Abstract Algebra, 3rd Edition
David S. Dummit and Richard M. Foote
newell.jensen@gmail.com

Chapter 3 - Quotient Groups and Homomorphisms

Exercises:

3.1 DEFINITION AND EXAMPLES

Let G and H be groups.

1. Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker\varphi \trianglelefteq G$.

Proof. Since E is a subgroup of H we know it contains the identity 1_H and since we know that homomorphisms map identities to identities, i.e., $\varphi(1_G) = 1_H$ we see that

$$\begin{aligned}\varphi^{-1}(1_H) &= \varphi^{-1}(\varphi(1_G)) \\ &= 1_G\end{aligned}$$

If $x, y \in \varphi^{-1}(E)$, say $\varphi(x) = a, \varphi(y) = b$, where $a, b \in E$. Then $\varphi(y^{-1}) = \varphi(y)^{-1} = b^{-1}$ [Proposition 1 (2)] and $b^{-1} \in E$ since E is a group and contains inverses.

$$\begin{aligned} ab^{-1} &= \varphi(x)\varphi(y)^{-1} & \\ ab^{-1} &= \varphi(x)\varphi(y^{-1}) & \text{[Proposition 1 (2)]} \\ ab^{-1} &= \varphi(xy^{-1}) & \text{[}\varphi\text{ is a homomorphism]} \\ \varphi^{-1}(ab^{-1}) &= xy^{-1} & \text{[applying } \varphi^{-1} \text{ to both sides]}\end{aligned}$$

Thus, $xy^{-1} \in \varphi^{-1}(E)$ and therefore by the subgroup criterion $\varphi^{-1}(E) \leq G$.

If $E \trianglelefteq H$ then for all $h \in H$ we have that $hEh^{-1} = E$. Let $g_1, g_2 \in G$ such that $g_1 = \varphi^{-1}(h)$ and $g_2 = \varphi^{-1}(h^{-1})$ so that

$$\begin{aligned} hEh^{-1} &= E & \text{[}E \trianglelefteq H\text{]} \\ \varphi^{-1}(hEh^{-1}) &= \varphi^{-1}(E) & \text{[applying } \varphi^{-1} \text{ to both sides]} \\ \varphi^{-1}(h)\varphi^{-1}(E)\varphi^{-1}(h^{-1}) &= \varphi^{-1}(E) & \text{[}\varphi\text{ is a homomorphism]} \\ g_1\varphi^{-1}(E)g_2^{-1} &= \varphi^{-1}(E) & \text{[Proposition 1 (2) for } g_2\text{]}\end{aligned}$$

Additionally, since this is true for all of $h \in H$ it is also true for all $g \in G$ as g_1 and g_2 where the fibers for h and h^{-1} (i.e., $\varphi(g_1) = h, \varphi(g_2) = h^{-1}$). Therefore, $\varphi^{-1}(E) \trianglelefteq G$

Furthermore, since $1_H \in E$ and the $\ker\varphi = \{g \in G \mid \varphi(g) = 1\}$ we see that the above proof can be extended to the kernel of φ such that

$$\begin{aligned} g_1\varphi^{-1}(1_H)g_2^{-1} &= \varphi^{-1}(1_H) & \\ g_1\varphi^{-1}(\varphi(g))g_2^{-1} &= \varphi^{-1}(\varphi(g)) & \text{[definition of kernel]} \\ g_1 g g_2^{-1} &= g & \end{aligned}$$

which is true as G is a group. Thus, we deduce that $\ker\varphi \trianglelefteq G$. □

2. Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

Proof. Suppose $u \in X$ and $w \in Z$. Let $v = u^{-1}w$. Then

$$\begin{aligned}
\varphi(v) &= \varphi(u^{-1}w) \\
&= \varphi(u^{-1})\varphi(w) \\
&= \varphi(u)^{-1}\varphi(w) \\
&= a^{-1}ab && [Z \text{ is defined to be the fiber above the product } ab] \\
&= b
\end{aligned}$$

Thus, $v \in Y$.

Therefore, if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. □

3. Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof. To show that A/B is abelian we must show that its elements commute. The elements of A/B are the left or right cosets. Let $X, Y \in A/B$ where for any $u \in X$ and $v \in Y$ we have $X = \{ub \mid b \in B\}, Y = \{vb \mid b \in B\}$. Thus, since A is abelian and its elements commute we see that

$$XY \implies (ub)(vb) = (vb)(ub) \implies YX$$

Therefore, A/B is abelian. □

An example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian is $G = D_8$ and $N = \langle r^2 \rangle$ which was shown in the examples to be isomorphic to the Klein 4 group which is abelian.

4. Prove that in the quotient group $G/N, (gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Proof. Since G/N is a quotient group N is the kernel of some homomorphism and by Theorem 3, this quotient group has elements of left cosets gN with the operation defined by

$$g_1N \circ g_2N = (g_1g_2)N$$

Therefore, for any $\alpha \in \mathbb{Z}$ we have that

$$(gN)^\alpha = (gN)_1 \cdots (gN)_\alpha = (g^\alpha)N$$

Therefore, in the quotient group G/N we have that $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$. □

5. Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Proof. Let $g \in G$ and $g^m = 1$ with m being the smallest integer with this property. Let's also suppose that the order of gN is n. Then, since N is the identity element in G/N we see that

$$(gN)^m = g^m N = N$$

Thus, since the order of gN was given to be n we also see that

$$|gN| = n \implies (gN)^n = N \implies g^n N = N$$

and $g^n \neq 1$ as m was the smallest integer with this property so therefore g^n must be an element of N. Additionally n is the smallest positive integer such that $g^n \in N$ [we know it is the smallest positive integer from the definition of order]. □

For an example showing the order of gN in G/N being strictly smaller than the order of g in G, let us take $G = Z_4$, the cyclic group of order 4. Let $g \in G$ such that $g^4 = 1$ and $N = \{1, g^2\}$ is a normal subgroup (this can easily be shown by conjugation). Then, $gN = \{g, g^3\}$ and we see that $(gN)^2 = g^2 N = \{g^2, 1\} = N$ so therefore the order of gN is 2 while the order of g is 4.

6. Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Proof. The fibers of φ are the positive and negative elements of $\mathbb{R}^\times$. That is $\varphi^{-1}(\pm 1) = \{\pm x \mid x \in \mathbb{R}^\times\}$

Let $x, y \in \mathbb{R}^\times$. Then

$$\varphi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \varphi(x)\varphi(y)$$

Therefore, φ is a homomorphism. □

7. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

Proof. First, let's show that π is a homomorphism. Let $x_1, x_2, y_1, y_2 \in \mathbb{R}^2$ so that

$$\begin{aligned} \pi((x_1, y_1) + (x_2, y_2)) &= \pi((x_1 + x_2, y_1 + y_2)) && \text{[vector addition in } \mathbb{R}^2\text{]} \\ &= (x_1 + x_2) + (y_1 + y_2) \\ &= (x_1 + y_1) + (x_2 + y_2) \\ &= \pi((x_1, y_1)) + \pi((x_2, y_2)) \end{aligned}$$

Therefore, π is a homomorphism. It is easy to see that this is a surjective homomorphism since any element of $\mathbb{R}$ can be produced from the components of the vector in $\mathbb{R}^2$, i.e., $z = x + y \in \mathbb{R} \implies (x, y) \in \mathbb{R}^2$. □

Let the coordinate axis of $\mathbb{R}^2$ be x and y. Then the kernel of π is the line $y = -x$ and the fibers of π are the summations of the vector projections on the axis x and y.

8. Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

Proof. Let $x, y \in \mathbb{R}^\times$ so that

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$$

Therefore, φ is a homomorphism. The image of φ is $\mathbb{R}^+$. The kernel of φ is $\{\pm 1\}$ and the fibers of φ are $\varphi^{-1}(a) = \{\pm a \mid a \in \mathbb{R}^\times\}$. □

9. Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

Proof. Let $a + bi, c + di \in \mathbb{C}^\times$ so that

$$\begin{aligned}
\varphi((a+bi)(c+di)) &= \varphi((ac-bd)+(ad+bc)i) \\
&= (ac-bd)^2 + (ad+bd)^2 \\
&= (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2adbc + (bc)^2 \\
&= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 \\
&= (a^2+b^2)(c^2+d^2) \\
&= \varphi(a+bi)\varphi(c+di)
\end{aligned}$$

Therefore, φ is a homomorphism. The image of φ is the square of the modulus of the complex vector, $a + bi$. The kernel of φ is the unit circle in $\mathbb{C}^\times$ since these complex numbers all have norm equal to 1. The fibers of φ are complex numbers that have the same norms. Thus, the fibers of φ are circles in the complex plane centered at the origin. □

10. Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. Show that this is well-defined, surjective homomorphism and describes its fibers and kernel explicitly (showing that φ is well-defined involves the fact that $\overline{a}$ has a different meaning in the domain and range of φ).

Proof. φ is obviously a homomorphism as

$$\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a+b}) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(\overline{a}) + \varphi(\overline{b})$$

Additionally, it is trivially surjective as $\varphi(\overline{a}) = \overline{a}$. To see that it is well-defined we can manually check that for all elements of the domain it maps to an element in the codomain.

$$\begin{aligned}
\varphi(\overline{0}) &= \overline{0} \\
\varphi(\overline{1}) &= \overline{1} \\
\varphi(\overline{2}) &= \overline{2} \\
\varphi(\overline{3}) &= \overline{3} \\
\varphi(\overline{4}) &= \overline{0}
\end{aligned}$$

$$\varphi(\overline{5}) = \overline{1}$$
$$\varphi(\overline{6}) = \overline{2}$$
$$\varphi(\overline{7}) = \overline{3}$$

The kernel of φ is $\{\overline{0}, \overline{4}\}$ and the fibers of φ are the sets $\{\overline{a}, \overline{a+4} \mid a \in \mathbb{Z}/4\mathbb{Z}\}$. □

11. Let F be a field and let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F, ac \neq 0 \right\} \leq GL_2(F)$.

(a) Prove that the map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ is a surjective homomorphism from G onto $F^\times$ (recall that $F^\times$ is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ.

