k, k_1 \in K \), then \( h_1^{-1}h = k_1k^{-1} \in H \cap K = \{ [1] \} \), and so \( h = h_1 \) and \( k = k_1 \).

As \( [2] \) is a generator of \( H \) and \([11]\) is a generator of \( K \), and as every element in \( G \) can be uniquely expressed as \([2]^i[11]^j \) where \( 0 \leq i \leq 3 \) and \( 0 \leq j \leq 1 \), the following map \( \phi : U(\mathbb{Z}_{15}) \to \mathbb{Z}_4 \times \mathbb{Z}_2 \) is an isomorphism.

\[
\phi = \begin{pmatrix}
(0, 0) & (0, 1) & (0, 2) & (0, 3) & (1, 0) & (1, 1) & (1, 2) & (1, 3)
\end{pmatrix}.
\]

(2.66) (i) Let \( H \) and \( K \) be groups. Without using the first isomorphism theorem, prove that \( H^* = \{ (h, 1) : h \in H \} \) and \( K^* = \{ (1, k) : k \in K \} \) are normal subgroups of \( H \times K \) with \( H \cong H^* \) and \( K \cong K^* \), and \( f : H \to (H \times K)/K^* \), defined by \( f(h) = (h, 1)K^* \), is an isomorphism.

(ii) Use the first isomorphism theorem to prove that \( K^* \trianglelefteq H \times K \) and that \( (H \times K)/K^* \cong H^* \).

Proof: (i) By the definition of \( H^* \), we have \( H^* \trianglelefteq H \times K \). Note that \( (1_H, 1_K) \in H^* \neq \emptyset \). \( \forall (h_1, 1_K), (h_2, 1_K) \in H^* \), we have \( h_1, h_2 \in H \). Since \( H \) is a group, \( h_1h_2^{-1} \in H \), and so \( (h_1, 1_K)(h_2, 1_K)^{-1} = (h_1h_2^{-1}, 1_K) \in H^* \), and so \( H^* \trianglelefteq H \times K \). \( \forall (h, 1) \in H^* \) and \( \forall (h_1, k_1) \in H \times K \), \( (h_1, k_1)(h, 1)(h_1, k_1)^{-1} = (h_1hh_1^{-1}, k_1k_1^{-1}) = (h', 1_K) \in H^* \), where \( h' = h_1hh_1^{-1} \in H \). By definition, \( H^* \trianglelefteq H \times K \). Similarly, \( K^* \trianglelefteq H \times K \).

Define a map \( \phi : H \to H^* \) by \( \phi(h) = (h, 1) \), \( \forall h \in H \). Then \( \forall h_1, h_2 \in H \), \( \phi(h_1h_2) = (h_1h_2, 1_K) = (h_1, 1_K)(h_2, 1_K) = \phi(h_1)\phi(h_2) \), and so \( \phi \) is a homomorphism. If \( h \in \ker(\phi) \), then \( (h, 1_K) = (1_H, 1_K) \), and so \( h = 1_H \). Hence \( \ker(\phi) = \{ 1_H \} \), and so \( \phi \) is an injection. \( \forall (h, 1_K) \in H^* \), \( h \in H \) and so \( \phi(h) = (h, 1_K) \), and so \( \phi \) is surjective. Hence \( H \cong H^* \). Similarly, \( K \cong K^* \).

To see that \( f \) is an isomorphism, we first check that \( f \) is a homomorphism. Let \( h_1, h_2 \in H \). Then

\[
f(h_1h_2) = (h_1h_2, 1_K)K^* = (h_1, 1_K)K^*(h_2, 1_K)K^* = f(h_1)f(h_2),
\]
and so \( f \) is a homomorphism. \( \forall (h, k)K^* \in (H \times K)/K^*, f(h) = (h, 1_K)K^* = (h, 1_K)(1_H, k)K^* = (h, k)K^* \), and so \( f \) is surjective. If \( h_1, h_2 \in H \) such that \((h_1, 1_K)K^* = f(h_1) = f(h_2) = (h_2, 1_K)K^*\), then \((h_2, 1_K)^{-1}(h_1, 1_K) \in K^*\), and so \((h_2^{-1}h_1, 1_K) \in K^*\). It follows that \( h_2^{-1}h_1 = 1_H \), or equivalently, \( h_1 = h_2 \). Thus \( f \) is injective, and so \( f \) is an isomorphism.