Proof. Let $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in G$ so that

$$\varphi(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}) = \varphi\left(\begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}\right) = a_1a_2 = \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}\right)$$

Thus, φ is a homomorphism and is surjective as a can be all of $F^\times$. The kernel of φ is the group of elements $\begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix}$. The fibers of φ for a given a are $\varphi^{-1}(a) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a \in F^\times \right\}$, the collection of matrices with matching entries in the position of a. □

(b) Prove that the map $\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

Proof. Let $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in G$ so that

$$\begin{aligned} \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}\right) \\ &= (a_1a_2, c_1c_2) \\ &= (a_1, c_1)(a_2, c_2) \\ &= \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\right)\varphi(\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}) \end{aligned}$$

Thus, φ is a homomorphism and is surjective as a and c can all of $F^\times$ so that (a, c) is all of $F^\times \times F^\times$. The kernel of φ is the group of elements $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. The fibers of φ for a given a and c are $\varphi^{-1}((a, c)) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in F^\times \right\}$, the collection of matrices with matching entries in the positions of a and c. □

(c) Let $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F \right\}$. Prove that H is isomorphic to the additive group F.

Proof. Let $\varphi : H \to F$ such that $\varphi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = b$, for $b \in F$. Then φ is a bijective homomorphism from H to F and therefore H is isomorphic to F (the proof of φ being a surjective homomorphism is similar to part (a) and we can see it is injective as $\varphi(b_1) = \varphi(b_2) \implies b_1 = b_2$). □

12. Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi ir}$. Draw the points on a real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points $-1, i$, and $e^{4\pi i/3}$ of H. (Figure 1 of the text for this homomorphism φ is usually depicted using the following diagram [please see text for the diagram].)

The points on a real line which lie in the kernel of φ are $\mathbb{Z}$ as the integers make $e^{2\pi ir}$ equal to 1. The elements in the fibers of φ above the points $-1, i$, and $e^{4\pi i/3}$ are $\frac{1+4n}{2}, \frac{1+4n}{4}, \frac{2n}{3}$, for $n \in \mathbb{Z}$, respectively.

13. Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi ir}$.

The kernel of φ is again $\mathbb{Z}$. The elements in the fibers of φ above the points $-1, i$, and $e^{4\pi i/3}$ are $\frac{1+4n}{4}, \frac{1+4n}{8}, \frac{n}{3}$, for $n \in \mathbb{Z}$, respectively.

14. Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

Proof. Every coset of $\mathbb{Z}$ in the additive quotient group $\mathbb{Q}/\mathbb{Z}$ is of the form $q+\mathbb{Z}$ for $q \in \mathbb{Q}$. Since representatives of a coset are equal let $t \in \mathbb{Z}$ so that the representative of the coset of $\mathbb{Z}$ in $\mathbb{Q}$ is $q + t$.

Then, if q is an integer let $t = -q$ so that $q + t = 0$. If q is not an integer then $q = \frac{m}{n}$ for relatively prime integers m, n (i.e., they don't have any common divisors). Let m be the integer that is either negative or positive (zero was covered in the previous case). Then if $m < 0$ let $t = \left\lceil \frac{m}{n} \right\rceil$ so that $0 \leq -\frac{m}{n} + \left\lceil \frac{m}{n} \right\rceil < 1$ and if $m > 0$ and $m > n$ then let $t = -\left\lfloor \frac{m}{n} \right\rfloor$ so that $0 \leq \frac{m}{n} - \left\lfloor \frac{m}{n} \right\rfloor < 1$. Lastly, if $m > 0$ and $m < n$ then let $t = 0$ so that $0 \leq \frac{m}{n} + 0 < 1$.

Therefore, every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$. □

(b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

Proof. From the proof of part (a) we know that there exists a representative, say q, of each coset that is in the range $0 \leq q < 1$. Thus, for $q = m/n$ we see that $n(q) = n(m/n) = m \in \mathbb{Z}$. Therefore, the order of $q + \mathbb{Z}$ is finite. Additionally, we can also see from this that there are elements of arbitrarily large order since this is dependent on n. □

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).

Proof. From the proof of part (b) we know that all elements of $\mathbb{Q}/\mathbb{Z}$ have finite order. To show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ we must show that these are the only elements of finite order.

Assume that, the elements of $\mathbb{R}/\mathbb{Z}$ are also of finite order. Thus, for $r \in \mathbb{R}$ and $t \in \mathbb{Z}$ we have that a representative of a coset in $\mathbb{R}/\mathbb{Z}$ is $r + t$. For this to be of finite order we must have that $n(r + t) \in \mathbb{Z}$.

However, if we choose r to be an irrational number then $n(r+t) \notin \mathbb{Z}$, which is a contradiction. Therefore, the order must be infinite. Thus, $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$. □

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

Proof. We will show that the map $\varphi : \mathbb{Q}/\mathbb{Z} \to U$ where $U = \{z \in \mathbb{C} \mid z^n = 1, n \in \mathbb{Z}^+\}$ and $\varphi(q+\mathbb{Z}) = \mathrm{e}^{2\pi i q}$ is an isomorphism.

homomorphism -

$$\begin{aligned}\varphi((q_1+\mathbb{Z})+(q_2+\mathbb{Z})) &= \varphi(q_1+q_2+\mathbb{Z}) \\ &= \mathrm{e}^{2\pi i(q_1+q_2)} \\ &= \mathrm{e}^{2\pi i q_1 + 2\pi i q_2} \\ &= \mathrm{e}^{2\pi i q_1}\,\mathrm{e}^{2\pi i q_2} \\ &= \varphi(q_1+\mathbb{Z})\varphi(q_2+\mathbb{Z})\end{aligned}$$

which shows this is a homomorphism as addition is the group operation for $\mathbb{Q}/\mathbb{Z}$ while multiplication is the group operation for the multiplicative group of root of unity in $\mathbb{C}^\times$.

injective -

$$\begin{aligned}\varphi(q_1+\mathbb{Z}) &= \varphi(q_2+\mathbb{Z}) \\ \mathrm{e}^{2\pi i q_1} &= \mathrm{e}^{2\pi i q_2} \\ \log(\mathrm{e}^{2\pi i q_1}) &= \log(\mathrm{e}^{2\pi i q_2}) \\ 2\pi i q_1 &= 2\pi i q_2 \\ q_1 &= q_2\end{aligned}$$

which implies $q_1+\mathbb{Z} = q_2+\mathbb{Z}$ and therefore φ is injective.

surjective - From φ it is easy to see that for some $\mathrm{e}^{2\pi i q}$ that we have some coset $q+\mathbb{Z}$ and therefore φ is surjective.

Therefore, $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$. □

15. Prove that the quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible (cf. Exercise 19, Section 2.4).

Proof. Let $(G,+)$ be a divisible abelian group and N a proper subgroup of G. If G is divisible then $ng = a$ for $g, a \in G$ and $n \in \mathbb{Z}^+$. Since G is abelian any subgroup is normal and therefore G/N is the quotient group with elements $\overline{g} = g+N$. Thus, $n\overline{g} = n(g+N) = ng+N = a+N$ [$nN = N$ for any group]. Therefore, G/N is divisible showing that every quotient of a divisible group is divisible.

Exercise 19, Section 2.4 showed that the abelian additive group $\mathbb{Q}$ is divisible and therefore the quotient $\mathbb{Q}/\mathbb{Z}$ must be divisible. □

16. Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that if $G = \langle x, y\rangle$ then $\overline{G} = \langle \overline{x}, \overline{y}\rangle$. Prove more generally that if $G = \langle S\rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S}\rangle$.

Proof. If $G = \langle x, y\rangle$ then

$$\begin{aligned} G/N &= \langle x, y\rangle/N \\ &= \{x^\alpha y^\beta N \mid \alpha, \beta \in \mathbb{Z}\} \\ &= \{x^\alpha N y^\beta N \mid \alpha, \beta \in \mathbb{Z}\} && \text{[well-defined since } N \text{ is normal]} \\ &= \{(xN)^\alpha (yN)^\beta \mid \alpha, \beta \in \mathbb{Z}\} \\ &= \langle xN, yN\rangle/N \\ &= \langle \overline{x}, \overline{y}\rangle/N \end{aligned}$$

so that $\overline{G} = \langle \overline{x}, \overline{y}\rangle$.

More generally, if $G = \langle S\rangle$ for any subset S then

$$\begin{aligned} G/N &= \langle S\rangle/N \\ &= \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} N \mid s_i \in S, \epsilon_i = \pm 1\} \\ &= \{s_1^{\epsilon_1} N s_2^{\epsilon_2} N \cdots s_n^{\epsilon_n} N \mid s_i \in S, \epsilon_i = \pm 1\} && \text{[well-defined since } N \text{ is normal]} \\ &= \{(s_1 N)^{\epsilon_1} (s_2 N)^{\epsilon_2} \cdots (s_n N)^{\epsilon_n} \mid s_i \in S, \epsilon_i = \pm 1\} \\ &= \langle s_i N\rangle/N \\ &= \langle \overline{S}\rangle/N \end{aligned}$$

so that $\overline{G} = \langle \overline{S}\rangle$. □

17. Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5):

$$G = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1}\rangle$$

and let $\overline{G} = G/\langle r^4\rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

Proof. Since the order of G is 16 and $\langle r^4\rangle = \{1, r^4\}$ is of order 2 this means $\langle r^4\rangle$ will partition G into 8 disjoint sets so that the order of $\overline{G}$ is 8. □

(b) Exhibit each element of $\overline{G}$ in the form $\overline{\tau}^a \overline{\sigma}^b$, for some integers a and b.

$$\text{Since } \langle r^4\rangle = \{1, r^4\} \text{ then } \overline{G} = \{\overline{1}, \overline{r}, \overline{r^2}, \overline{r^3}, \overline{s}, \overline{sr}, \overline{sr^2}, \overline{sr^3}\}$$

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

$$|1| = 1, |\overline{r}| = 4, |\overline{r^2}| = 2, |\overline{r^3}| = 4, |\overline{s}| = 2, |\overline{sr}| = 4, |\overline{sr^2}| = 2, |\overline{sr^3}| = 4$$

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b as in (b):

$$\overline{rs}, \quad \overline{sr^{-2}s}, \quad \overline{s^{-1}r^{-1}sr}.$$

$$\begin{aligned} \overline{rs} &= \overline{sr^{-1}} \\ \overline{sr^{-2}s} &= \overline{rsr^{-1}s} = \overline{rrss} = \overline{r^2} \\ \overline{s^{-1}r^{-1}sr} &= \overline{rssr} = \overline{r^2} && \text{[since } s = s^{-1}\text{]} \end{aligned}$$

(e) Prove that $\overline{H} = \langle \overline{s}, \overline{r^2} \rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.

Proof. From Lagrange's Theorem we know that since $\overline{G}$ is finite that $\overline{H}$ must divide its order, which it obviously does since $\langle \overline{s}, \overline{r^2} \rangle = \{\overline{1}, \overline{s}, \overline{r^2}, \overline{sr^2}\}$ which is of order 4 and $4 \mid 8$. Furthermore, we know that

$$\overline{H} \leq \mathrm{N}_{\overline{G}}(\overline{H}) \leq \overline{G}$$

and for $\overline{H}$ to be a normal subgroup of $\overline{G}$ we must have that $\mathrm{N}_{\overline{G}}(\overline{H}) = \overline{G}$. To verify that $\mathrm{N}_{\overline{G}}(\overline{H}) = \overline{G}$ we can find an element not in $\overline{H}$ that normalizes $\overline{H}$ which would show that $\mathrm{N}_{\overline{G}}(\overline{H})$ must have order 8 by Lagrange's Theorem.

$$\begin{aligned} \overline{r1r^{-1}} &= \overline{1} \in \overline{H} \\ \overline{rsr^{-1}} &= \overline{sr^{-2}} = \overline{sr^2} \in \overline{H} \\ \overline{rr^2r^{-1}} &= \overline{r^2} \in \overline{H} \\ \overline{rsr^2r^{-1}} &= \overline{sr^{-2}} = \overline{sr^2} \in \overline{H} \end{aligned}$$

Since $\overline{r}$ normalizes $\overline{H}$ and $\overline{r} \notin \overline{H}$, we see that $\overline{r} \in \mathrm{N}_{\overline{G}}(\overline{H})$ so therefore the order must be 8 showing us that $\overline{H} \trianglelefteq \overline{G}$.

From the classification of groups of order 4 we know that this group is either isomorphic to V_4 or Z_4. To show that $\overline{H}$ is isomorphic to V_4 we can show that each element has at most order 2 (i.e., no element of order 4).

$$\begin{aligned} |\overline{1}| &= 1 \\ |\overline{s}| &= 2 \\ |\overline{r^2}| &= 2 \qquad\qquad [\text{since } |\overline{r}| = 4] \\ |\overline{sr^2}| &= 2 \end{aligned}$$

Therefore, $\overline{H} \cong V_4$. The complete preimage of $\overline{H}$ in G is $\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ which is isomorphic to D_8. □

(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/\operatorname{Z}\overline{G})$

Proof. The center of $\overline{G}$ is $\langle \overline{r^2} \rangle = \{\overline{1}, \overline{r^2}\}$. The elements of $\overline{G}/\operatorname{Z}\overline{G})$ are $\{\overline{\overline{1}}, \overline{\overline{r}}, \overline{\overline{s}}, \overline{\overline{sr}}\}$ and by the classification of groups or order 4 we know that this group is isomorphic to V_4 since all non-identity elements have order 2. □

18. Let G be the quasidihedral group of order 16 (whose lattice was computed in Exercise 11 of Section 2.5):

$$G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

and let $\overline{G} = G/\langle \sigma^4 \rangle$ be the quotient of G by the subgroup generated by σ^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

Proof. Since the order of G is 16 and $\langle \sigma^4 \rangle = \{1, \sigma^4\}$ is of order 2 this means $\langle \sigma^4 \rangle$ will partition G into 8 disjoint sets so that the order of $\overline{G}$ is 8. □

(b) Exhibit each element of $\overline{G}$ in the form $\overline{\tau}^a\overline{\sigma}^b$, for some integers a and b.

$$\text{Since } \langle\sigma^4\rangle = \{1, \sigma^4\} \text{ then } \overline{G} = \{\overline{1}, \overline{\sigma}, \overline{\sigma^2}, \overline{\sigma^3}, \overline{\tau}, \overline{\tau\sigma}, \overline{\tau\sigma^2}, \overline{\tau\sigma^3}\}$$

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

$$|1| = 1, |\overline{\sigma}| = 4, |\overline{\sigma^2}| = 2, |\overline{\sigma^3}| = 4, |\overline{\tau}| = 2, |\overline{\tau\sigma}| = 4, |\overline{\tau\sigma^2}| = 2, |\overline{\tau\sigma^3}| = 4$$

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{\tau}^a\overline{\sigma}^b$, for some integers a and b as in (b):

$$\overline{\sigma\tau}, \quad \overline{\tau\sigma^{-2}\tau}, \quad \overline{\tau^{-1}\sigma^{-1}\tau\sigma}$$

$$\begin{aligned}
\overline{\sigma\tau} &= \overline{\tau\sigma^3} \\
\overline{\tau\sigma^{-2}\tau} &= \overline{\tau\sigma^2\tau} = \overline{\tau\sigma\tau\sigma^3} = \overline{\tau\tau\sigma^2} = \overline{\sigma^2} \\
\overline{\tau^{-1}\sigma^{-1}\tau\sigma} &= \overline{(\sigma\tau)^{-1}\tau\sigma} = \overline{(\tau\sigma^3)^{-1}\tau\sigma} = \overline{\sigma^{-3}\tau^{-1}\tau\sigma} = \overline{\sigma^{-2}} = \overline{\sigma^2}
\end{aligned}$$

(e) Prove that $\overline{G} \cong D_8$.

Proof. Let $\varphi : \overline{G} \to D_8$ such that $\varphi(\overline{\tau^a\sigma^b}) = s^a r^b$. This map is obviously bijective since $\overline{G} = \{\overline{1}, \overline{\sigma}, \overline{\sigma^2}, \overline{\sigma^3}, \overline{\tau}, \overline{\tau\sigma}, \overline{\tau\sigma^2}, \overline{\tau\sigma^3}\}$ and $\varphi(\overline{G}) = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

This is also a homomorphism since in $\overline{G}$ the relation $\overline{\sigma\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^{-1}}$ and therefore the multiplicative operation will be preserved between $rs = sr^{-1}$. □

19. Let G be the modular group of order 16 (whose lattice was computed in Exercise 14 of Section 2.5):

$$G = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5\rangle$$

and let $\overline{G} = G/\langle v^4\rangle$ be the quotient of G by the subgroup generated by v^4 (this subgroup is contained in the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

Proof. Since the order of G is 16 and $\langle v^4\rangle = \{1, v^4\}$ is of order 2 this means $\langle v^4\rangle$ will partition G into 8 disjoint sets so that the order of $\overline{G}$ is 8. □

(b) Exhibit each element of $\overline{G}$ in the form $\overline{u}^a\overline{v}^b$, for some integers a and b.

$$\text{Since } \langle v^4\rangle = \{1, v^4\} \text{ then } \overline{G} = \{\overline{1}, \overline{v}, \overline{v^2}, \overline{v^3}, \overline{u}, \overline{uv}, \overline{uv^2}, \overline{uv^3}\}$$

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

$$|1| = 1, |\overline{v}| = 4, |\overline{v^2}| = 2, |\overline{v^3}| = 4, |\overline{u}| = 2, |\overline{uv}| = 4, |\overline{uv^2}| = 2, |\overline{uv^3}| = 4$$

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{u}^a\overline{v}^b$, for some integers a and b as in (b):

$$\overline{vu}, \quad \overline{uv^{-2}u}, \quad \overline{u^{-1}v^{-1}uv}$$

$$\begin{aligned}
\overline{vu} &= \overline{uv} \\
\overline{uv^{-2}u} &= \overline{uv^2u} = \overline{uvuv} = \overline{uuv^2} = \overline{v^2} \\
\overline{u^{-1}v^{-1}uv} &= \overline{(vu)^{-1}uv} = \overline{(uv)^{-1}uv} = \overline{1}
\end{aligned}$$

(e) Prove that $\overline{G}$ is abelian and is isomorphic to $Z_2 \times Z_4$.

Proof. We already saw above that $\overline{uv} = \overline{vu}$ and therefore $\overline{G}$ is abelian.

Let $\varphi : \overline{G} \to Z_2 \times Z_4$ such that $\varphi(\overline{u^a v^b}) = (\overline{u^a}, \overline{v^b})$. Since $\overline{u^2} = \overline{1} \implies \langle \overline{u} \rangle$ and $\overline{v^4} = \overline{1} \implies \langle \overline{v} \rangle$ with orders 2 and 4 respectively. Therefore, since any two cyclic groups of the same order are isomorphic we see that φ is an isomorphic map so that $\overline{G} \cong Z_2 \times Z_4$. □

20. Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\widetilde{G} = G/\langle \overline{12} \rangle$, where for each integer a we simplify notation by writing $\tilde{\bar{a}}$ as $\tilde{a}$.

(a) Show that $\widetilde{G} = \{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{11}\}$.

Proof. Since the order of G is 24 and $\langle \overline{12} \rangle = \{\overline{0}, \overline{12}\}$ is of order 2 this means $\langle \overline{12} \rangle$ will partition G into 12 disjoint sets so that the order of $\overline{G}$ is 12. Therefore, $\widetilde{G} = \{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{11}\}$. □

(b) Find the order of each element of $\widetilde{G}$.

$$|\widetilde{0}| = 1, |\widetilde{1}| = 12, |\widetilde{2}| = 6, |\widetilde{3}| = 4, |\widetilde{5}| = 12, |\widetilde{6}| = 2, |\widetilde{7}| = 12, |\widetilde{8}| = 3, |\widetilde{9}| = 4, |\widetilde{10}| = 6, |\widetilde{11}| = 12$$

(c) Prove that $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. (Thus $(\mathbb{Z}/24\mathbb{Z})/(12\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, just as if we inverted and canceled the $24\mathbb{Z}$s.)

Proof. Let $\varphi : \widetilde{G} \to \mathbb{Z}/12\mathbb{Z}$ such that $\varphi(\widetilde{a}) = \overline{a}$. Obviously this is a bijective map and it is also a homomorphism as both $\widetilde{G}$ and $\mathbb{Z}/12\mathbb{Z}$ are both modulo 12 so that the group operation holds in both. Therefore, $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. □

21. Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx \rangle$$

Let $\overline{G} = G/\langle x^2 y^2 \rangle$ (note that every subgroup of the abelian group G is normal).