(ii) Define a map \( f : (H \times K) \mapsto H^* \) by \( f(h, k) = (h, 1_K) \). Then

\[
f((h_1, k_1)(h_2, k_2)) = f((h_1h_2, k_1k_2)) = (h_1h_2, 1_K) = (h_1, 1_K)(h_2, 1_K) = f(h_1, k_1)f(h_2, k_2).
\]

Thus \( f \) is a homomorphism. To determine the kernel of \( f \), we note that

\[
ker(f) = \{(h, k) : (h, 1_K) = (1_H, k)\} = \{(1_H, k) : \forall k \in K\} = K^*.
\]

Consider the image of \( f \). \( \forall (h, 1_K) \in H^*, f(h, 1_K) = (h, 1_K) \) and so \( \text{im}(f) = H^* \). Therefore by the 1st isomorphism theorem, \((H \times K)/K^* \cong H^*\).

(2.67) (i) Prove that \( \text{Aut}(V) \cong S_3 \) and that \( \text{Aut}(S_3) \cong S_3 \). Conclude that non isomorphic groups can have isomorphism groups.

(ii) Prove that \( \text{Aut}(Z) \cong Z_2 \). Conclude that an infinite group can have a finite automorphism group.

**Proof:**

(i) Recall that

\[
V = \{(1)(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.
\]

Let \( a_1 = (1, 2)(3, 4), a_2 = (1, 3)(2, 4) \) and \( a_3 = (1, 4)(2, 3) \). Since any automorphism \( f \in \text{Aut}(V) \) must fix the identity element, the map \( f \) is uniquely determined by its image on \( f(a_1), f(a_2) \) and \( f(a_3) \). Since \( a_i a_j = a_k \) for \( \{i, j, k\} = \{1, 2, 3\} \), \( f \) is uniquely determined by its image on \( f(a_1) \) and \( f(a_2) \).

Direct computation shows that each \( a_i \) has order 2. Let \( f \in \text{Aut}(V) \). Then as \( f(a_i) \) must have the same order of \( a_i \), we must have \( f(a_i) = a_{f(i)} \), \( \forall i \in \{1, 2, 3\} \), where \( f' \in S_3 \). Therefore, the map \( \phi(f) = f' \) is a map \( \phi : \text{Aut}(V) \mapsto S_3 \).

Let \( f_1, f_2 \in \text{Aut}(V) \). Then \( \forall a_i \in V \),

\[
(f_1f_2)(a_i) = f_1(f_2(a_i)) = f_1a_{f_2(i)} = a_{f'_1(f'_2(i))}.
\]

Thus \( \phi(f_1f_2) = \phi(f'_1f'_2) = \phi(f_1)\phi(f_2) \), and so \( \phi \) is a group homomorphism. Let \( f \in ker(\phi) \). Then \( f(a_i) = a_i \) for any \( i \), which implies that \( f \) is the identity map in \( \text{Aut}(V) \), and so \( \phi \) is injective.

It remains to show that \( \phi \) is surjective. For any \( s \in S_3 \), Define \( f_s : V \mapsto V \) by \( f_s(1) = (1) \) and \( f_s(a_i) = a_{s(i)} \). Then \( f_s \) is a bijection. Moreover, as \( s \) is a permutation on \( \{1, 2, 3\} \), and
as every \( a_i \) has order 2, \( \forall a_i, a_j \in V \), \( f_s(a_i a_j) = f_s(a_k) = a_s(k) = a_s(i)a_s(j) = f_s(a_i)f_s(a_j) \), and so \( f_s \in Aut(V) \) and \( \phi(f_s) = s \). Thus \( \phi \) is onto. This proves that \( Aut(V) \cong S_3 \).