(a) Show that the order of $\overline{G}$ is 8.

Proof. Since the order of G is 16 and $\langle x^2 y^2 \rangle = \{1, x^2 y^2\}$ is of order 2 this means $\langle x^2 y^2 \rangle$ will partition G into 8 disjoint sets so that the order of $\overline{G}$ is 8. □

(b) Exhibit each element of $\overline{G}$ in the form $\overline{x}^a \overline{y}^b$, for some integers a and b.

$$\text{Since } \langle x^2 y^2 \rangle = \{1, x^2 y^2\} \text{ then } \overline{G} = \{\overline{1}, \overline{x}, \overline{x^2 = y^2}, \overline{x^3}, \overline{y}, \overline{y^3}, \overline{xy}, \overline{x^3 y = xy^3}\}$$

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

$$|1| = 1, |\overline{x}| = 4, |\overline{x^2 = y^2}| = 2, |\overline{x^3}| = 4, |\overline{y}| = 4, |\overline{y^3}| = 4, |\overline{xy}| = 2, |\overline{x^3 y = xy^3}| = 2$$

(d) Prove that $\overline{G} \cong Z_4 \times Z_2$.

Proof. Let $\varphi : \overline{G} \to Z_4 \times Z_2$ such that $\varphi(\overline{x^a y^b}) = \varphi(\overline{x^{a-b}(xy)^b}) = (x^{a-b}, (xy)^b)$. Note that $\overline{xy}$ has order 2 and therefore φ will map this information over into Z_2. A similar argument follows for $\overline{x^{a-b}}$ and Z_4.

Now, let's show that this map is actually an isomorphism.

injective -

$$\begin{aligned}\varphi(\overline{x^a y^b}) &= \varphi(\overline{x^c y^d}) \\ \varphi(\overline{x^{a-b}(xy)^b}) &= \varphi(\overline{x^{c-d}(xy)^d}) \\ (x^{a-b}, (xy)^b) &= (x^{c-d}, (xy)^d) \\ \implies a-b &= c-d,\ b=d \\ \implies a &= c,\ b=d\end{aligned}$$

which shows that it is 1-1.

surjective -

$$\varphi(\overline{x^a y^b}) = \varphi(\overline{x^{a-b}(xy)^b}) = (x^{a-b}, (xy)^b)$$

which shows that it is onto.

homomorphism -

$$\begin{aligned}\varphi(\overline{x^a y^b x^c y^d}) &= \varphi(\overline{x^{a+c} y^{b+d}}) \\ &= \varphi(\overline{x^{(a+c)-(b+d)}(xy)^{b+d}}) \\ &= (x^{(a+c)-(b+d)}, (xy)^{b+d}) \\ &= (x^{a-b}x^{c-d}, (xy)^b(xy)^d) \\ &= (x^{a-b}, (xy)^b)(x^{c-d}, (xy)^d) \\ &= \varphi(\overline{x^{a-b}(xy)^b})\varphi(\overline{x^{c-d}(xy)^d}) \\ &= \varphi(\overline{x^a y^b})\varphi(\overline{x^c y^d})\end{aligned}$$

showing that φ is a homomorphism.

Therefore, $\overline{G} \cong Z_4 \times Z_2$. □

22. (a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Proof. If $H \trianglelefteq G$ and $K \trianglelefteq G$ then $gHg^{-1} = H$ and $gKg^{-1} = K$ for all $g \in G$. Therefore, for all $x \in H$ there exists $y \in H$ such that $gxg^{-1} = y$ and similarly the same argument holds for K. Thus, for all $x \in H \cap K$ there exists $y \in H \cap K$ such that $gxg^{-1} = y$ for all $g \in G$. Therefore, $g(H \cap K)g^{-1} = H \cap K$ for all $g \in G$ so that $H \cap K \trianglelefteq G$. □

(b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Proof. If we have an arbitrary nonempty collection of normal subgroups of a group then with the same argument used in the proof of part (a) we see that their intersection is also a normal subgroup. □

23. Prove that the join (cf. Section 2.5) of any nonempty collection of normal subgroups of a group is a normal subgroup.

Proof. Let $\{H_i \mid i \in I\}$ be a collection of normal subgroups of G and $J = \langle \bigcup_{i\in I} H_i \rangle$. We need to show that J is a normal subgroup of G.

An element of J will be of the form $h_1^{\epsilon_1} h_2^{\epsilon_2} \cdots h_n^{\epsilon_n}$ with $\epsilon_k = \pm 1$ and $h_j \in H_i$ for some $i \in I$ for all $1 \leq j \leq n$. Then, $g(h_1^{\epsilon_1} h_2^{\epsilon_2} \cdots h_n^{\epsilon_n})g^{-1} = (gh_1^{\epsilon_1}g^{-1})(gh_2^{\epsilon_2}g^{-1}) \cdots (gh_n^{\epsilon_n}g^{-1})$ for all $g \in G$ and since each $(gh_j^{\epsilon_k}g^{-1}) \in H_i$ for some $i \in I$ we see that $g(h_1^{\epsilon_1} h_2^{\epsilon_2} \cdots h_n^{\epsilon_n})g^{-1} \in J$. Thus, $J \trianglelefteq G$. □

24. Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Proof. Since H is a group we obviously have that $hHh^{-1} = H$ and since $N \trianglelefteq G$ and $H \leq G$ we also have that $hNh^{-1} = N$. Therefore, we must have that $h(N \cap H)h^{-1} = N \cap H$ which implies that $N \cap H \trianglelefteq H$. □

25. (a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for *all* $g \in G$.

Proof. If $N \trianglelefteq G$ then by definition $gNg^{-1} = N$ for all $g \in G$ and therefore we obviously have that $gNg^{-1} \subseteq N$. Conversely, if $gNg^{-1} \subseteq N$ for all $g \in G$ then

$$\begin{aligned} gNg^{-1} &\subseteq N \\ g^{-1}gNg^{-1}g &\subseteq g^{-1}Ng \\ N &\subseteq g^{-1}Ng \end{aligned}$$

but since this was for all $g \in G$ this is also true if we set $g = x^{-1}, x \in G$ since g will be the inverse of some other element in the group. Then

$$\begin{aligned} N &\subseteq g^{-1}Ng \\ N &\subseteq (x^{-1})^{-1}Nx^{-1} \\ N &\subseteq xNx^{-1} \end{aligned}$$

and therefore, $gNg^{-1} = N$ which shows that $N \trianglelefteq G$. □

(b) Let $G = GL_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries 2,1. Show that $gNg^{-1} \subseteq N$ but g does *not* normalize N.

Proof. $N = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}\}$, $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \implies g^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$ so that we have

$$\begin{aligned} gNg^{-1} &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & a \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2a \\ 0 & 1 \end{pmatrix} \in N \implies \\ gNg^{-1} &\subseteq N \end{aligned}$$

This shows that g does not normalize N because $\begin{pmatrix} 1 & 2a \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. □

26. Let $a, b \in G$.

(a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conjugate of b. Prove that the order of a and the order of any conjugate of a are the same.

Proof. The conjugate of the product of a and b is

$$g(ab)g^{-1} = ga(g^{-1}g)bg^{-1} = (gag^{-1})(gbg^{-1})$$

which is the product of the conjugate of a and the conjugate of b.

Suppose the order of a is n. Then $a^n = 1$ and

$$\begin{aligned} 1 &= gg^{-1} \\ &= ga^n g^{-1} \\ &= (gag^{-1})_1(gag^{-1})_2 \cdots (gag^{-1})_n \\ &= (gag^{-1})^n \end{aligned}$$

showing that the order of a and any conjugate of a are the same. □

(b) Prove that the conjugate of a^{-1} is the inverse of the conjugate of a.

Proof. $ga^{-1}g^{-1} = (g^{-1})^{-1}a^{-1}g^{-1} = (gag^{-1})^{-1}$ □

(c) Let $N = \langle S \rangle$ for some subset S of G. Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.

Proof. If $gSg^{-1} \subseteq N$ then for all $g \in G, s \in S$ we have that $gsg^{-1} \in N$. Since N is a group we also have that $(gsg^{-1})(gs^{-1}g^{-1}) = 1 \in N \implies (gs^{-1}g^{-1}) \in N$ for all $s \in S$. Then, since $N = \langle S \rangle$ we see that $n \in N \implies n = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ for $s_i \in S, \epsilon_i = \pm 1$.

Therefore, $gng^{-1} = gs_1^{\epsilon_1} \cdots s_n^{\epsilon_n} g^{-1} = (gs_1^{\epsilon_1} g^{-1}) \cdots (gs_n^{\epsilon_n} g^{-1}) \in N$ which shows that $gNg^{-1} \subseteq N$ so that $N \trianglelefteq G$. □

(d) Deduce that if N is the cyclic group $\langle x \rangle$, then N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

Proof. N is the cyclic group $\langle x \rangle$.

If $N \trianglelefteq G$ then for all $g \in G, x \in N$ we have that $gxg^{-1} \in N \implies gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

Conversely, if $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$, then $gxg^{-1} \in N$ for all $x \in N, g \in G \implies N \trianglelefteq G$.

Therefore, N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$. □

(e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G.

Proof. Let $N = \{x \in G \mid x^n = 1\}$ and therefore for all $g \in G, x \in N$ we have that

$$\begin{aligned} 1 &= gg^{-1} \\ &= gx^n g^{-1} \\ &= (gxg^{-1})_1 (gxg^{-1})_2 \cdots (gxg^{-1})_n \\ &= (gxg^{-1})^n \end{aligned}$$

showing that $gxg^{-1} \in N \implies N \trianglelefteq G$. □

27. Let N be a *finite* subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $\mathrm{N}_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Proof. From the proof of Exercise 25 we saw that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for *all* $g \in G$, and therefore $gNg^{-1} = N$ if and only if $gNg^{-1} \subseteq N$ for all $g \in G$. However, because *finite* was emphasized we will also show a proof that uses the size of N to verify the hypothesis.