To show that \( Aut(S_3) \cong S_3 \), we again first study how an \( f \in Aut(S_3) \) would behave. Let
\[
a_1 = (1\ 2), \ a_2 = (1\ 3), \ a_3 = (2\ 3), \ b_1 = (1\ 2\ 3), \ b_2 = (1\ 3\ 2).
\]
Then as \( f(x) \) and \( x \) must have the same order, \( f(a_i) = a_j \) where \( i, j \in \{1, 2, 3\} \). Moreover, as \( a_1 a_2 = b_2 \) and \( a_1 a_3 = b_1 \), when \( f \) is an automorphism, the image of \( f(b_1) \) and \( f(b_2) \) are uniquely determined by \( f(a_1), f(a_2) \) and \( f(a_3) \). As \( f(a_i) = a_s(i) \) for some \( s \in S_3 \), the isomorphism between \( Aut(S_3) \cong S_3 \) can be found similar to what we have done in \( Aut(V) \cong S_3 \).

(ii) Let \( f \in Aut(Z) \). Then consider the image of \( f(1) \). If \( f(1) = m \notin \{1, -1\} \), then as \( 0 = f(0) = f(1 + (-1)) = f(1) + f(-1) = m + f(-1) \), we must have \( f(-1) = -m \). It follows by the assumption that \( f \) is an homomorphism, \( \forall n \in Z \) with \( n > 0 \), \( f(n) = f(1+1+\cdots+1) = n \cdot f(1) = nm \in mZ \), and \( f(-n) = -mn \). Thus \( f(Z) \subseteq mZ \subseteq Z - \{1, -1\} \), contrary to the assumption that \( f \) is an automorphism. Therefore, either \( f(1) = 1 \) or \( f(1) = -1 \). Let \( f_0, f_1 \in Aut(Z) \) be such that \( f_0(1) = 1 \) and \( f_1(1) = -1 \). Then since \( f_0, f_1 \) are homomorphisms, \( f_0(n) = n \) and \( f_1(n) = -n \). The map composition yields that \( f_1 f_0 = f_0 f_1 = f_1 \), \( f_1 f_1 = f_0 = f_0 f_0 \). Therefore, a map \( \phi : Aut(Z) \rightarrow \mathbb{Z}_2 \) given by \( \phi(f_0) = 0 \) and \( \phi(f_1) = 1 \) is a group isomorphism.

(2.69) Prove that if \( G \) is a group for which \( G/Z(G) \) is cyclic, where \( Z(G) \) denotes the center of \( G \), then \( G \) is abelian.

**Proof:** Let \( Z = Z(G) \). Since \( G/Z \) is cyclic, we may assume the for some \( a \in G \), \( G/Z = \langle aZ \rangle \). Let \( g, h \in G \). (We want to show that \( gh = hg \)). Then \( gZ = aZ \) and \( hZ = aZ \), and so \( \exists z_1, z_2 \in Z \) such that \( g = a^i z_1 \) and \( h = a^j z_2 \). It follows by the definition of \( Z(G) \) and by \( z_1, z_2 \in Z \) that
\[
gh = a^i z_1 a^j z_2 = a^i a^j z_1 z_2 = a^{i+j} z_2 z_1 = a^j a^i z_2 z_1 = a^j z_2 a^i z_1 = hg.
\]

(2.70) (i) Prove that \( Q/Z(Q) \cong V \), where \( Q \) is the group of quaternions and \( V \) is the four-group; conclude that the quotient of a group by its center can be abelian.
(ii) Prove that \( Q \) has no subgroup isomorphic to \( V \). Conclude that the quotient \( Q/Z(Q) \) is not isomorphic to a subgroup of \( Q \).
Proof: Recall that

\[ V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}. \]

Note that \( \phi : V \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \) given below

\[
\phi = \begin{pmatrix}
(1) & (1,2)(3,4) & (1,3)(2,4) & (1,4)(2,3) \\
(0,0) & (0,1) & (1,0) & (1,1)
\end{pmatrix}
\]

is an isomorphism. Therefore we can have the following proofs. The following proofs can also be given directly without going through \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) by replacing \((x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \) by \( \phi^{-1}(x, y) \).

(i) Let \( Z = Z(Q) \). Note that \( Q/Z = \{Z, AZ, BZ, (BA)Z\} \), as \( Z = A^2Z \), \( AZ = A^3Z \), \( BZ = (BA^2)Z \) and \( (BA)Z = BA^3Z \).