Obviously, if $gNg^{-1} = N$ then $gNg^{-1} \subseteq N$. Conversely, if $gNg^{-1} \subseteq N$ then let $\varphi(x) = gxg^{-1}$ for $x \in N,\ g \in G$. Then, we see that φ maps N into N. Therefore

$$\begin{aligned} \varphi(x_1) &= \varphi(x_2) \\ gx_1g^{-1} &= gx_2g^{-1} \\ \implies x_1 &= x_2 \end{aligned}$$

This shows that φ is injective and therefore the image has the same amount of elements as the domain, i.e., $|N| = |gNg^{-1}|$. Since we assumed that $gNg^{-1} \subseteq N$, then if gNg^{-1} has the same amount of elements as N then they must be equal. Therefore, $gNg^{-1} = N$. □

Additionally, since the definition of the normalizer of A in G is the set $\mathrm{N}_G(A) = \{g \in G \mid gAg^{-1} = A\}$ [section 2.2] and we see that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$ then we can substitute this in the definition to deduce that

$$\mathrm{N}_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$$

28. Let N be a *finite* subgroup of a group G and assume $N = \langle S \rangle$ for some subset S of G. Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.

Proof. If an element $g \in G$ normalizes N then by definition we have

$$\begin{aligned} & gNg^{-1} = N \\ \implies & gNg^{-1} \subseteq N \\ \implies & g(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n})g^{-1} \in N && [s_i \in S, \epsilon_i = \pm 1] \\ \implies & (gs_1^{\epsilon_1} g^{-1})(gs_2^{\epsilon_2} g^{-1}) \cdots (gs_n^{\epsilon_n} g^{-1}) \in N && [s_i \in S, \epsilon_i = \pm 1] \\ \implies & gsg^{-1} \in N && [s \in S] \\ \implies & gSg^{-1} \subseteq N \end{aligned}$$

Conversely, if $gSg^{-1} \subseteq N$ for some $g \in G$ then we have that

$$\begin{aligned} & gsg^{-1} \in N && [s \in S] \\ \implies & (gs_1^{\epsilon_1} g^{-1})(gs_2^{\epsilon_2} g^{-1}) \cdots (gs_n^{\epsilon_n} g^{-1}) \in N && [s_i \in S, \epsilon_i = \pm 1] \\ \implies & g(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n})g^{-1} \in N && [s_i \in S, \epsilon_i = \pm 1] \end{aligned}$$

$$\implies gNg^{-1} \subseteq N$$
$$\implies gNg^{-1} = N \qquad \text{[proof of Exercise 27]}$$

Therefore, an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$. □

29. Let N be a *finite* subgroup of a group G and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subset S and T of G. Prove that N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.

Proof. If $N \trianglelefteq G$ then from the proof of Exercise 28, since this exercise also had $N = \langle S \rangle$ for a subset S of G, we know that $gSg^{-1} \subseteq N$. Then, since $g \in G \implies g \in \langle T \rangle \implies$ there exists $g \in T$ so that

$$gSg^{-1} \subseteq N \implies tSt^{-1} \subseteq N \text{ for all } t \in T$$

Conversely, if $tSt^{-1} \subseteq N$ for all $t \in T$ then

$$tSt^{-1} \subseteq N$$
$$\implies tst^{-1} \in N \qquad [s \in S]$$

Therefore, N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$. □

30. Let $N \leq G$ and $g \in G$. Prove that $gN = Ng$ if and only if $g \in \mathrm{N}_G(N)$.

Proof. If $gN = Ng$ then $gNg^{-1} = N$ and therefore g normalizes N so that $g \in \mathrm{N}_G(N)$. Conversely, if $g \in \mathrm{N}_G(N)$ then g normalizes N so that we have $gNg^{-1} = N$ and therefore $gN = Ng$.

Therefore, $gN = Ng$ if and only if $g \in \mathrm{N}_G(N)$. □

31. Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq \mathrm{N}_G(N)$. Deduce that $\mathrm{N}_G(N)$ is the largest subgroup of G in which N is normal (i.e., is the join of all subgroups H for which $N \trianglelefteq H$).

Proof. $N \trianglelefteq H \implies hNh^{-1} = N$ for all $h \in H$. Thus, $h \in \mathrm{N}_G(N)$ therefore $H \leq \mathrm{N}_G(N)$. □

Since $N \trianglelefteq H \leq \mathrm{N}_G(N) \leq G$ we deduce that the largest subgroup H of G where N is normal is $\mathrm{N}_G(N)$.

32. Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient. [You may use the lattice subgroups for Q_8 in Section 2.5.]

Proof. The non-trivial subgroups of Q_8 are $\langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$. $\langle -1 \rangle$ commutes with all elements of Q_8 so it is obviously normal. For the others

$$ji(-j) = -i \in \langle i \rangle$$
$$ki(-k) = -i \in \langle i \rangle$$
$$ij(-i) = -j \in \langle j \rangle$$
$$kj(-k) = -j \in \langle j \rangle$$
$$ik(-i) = -k \in \langle k \rangle$$
$$jk(-j) = -k \in \langle k \rangle$$

showing that $\langle i \rangle, \langle j \rangle, \langle k \rangle, \langle -1 \rangle$ are normal subgroups.

Therefore, all the subgroups of Q_8 are normal. $\square$

$Q_8/1 \cong Q_8$ and $Q_8/Q_8 \cong 1$

$Q_8/\langle -1\rangle = \{\overline{1}, \overline{i}, \overline{j}, \overline{k}\}$ where each element has order two (remember that the identity element of this quotient group is the kernel). From the classification of groups of order 4 we know that this group is either isomorphic to V_4 or Z_4 and since every non-identity element has order 2, we know it must be isomorphic to V_4. Therefore, $Q_8/\langle -1\rangle \cong V_4$.

$Q_8/\langle i\rangle = \{\overline{1}, \overline{j}\}$ and therefore, since this is a group of order 2 it must be isomorphic to Z_2 since all groups have the identity element and the other element multiplied by itself must be closed under the group operation, i.e., $\langle \overline{j}\rangle = Q_8/\langle i\rangle \cong Z_2$. A similar argument holds for $Q_8/\langle j\rangle$ and $Q_8/\langle k\rangle$.

33. Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for D_8 in Section 2.5.]

The non-trivial subgroups of D_8 are $\langle s, r^2\rangle, \langle r\rangle, \langle rs, r^2\rangle, \langle s\rangle, \langle r^2 s\rangle, \langle r^2\rangle, \langle rs\rangle, \langle r^3 s\rangle$.

$\langle s\rangle$ and $\langle r\rangle$ cannot be normal as they do not commute with one another.

Nor are the subgroups $\langle rs\rangle \to s(rs)s^{-1} = sr \notin \langle rs\rangle$, $\langle r^2 s\rangle \to s(r^2 s)s^{-1} = sr^2 \notin \langle r^2 s\rangle$, $\langle r^3 s\rangle \to s(r^3 s)s^{-1} = sr^3 \notin \langle r^3 s\rangle$.

The center of $D_8, \langle r^2\rangle$ is obviously normal and the quotient of this is isomorphic to V_4.

Additionally, the subgroups of order 4 are all normal, $\langle s, r^2\rangle, \langle r\rangle, \langle sr, r^2\rangle$, and the quotient of these are all isomorphic to Z_2.

34. Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$ be the usual presentation of the dihedral group of order $2n$ and let k be a positive integer dividing n.

(a) Prove that $\langle r^k\rangle$ is a normal subgroup of D_{2n}.

Proof. From Exercise 33 we know that $\langle r\rangle$ is a cyclic normal subgroup of D_{2n} with order n. Since $k \mid n$ we know that by Lagrange's Theorem that $\langle r^k\rangle$ is a subgroup of $\langle r\rangle$. Additionally, we know that since

$$\langle r^k\rangle \leq \langle r\rangle \trianglelefteq D_{2n} \implies \mathrm{N}_{D_{2n}}(\langle r\rangle) = D_{2n}$$

and therefore, since all of D_{2n} normalizes $\langle r\rangle$ it must also normalize the elements of $\langle r^k\rangle$.

Thus, $\langle r^k\rangle \trianglelefteq D_{2n}$. $\square$

(b) Prove that $D_{2n}/\langle r^k\rangle \cong D_{2k}$.

Proof. Since $\langle r^k\rangle$ is a normal subgroup and $k \mid n$ let $d = n/k$ so that $\langle r^k\rangle$ has order d and therefore by Lagrange's Theorem $|D_{2n}/\langle r^k\rangle| = 2k$, i.e., there will be $2k$ cosets. The cosets will be $\{\overline{1}, \overline{r}, \overline{r^2}, \ldots, \overline{r^{k-1}}, \overline{s}, \overline{sr}, \ldots, \overline{sr^{k-1}}\}$ and therefore $D_{2n}/\langle r^k\rangle \cong D_{2k}$. $\square$

35. Prove that $SL_n(F) \trianglelefteq GL_n(F)$ and describe the isomorphism type of the quotient group (cf. Exercise 9, Section 2.1).

Proof. For determinants we have the property that

$$\det(ABC) = \det(A)\det(B)\det(C) \text{ and } \det(A^{-1}) = \frac{1}{\det(A)}$$

and therefore we see that for any $g \in GL_n(F)$ and $s \in SL_n(F)$ that

$$\det(gsg^{-1}) = \det(g)\det(s)\det(g^{-1}) = \det(g) \cdot 1 \cdot \det(g^{-1}) = \det(g)\frac{1}{\det(g)} = 1$$

so that resulting matrix has determinant 1 and thus is in $SL_n(F)$. Therefore, $SL_n(F) \trianglelefteq GL_n(F)$.

The isomorphism type of the quotient group can be seen from the looking at the map $\det(GL_n(F)) \mapsto F^\times$. This is a group homomorphism from the argument of the proof above since the determinant of a product is the product of the determinants. Additionally, the kernel of this homomorphism is $SL_n(F)$ as the identity element in $F^\times$ is 1. Then, as we saw in the text, since the multiplication of fibers is defined from the multiplication in $F^\times$, by construction the quotient group with this multiplication is naturally isomorphic to the image of $GL_n(F)$ under this homomorphism. Therefore, $GL_n(F)/SL_n(F) \cong F^\times$. □

36. Prove that if $G/\operatorname{Z}(G)$ is cyclic then G is abelian. [If $G/\operatorname{Z}(G)$ is cyclic with generator $x\operatorname{Z}(G)$, show that every element of G can be written in the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in \operatorname{Z}(G)$.]

Proof. If $G/\operatorname{Z}(G)$ is cyclic with generator $x\operatorname{Z}(G)$ the elements of $G/\operatorname{Z}(G)$ are $(x\operatorname{Z}(G))^a = x^a\operatorname{Z}(G) \implies \{x^a\operatorname{Z}(G) \mid a \in \mathbb{Z}\}$. Since this quotient will partition all of G we see that each element of G must be of the form $x^a z$ for some $z \in \operatorname{Z}(G)$. Since the elements of $\operatorname{Z}(G)$ commute will all elements of G we see that G must be abelian. □

37. Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Proof. Let $G = A \times B$ and $N = \{(a, 1) \mid a \in A\}$.

For all $(a, b) \in G$ and $(a, 1) \in N$

$$\begin{aligned}(a, b)(a, 1)(a, b)^{-1} &= (a, b)(a, 1)(a^{-1}, b^{-1}) \\ &= (a, b)(1, b^{-1}) \\ &= (a, 1) \in N\end{aligned}$$

which shows that all (a, b) normalizes all $(a, 1)$ therefore $N \trianglelefteq G$.

G/N has elements

$$\overline{(a, b)} = (a, b)N$$

However, $\overline{(a, b)} = \overline{(1, b)}$ since $(a, b) \in (1, b)N$. Therefore, every coset uniquely corresponds to an element of B via the map

$$\overline{(a, b)} \longleftrightarrow b$$

and since the multiplication is the same in B, we see that $G/N \cong B$. □

38. Let A be an abelian group and let D be the (diagonal) subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

Proof. Since A is an abelian group so too is $A \times A$ and every subgroup of an abelian group is normal because for all $a \in A$ and $n \in N \leq A$ we see that

$$ana^{-1} = aa^{-1}n = n \in N$$

Therefore, since D is a subgroup of $A \times A$ it must be a normal subgroup of $A \times A$.

The quotient group $(A \times A)/D$ has elements of the from

$$(a_1, a_2)D$$

and since representatives are equal we can see that for $(a_2^{-1}, a_2^{-1}) \in D$

$$(a_1, a_2)D = (a_1, a_2)(a_2^{-1}, a_2^{-1})D = (a_3, 1)D$$

for some $a_3 \in A$. This representation is unique as it relies on the inverse of a_2, which is unique. This shows that each coset corresponds uniquely to an element of A.

Let $\varphi : (A \times A)/D \to A$ such that $(a,1)D \xrightarrow{\varphi} z$. This is well-defined, since the representation is unique, and it is obviously a bijection. Now we need to check that it is a homomorphism.

$$\begin{aligned} \varphi((a_1,1)(a_2,1)) &= \varphi((a_1a_2,1)) \\ &= a_1a_2 \\ &= \varphi((a_1,1))\varphi((a_2,1)) \end{aligned}$$

Therefore, φ is an isomorphism and therefore $(A \times A)/D \cong A$. □

39. Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.

Proof. Let $(a,a) \in D$ and $(a_1, a_2) \in A \times A$. Then

$$\begin{aligned} (a_1,a_2)(a,a)(a_1,a_2)^{-1} &= (a_1,a_2)(a,a)(a_1^{-1},a_2^{-1}) \\ &= (a_1aa_1^{-1}, a_2aa_2^{-1}) \notin D \end{aligned}$$

Therefore, D is not normal in $A \times A$. □

40. Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x,y]$.)

Proof. If $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ then

$$\begin{aligned} \overline{xy} &= \overline{yx} \\ xNyN &= yNxN \\ xyN &= yxN && [N \text{ normal}] \end{aligned}$$

$$(yx)^{-1}xyN = N$$
$$x^{-1}y^{-1}xyN = N$$

showing that $x^{-1}y^{-1}xy \in N$

Conversely, if $x^{-1}y^{-1}xy \in N$ then

$$\begin{aligned} N &= N \\ x^{-1}y^{-1}xyN &= N && [x^{-1}y^{-1}xy \in N] \\ (yx)^{-1}xyN &= N \\ xyN &= yxN \\ xNyN &= yNxN && [N \text{ normal}] \\ \overline{xy} &= \overline{yx} \end{aligned}$$

showing that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$.

Therefore, $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. □

41. Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator subgroup* of G).

Proof. Let $g \in G$ and $x^{-1}y^{-1}xy \in N,\ x, y \in G$. Then

$$\begin{aligned} g(x^{-1}y^{-1}xy)g^{-1} &= g(x^{-1}g^{-1}gy^{-1}g^{-1}gxg^{-1}gy)g^{-1} \\ &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &= x_o^{-1}y_o^{-1}x_oy_o \in N,\ x_o, y_o \in G \end{aligned}$$

Therefore, N is a normal subgroup of G. G/N has cosets of the form $\overline{x} = xN$ for $x \in G$. Then, since $x^{-1}y^{-1}xy \in N$ implies $(x^{-1}y^{-1}xy)N = N$. Therefore, for $x, y \in G$ we would have that

$$\begin{aligned} \overline{xy} &= xNyN \\ &= xyN \\ &= xy(x^{-1}y^{-1}xy)N \\ &= yxN \\ &= yNxN \\ &= \overline{yx} \end{aligned}$$

showing us that G/N is abelian. □

42. Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show $x^{-1}y^{-1}xy \in H \cap K$.]

Proof. For $x \in H$ and $y \in K$ we have that $yx^{-1}y^{-1} \in H$ and $xyx^{-1} \in K$. Then

$$x(yx^{-1}y^{-1}) \in H \text{ and } (xyx^{-1})y^{-1} \in K \text{ and therefore } xyx^{-1}y^{-1} \in H \cap K$$

and thus $xyx^{-1}y^{-1} = 1$ since $H \cap K = 1$ we see that $xy(yx)^{-1} = 1 \implies xy = yx$. □

43. Assume $\mathcal{P} = \{A_i \mid i \in I\}$ is any partition of G with the property that $\mathcal{P}$ is a group under the "quotient operation" defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and any element a_j of A_j and let A_iA_j be the element of $\mathcal{P}$ containing a_ia_j (this operation is assumed to be well-defined). Prove that the element of $\mathcal{P}$ that contains the identity of G is a normal subgroup of G and the elements of $\mathcal{P}$ are the cosets of this subgroup (so $\mathcal{P}$ is just a quotient group of G in the usual sense).

Proof. Let A_e be the element of $\mathcal{P}$ that contains the identity of G. Then for any $A_i \in \mathcal{P}$ we have that

$$A_iA_eA_i^{-1} = A_e \implies a_i1a_i^{-1} = 1$$

as we can take any element from A_i and A_e and therefore A_e is a normal subgroup of G.

The cosets of $\mathcal{P}/A_e$ are:

$$\overline{A_i} = A_iA_e = a_i \cdot 1 = a_i = A_i$$

Therefore, the elements of $\mathcal{P}$ are the cosets of this quotient group. □

3.2 MORE ON COSETS AND LAGRANGE'S THEOREM

Let G be a group.

1. Which of the following are permissible orders for subgroups of a group of order 120: 1,2,5,7,9,15,60,240? For each permissible order give the corresponding index.

1,2,5,15,60 and 120,60,24,8,2

2. Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).

Proof. The elements of S_3 have the cycle decompositions: 1, (1 2), (1 3), (2 3), (1 2 3), and (1 3 2). Since $|S_3| = 3! = 6$ and 6 has the factors 1,2,3,6 we see that the order of the nontrivial subgroups must be either 2 or 3. From the lattice in Section 2.5 we see that the subgroups of S_3 are $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$, where the orders are 2,2,2,3, respectively.

In Exercise 2, Section 1.5 we drew the group table for S_3 which showed that combinations (i.e., their pairwise joins and intersections) of these subgroups doesn't yield any other subgroups and that the lattice of subgroups of S_3 in Section 2.5 is correct. □

3. Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

Proof. Q_8 has order 8 and we saw earlier that all of its subgroups are normal. The subgroups $\langle i\rangle, \langle j\rangle, \langle k\rangle$ have order 4 while $\langle -1\rangle$ has order 2. Once again, looking at the group table in Exercises 2, Section 1.5 we see that these are all the subgroups and that the lattice of subgroups of Q_8 in Section 2.5 is correct. □

4. Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]

Proof. G is either abelian or it's not. If G is abelian, we are done. Therefore, let's assume that G is non-abelian. In Exercise 36, Section 1 we saw that if $G/\operatorname{Z}(G)$ is cyclic then G is abelian. Taking the contrapositive of this we see that since G is non-abelian, then $G/\operatorname{Z}(G)$ is not cyclic. We know that $G/\operatorname{Z}(G)$ is a quotient group since $\operatorname{Z}(G) \trianglelefteq G$. Let's suppose that $\operatorname{Z}(G)$ is nontrivial. Therefore, by Lagrange's Theorem $G/\operatorname{Z}(G)$ must either have order p or q. However, from Corollary 10, a group of prime order is cyclic, which is a contradiction. Therefore, $\operatorname{Z}(G)$ must be trivial. □

5. Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

Proof. Let $h \in H$ and for fixed element $g \in G$ we have that $ghg^{-1} \in gHg^{-1}$. Since H is a group it is closed under multiplication and inverses. Therefore, for $h_1, h_2 \in H$ we have that $h_1 h_2^{-1} \in H$ so that $g(h_1 h_2^{-1})g^{-1} \in gHg^{-1} \implies gh_1(gh_2)^{-1} \in gHg^{-1}$ so that gHg^{-1} is also closed under multiplication and inverses and by the subgroup criterion gHg^{-1} is a subgroup of G.

Since g is fixed, and each element of gHg^{-1} is of the form gh (where h can be the identity), we see that $|gHg^{-1}| = |H|$. □

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

Proof. It is easy to see that if $h \in H$ then h is also in gHg^{-1} so that $H \subseteq gHg^{-1}$. From the proof of part (a) we saw that the orders of H and gHg^{-1} are equal, which in this case is n, so these groups must be equal. Therefore, since $gHg^{-1} = H$ for any $g \in G$ we see that $H \trianglelefteq G$. □

6. Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals *some* left coset of H in G then it equals the left coset gH and g must be in $\operatorname{N}_G(H)$.

Proof. If Hg is equal to *some* left coset of H, say aH for $a \in G$ then

$$\begin{aligned} Hg &= aH \\ \implies \overline{g} &= \overline{a} \\ \implies g &= a \\ \implies Hg &= gH \end{aligned}$$

and therefore $H \trianglelefteq G$, which means g must be an element in $\operatorname{N}_G(H)$. □

7. Let $H \leq G$ and define a relation $\sim$ on G be $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

Proof.