Define a map \( f : Q/Z \rightarrow V \) by \( f(Z) = (0,0), f(AZ) = (1,0), f(BZ) = (0,1) \) and \( f((BA)Z) = (1,1) \). Since \((AZ)(BZ) = (AB)Z = (BA)Z = (BZ)(AZ), (BAZ)(AZ) = (BZ)(BA)Z = (AB)(BA)Z = (BA)Z((BA)Z) = (BA)Z((BA)Z) = (BBA^3)Z = ((BA)Z)(BZ)\), and since in \( V \), \((1,0) + (0,1) = (1,1) \), \((1,1) + (1,0) = (0,1) \) and \((0,1) + (1,1) = (1,0) \), \( f \) is a bijective homomorphism, and so \( f \) is an isomorphism.

(ii) Since \( V \) has 3 elements of order 2, and \( Q \) has only one element of order 2 (Exercise (2.59)(iii)), no subgroup of \( Q \) can be isomorphic to \( V \).

(2.72) If \( H \) and \( K \) are subgroups of a group \( G \), prove that \( HK \) is a subgroup of \( G \) if and only if \( HK = KH \).

Proof: Suppose first that \( HK \leq G \). Note that \( \forall h \in H \) an \( \forall k \in K \), as \( h = h \cdot 1 \in HK \)
and \( k = 1 \cdot k \in HK \), \( kh \in HK \), and so \( KH \subseteq HK \). On the other hand, since \( HK \leq G \), \( HK = \{x^{-1} : x \in HK\} \). Therefore, \( \forall x \in HK \), we can write \( x = (h)^{-1} \) for some \( h \in H \) and \( k \in K \). However, \( (hk)^{-1} = k^{-1}h^{-1} \in KH \), and so \( HK \subseteq KH \).

Conversely, we assume that \( HK = KH \). Then \( 1 \in HK \neq \emptyset \). For \( x, y \in HK \), we can write \( x = h_1k_1 \) and \( y = h_2k_2 \) for some \( h_1, h_2 \in H \) and \( k_1, k_2 \in K \). Then \( xy^{-1} = h_1k_1^{-1}h_2^{-1} \).
Note that since \( K \leq G \) and \( H \leq G \) \( k_1k_2^{-1}h_2^{-1} \in KH \). As \( KH = HK \), we can write \( k_1k_2^{-1}h_2^{-1} = kh \) for some \( h \in H \) and \( k \in K \). Thus \( xy^{-1} = h_1k_1^{-1}h_2^{-1} = (h_1h)k \in HK \), and so \( HK \leq G \).

(2.76) If \( H \) and \( K \) are normal subgroups of a group \( G \) with \( HK = G \), prove that \( G/(H \cap K) \cong (G/H) \times (G/K) \).

Proof: Since \( H \) and \( K \) are normal in \( G \), \( G/H \) and \( G/K \) are groups. Define a map
\( f : G \mapsto (G/H) \times (G/K) \) by \( f(x) = (xH, xK) \). Then \( \forall x, y \in G, \)

\[
f(xy) = ((xy)H, (xy)K) = (xH, xK)(yH, yK) = f(x)f(y),
\]

and so \( f \) is a homomorphism. Let \( L = \ker(f) \). Then

\[
L = \{ x \in G : f(x) = (H, K) \} = \{ x \in G : xH = H \& xK = K \} = \{ x \in G : x \in H \& x \in K \} = H \cap K.
\]

Since \( HK = G \), by Exercise 2.72, \( G = KH \). For any \( (aH, bK) \in (G/H) \times (G/K) \), we can write \( a = a_ka_H \) with \( a_H \in H \) and \( a_K \in K \), and \( b = b_kb_K \) with \( b_H \in H \) and \( b_K \in K \). Let \( x = a_Kb_H \in G \). Then \( f(x) = ((a_Kb_H)H, (a_Kb_H)K) = (a_KH, b_HK) = ((a_Ka_H)H, (b_Kb_H)K) = (aH, bK) \). Therefore, \( f \) is onto. By the first isomorphism Theorem, \( G/(H \cap K) \cong (G/H) \times (G/K) \).