$a \sim a \implies a^{-1}a = 1 \in H \implies a \sim a$ [reflexive]

$a \sim b \implies b^{-1}a \in H \implies (b^{-1}a)^{-1} = a^{-1}b \in H \implies b \sim a$ [symmetric]

$a \sim b \implies b^{-1}a \in H,\ b \sim c \implies c^{-1}b \in H \implies (c^{-1}b)(b^{-1}a) = c^{-1}a \in H \implies a \sim c$ [transitive]

Therefore, $\sim$ is an equivalence relation as it is reflexive, symmetric, and transitive. The equivalence class of each $a \in G$ is some coset aH. Using this face we see that if $b^{-1}a \in H$ then for $h = b^{-}a$ we have

$$bh = b(b^{-1}a) = a \implies a \in bH$$

and since representatives of a coset are equal we see that $aH = bH$, proving Proposition 4. □

8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Proof. By Lagrange's Theorem, if H and K are finite subgroups of G whose orders are relatively prime, we know that H and K cannot be subgroups of one another. Therefore, their intersection must be the identity so that $H \cap K = 1$. □

9. This exercise outlines a proof of Cauchy's Theorem due to James McKay. Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}$$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Proof. From $x_1 x_2 \cdots x_p = 1$ we see that x_p is dependent on the other coordinates, $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Therefore, we can restate $\mathcal{S}$ as $\{(x_1, x_2, \ldots, x_{p-1}, (x_1 x_2 \cdots x_{p-1})^{-1}) \mid x_i \in G\}$. From this we can see that $\mathcal{S}$ will have order

$$|\mathcal{S}| = |G|_1 \cdot |G|_2 \cdots |G|_{p-1} = |G|^{p-1}$$

since for each coordinate in the p-tuples, there are $|G|$ options. Obviously $|G|^{p-1}$ is divisible by p since p divides $|G|$. □

Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) Show that a cyclic permutation on an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

Proof. An element of $\mathcal{S}$ has the form $(x_1, x_2, \ldots, x_p)$ such that $x_i \in G$ and whose product of coordinates is equal to 1. Then, it is easy to to see that any cyclic permutation, say $\beta = (x_i, x_{i+1}, \ldots, x_p, x_1, \ldots, x_{i-1})$, of these coordinates is another element of $\mathcal{S}$ as we still have a p-tuple with coordinates from G whose product is equal to 1. □

(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

Proof. $\alpha \sim \alpha$ since α is the identity permutation of α [reflexive].

$\alpha \sim \beta \implies \beta \sim \alpha$ since proof from part (b) showed us that a cyclic permutation of an element of $\mathcal{S}$ is another element of $\mathcal{S}$ and therefore all the elements are permutations of one another [symmetric].

$\alpha \sim \beta$ and $\beta \sim \gamma \implies \alpha \sim \gamma$ since the composition of permutations is a permutation [transitive].

Therefore, $\sim$ is an equivalence relation. □

(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

Proof. If $(x, x, \ldots, x)$ with $x^p = 1$ then since all cyclic permutations of this element still equal this element then its equivalence class only has this one element.

Conversely, if an equivalence class only has one element then it is equal to its own permutations and therefore we must have that $(x, x, \ldots, x)$ with $x^p = 1$.

Therefore, an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$. □

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a *prime*). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p.

Proof. From the proof of part (d) we saw that there exists an equivalence class with order 1. Suppose that we do not have $(x, x, \ldots, x)$ with $x^p = 1$. Then we will have $(x_1, x_2, \ldots, x_p)$ where some or all of the x_i differ. The equivalence relation mandates that all elements of an equivalence class are *cyclic* p-cycles of each other which means we can only have cycles where every coordinate of the p-tuple is shifted by the same amount. This is a subtle distinction that is crucial to understand but is necessary if every element will be a permutation of each other. Thus, each equivalence class can only have p elements since after p iterations will we arrive back to the same element of the equivalence class.

From part (a) we saw that $|\mathcal{S}| = |G|^{p-1}$ and since $\sim$ partitions $|\mathcal{S}|$ it must partition $|G|^{p-1}$. It will partition it with k classes of order 1 and d classes of order p so that $|G|^{p-1} = k + pd$. □

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p. [Show $p \mid k$ and so $k > 1$.]

Proof. From part (a) we saw that p divides $|G|^{p-1}$. From part (e) we saw that p divides $k + pd$ which implies p divides k and therefore k must be a multiple of p, showing that $k > 1$. Hence, there must be a nonidentity element x in G with $x^p = 1$. □

10. Suppose H and K are subgroups of finite index in the (possibly infinite) group G with $|G : H| = m$ and $|G : K| = n$. Prove that $\text{lcm}(m, n) < |G : H \cap K| < mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

Proof. If we take the intersection of H and K then $H \cap K$ can partition K into cosets and the elements in these cosets will also be elements contained in the cosets of G partitioned by H. That is

$$|K : H \cap K| \leq |G : H| = m$$

where $\leq$ is for less than or equal to. Now we can multiple both sides of the inequality with $|G : K|$ to get

$$|G : K| \cdot |K : H \cap K| \leq |G : K| \cdot |G : H| = nm$$

K partitions G and $H \cap K$ partitions K so therefore $H \cap K$ partitions G and we see that $|G : H \cap K| = |G : K| \cdot |K : H \cap K|$. This shows that n divides $|G : H \cap K|$. We could have also made the same argument using H instead of K so therefore m also divides $|G : H \cap K|$. Since we know that m and n divide this, we get the desired inequality (bounded below by $\text{lcm}(m, n)$) and from this we can see that when $(m, n) = 1$ that we will have that it will be equal to mn and therefore $|G : H \cap K| = |G : H| \cdot |G : K|$. □

11. Let $H \leq K \leq G$. Prove that $|G \,:\, H| = |G \,:\, K| \cdot |K \,:\, H|$. (do not assume G is finite).

Proof. Let $|G \,:\, K| = p$, $|K \,:\, H| = q$ and then

$$G = \bigcup_{i=1}^{p} g_i K, \;\; K = \bigcup_{j=1}^{q} k_j H$$
$$\implies G = \bigcup_{i=1}^{p} \bigcup_{j=1}^{q} g_i(k_j H) = \bigcup_{i=1}^{p} \bigcup_{j=1}^{q} (g_i k_j) H$$

which shows that G is the disjoint union of pq cosets. Therefore, the number of elements of the coset space is

$$|G \,:\, H| = pq = |G \,:\, K| \cdot |K \,:\, H|$$

Therefore, $|G \,:\, H| = |G \,:\, K| \cdot |K \,:\, H|$. □

12. Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left cosets and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets).

Proof. Let $\varphi(x) = x^{-1}$ and let gH be a left coset of H in G. Then for $g_1 h, g_2 h \in gH$

$$\begin{aligned}
\varphi(g_1 h) &= \varphi(g_2 h) \\
(g_1 h)^{-1} &= (g_2 h)^{-1} \\
h^{-1} g_1^{-1} &= h^{-1} g_2^{-1} \\
h h^{-1} g_1^{-1} &= h h^{-1} g_2^{-1} \\
g_1^{-1} &= g_2^{-1} \\
(g_1^{-1})^{-1} &= (g_2^{-1})^{-1} \\
g_1 &= g_2
\end{aligned}$$

therefore, φ is injective.

We can also see that for $g^{-1} h^{-1} \in gH$ we have

$$\varphi(g^{-1} h^{-1}) = (g^{-1} h^{-1})^{-1} = hg$$

which shows that φ is surjective and sends each left coset of H tin G onto a right coset of h and gives a bijection between the set of left cosets and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets). □

13. Fix any labeling of the vertices of a square and use this to identify D_8 as a subgroup of S_4. Prove that the elements of D_8 and $\langle (1\ 2\ 3) \rangle$ do not commute in S_4.

Proof. Since the generators for D_8 are s and r, if we label the vertices of a square (starting with 1 in the top right corner and then incremented clockwise) and look at the permutations of these numbers we see that $s = (2\ 4)$ and $r = (1\ 2\ 3\ 4)$. Then

$$(2\ 4)(1\ 2\ 3) = (1\ 4\ 2\ 3), \quad (1\ 2\ 3)(2\ 4) = (1\ 2\ 4\ 3)$$

$$(1\ 2\ 3\ 4)(1\ 2\ 3) = (1\ 3\ 2\ 4), \quad (1\ 2\ 3)(1\ 2\ 3\ 4) = (1\ 3\ 4\ 2)$$

Therefore, the elements of D_8 and $\langle(1\ 2\ 3)\rangle$ do not commute in S_4. □

14. Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

Proof. From Proposition 13, if H and K are finite subgroups of a group we have

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Let H be a normal subgroup of S_4 of order 8. Then from Corollary 15 we know that for any $K \leq S_4$ that HK is a subgroup of S_4. Since there are 9 elements in S_4 of order 2, let the first 8 be elements in H so that K will be the subgroup generated by the last element and therefore the intersection of $H \cap K = 1$. Then, from Proposition 13 we have that $|HK| = 16$ but this is a contradiction as S_4 has order 24 and 16 is not a divisor of 24. This is a contradiction. Therefore, there is no normal subgroup of order 8 in S_4.

Similarly, there are 8 elements in S_4 of order 3. If the first three comprised H then there would be another element of order 3 that we could generate a subgroup from. However, using the same argument above we would see that we would have a subgroup of order 9, which is not a divisor of 24.

Therefore, S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3. □

15. Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

Proof. The stabilizer of i is the set $G_i = \{\sigma \in G \mid \sigma(i) = i\}$. If we remove the 1-cycle of i (i.e., the cycle (i) in the permutation σ) for all $\sigma \in G_i$ then we have the symmetric group on $\Omega = \{1, 2, \ldots, i-1, i+1, \ldots, n\}$ so that $|\Omega| = n - 1$. Two symmetric groups are isomorphic if the cardinality of the underlying sets being permuted are equal. Therefore, $G_i \cong S_{n-1}$. Furthermore, from Exercise 10 in Section 1.6, we saw that symmetric groups $S_\triangle$ and S_Ω are isomorphic if $|\triangle| = |\Omega|$ (this showed an isomorphism exists). □

16. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Proof. Since p is prime the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p - 1$. This is due to the fact that all numbers less than p are coprime to p and therefore have multiplicative inverses. By Lagrange's Theorem, the order of the elements of this group must divide the order of the group. Then, let a be an element in $(\mathbb{Z}/p\mathbb{Z})^\times$ so that $\langle a\rangle = \{1, a, a^2, \ldots, a^k\}$ where $k \mid p - 1 \implies kd = p - 1$ for some $d \in \mathbb{Z}$. Therefore we must have that

$$a^{p-1} = a^{kd} = (a^k)^d \equiv 1^d = 1 \equiv 1 \pmod{p}$$

so that multiplying the congruence by a factor of a we arrive at

$$a(a^{p-1} - 1) \equiv 0 \pmod{p} \implies a^p \equiv a \pmod{p}$$

which proves *Fermat's Little Theorem*. □

17. Let p be a prime and let n be a positive integer. Find the order of $\overline{p}$ in $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and deduce that $n \mid \varphi(p^n-1)$ (here φ is Euler's function).

Proof. The order of the element $\overline{p}$ is the smallest number k such that

$$\begin{aligned} p^k &\equiv 1 \pmod{p^n-1} \\ p^k - 1 &\equiv 0 \pmod{p^n-1} \\ \implies p^n - 1 &\mid p^k - 1 \\ \implies n &= k \end{aligned}$$

It cannot be a smaller number because then the divisor would be bigger than the dividend so we see that the order of $\overline{p}$ is n. Since, by Lagrange's Theorem, $|\overline{p}|$ must divide $\varphi(p^n-1)$ we see that $n \mid \varphi(p^n-1)$. □

18. Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Proof. If G is of prime order then the normal subgroups are trivial ones. Therefore, let's assume that G is not of prime order. Then the we can write the order of G as $|G| = pq$, for positive integers p and q.

Let $|G : N| = q$ so that $|N| = p$. Since $(|H|, |G : N|) = 1$ we see that H must not have any elements that divide order q. Thus, H must have elements that have orders that divide p which means that the elements of H are also elements of N which implies $H \leq N$.

Therefore, if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$. □

19. Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Proof. If G is of prime order then the normal subgroups are trivial ones. Therefore, let's assume that G is not of prime order. Then the we can write the order of G as $|G| = pq$, for positive integers p and q.

Let $|G : N| = q$ so that $|N| = p$. Since $(|N|, |G : N|) = 1$ we see that p and q are relatively prime and therefore N must not have any elements that divide the order q.

Similarly, any other subgroup of order p would also be relatively prime to q and therefore wouldn't have any elements that divide the order q. Therefore, this subgroup would have the same elements that N does, showing that they are equal and thus N is the unique subgroup of G of order $|N|$.

Therefore, if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$. □

20. If A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$.

Proof. Since A and B are both subgroups of G and $A \trianglelefteq G$ we know from Corollary 15 that AB is a subgroup of G. Since AB is a group we can show that $A \cap B \trianglelefteq AB$ by looking at the normalizer of $A \cap B$ in AB. Since AB is a group we have that $AB = BA$ which means that for an element $ab \in AB$ we have that $ab = b'a'$ which is an element of BA. Therefore, for $ab \in AB$ we have that $b'a'$ gives us

$$\begin{aligned} (b'a')g(b'a')^{-1} &= b'a'ga'^{-1}b'^{-1} \\ &= b'ga'a'^{-1}b'^{-1} && [g \in A \cap B] \end{aligned}$$

$$= b'gb'^{-1} \in B \implies \in A \cap B \qquad [g \in A \cap B \implies g \in B]$$

Thus, we see that $A \cap B \trianglelefteq AB$.

Therefore, if A is an abelian group with $A \trianglelefteq G$ and B is any subgroup of G prove that $A \cap B \trianglelefteq AB$. □

21. Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index. [Recall Exercise 21, Section 1.6 and Exercise 15, Section 1.]

Proof. Suppose that $\mathbb{Q}$ has a proper subgroup of finite index, say m. Since $\mathbb{Q}$ is abelian, the subgroup is normal and partitions $\mathbb{Q}$ into m cosets so that the quotient group has order m. By Lagrange's Theorem and Corollary 9 we know that if x is an element in this quotient group then $x^m = 1$. However, since this quotient group is divisible (Exercise 14, Section 1) we also have that there exists y in this quotient group such that $x^m = y$, which is a contradiction since we have that $x^m = 1$. Therefore, $\mathbb{Q}$ has no proper subgroups of finite index.

Suppose that $\mathbb{Q}/\mathbb{Z}$ has a proper subgroup of finite index. Then, since the quotient group of a divisible abelian group is divisible and abelian, the same argument as above will arrive at a contradiction. Therefore, we deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index. □

22. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

Proof. The order or $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$. Therefore, from Corollary 9 and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we must have that

$$a^{\varphi(n)} = 1 \equiv 1 \pmod{n}.$$

Therefore, $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n, where φ denotes Euler's φ-function. □

23. Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \pmod{\varphi(100)}$ and use the previous exercise.]

Proof. As the hint suggests, let us first determine $3^{100} \pmod{\varphi(100)}$. Since $(3, \varphi(100)) = 1$ we can use Euler's Theorem to see that

$$3^{\varphi(\varphi(100))} \equiv 1 \pmod{\varphi(100)}$$

Since $\varphi(\varphi(100)) = 16$ we therefore see that

$$3^{16} \equiv 1 \pmod{\varphi(100)}$$

Using this, we can solve for $3^{100} \pmod{\varphi(100)}$

$$3^{100} \equiv 3^{16 \cdot 6 + 4} \equiv (3^{16})^6 \cdot 3^4 \equiv (1)^6 \cdot 3^4 \equiv 81 \equiv 1 \pmod{\varphi(100)}$$

Now, if $m = d + k\varphi(n)$, then

$$a^m = a^{d + k\varphi(n)} = a^d (a^{\varphi(n)})^k \equiv a^d \pmod{n}$$

Therefore, we can see that using both the above expressions we get

$$3^{3^{100}} \equiv 3^1 \equiv 3 \pmod{100}$$

Therefore, the last two digits of $3^{3^{100}}$ is 03. □

3.3 THE ISOMORPHISM THEOREMS

Let G be a group.

1. Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|GL_n(F) : SL_n(F)| = q - 1$. [See Exercise 35, Section 1.]

Proof. From Exercise 35 in Section 1 we saw that $SL_n(F) \trianglelefteq GL_n(F)$ and $GL_n(F)/SL_n(F) \cong F^\times$ with the map $\det(GL_n(F)) \mapsto F^\times$. Since $\det(GL_n(F)) \mapsto F^\times$ is an isomorphic map by Corollary 17(2) we see that $|GL_n(F) : SL_n(F)| = |\varphi(GL_n(F))| = |F^\times|$. Since the order of F is q, then the order of $F^\times$ is $q - 1$ which are the nonzero elements of the field.

Therefore, $|GL_n(F) : SL_n(F)| = q - 1$. □

2. Prove all parts of the Lattice Isomorphism Theorem.

The Fourth or Lattice Isomorphism Theorem.

Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

Proof. If $A \leq B$ then we know that for $x, y \in B$ that $xy^{-1} \in A$. Then for $\overline{a} \in \overline{A}$ we have that

$$\begin{aligned} \overline{a} = aN \in \overline{A} &\implies \in \overline{B} && [a \in A \implies a \in B] \\ = xy^{-1}N \in \overline{A} &\implies \in \overline{B} && [a = xy^{-1} \in A \implies \in B] \\ = \overline{xy^{-1}} \in \overline{A} &\implies \in \overline{B} \end{aligned}$$

Therefore, by the subgroup criterion $\overline{A} \leq \overline{B}$.

Conversely, if $\overline{A} \leq \overline{B}$ then we know that for $\overline{x}, \overline{y} \in \overline{B}$ that $\overline{xy^{-1}} \in \overline{A}$. Then

$$\begin{aligned} \overline{xy^{-1}} = xy^{-1}N \in \overline{A} &\implies \in \overline{B} \\ \implies xy^{-1} \in A &\implies \in B \end{aligned}$$

Therefore, by the subgroup criterion $A \leq B$. □

(2) if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$,

Proof. From The Third Isomorphism Theorem we see that $\overline{B}/\overline{A} = (B/N)/(A/N) \cong B/A$ and since they are isomorphic there is an injective maps which implies $|\overline{B} \ : \ \overline{A}| = |B \ : \ A|$. □

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

Proof. If $g \in \overline{\langle A, B\rangle} = \langle A, B\rangle/N$ then

$$\begin{aligned} g &= (a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} b_1^{\gamma_1} \cdots b_n^{\gamma_n})N \\ &= (a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} N)(b_1^{\gamma_1} \cdots b_n^{\gamma_n} N) \\ &= (a_1^{\epsilon_1} N \cdots a_n^{\epsilon_n} N)(b_1^{\gamma_1} N \cdots b_n^{\gamma_n} N) \\ &\in \langle \overline{A}, \overline{B}\rangle \implies \overline{\langle A, B\rangle} \subset \langle \overline{A}, \overline{B}\rangle \end{aligned}$$

If $g \in \langle \overline{A}, \overline{B}\rangle$ then

$$\begin{aligned} g &= (a_1^{\epsilon_1} N \cdots a_n^{\epsilon_n} N)(b_1^{\gamma_1} N \cdots b_n^{\gamma_n} N) \\ &= (a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} N)(b_1^{\gamma_1} \cdots b_n^{\gamma_n} N) \\ &= (a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} b_1^{\gamma_1} \cdots b_n^{\gamma_n})N \\ &\in \overline{\langle A, B\rangle} \implies \langle \overline{A}, \overline{B}\rangle \subset \langle \overline{A}, \overline{B}\rangle \end{aligned}$$

Therefore, $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$. □

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and

Proof. If $g \in \overline{A \cap B} = (A \cap B)/N$ then

$$\begin{aligned} g &\in (A \cap B)N \\ &\in AN \cap BN \\ &\in \overline{A} \cap \overline{B} \end{aligned}$$

which implies that $\overline{A \cap B} \subseteq \overline{A} \cap \overline{B}$.

If $g \in \overline{A} \cap \overline{B}$ then

$$\begin{aligned} g &\in AN \cap BN \\ &\in (A \cap B)N \\ &\in \overline{A \cap B} \end{aligned}$$

which implies that $\overline{A} \cap \overline{B} \subseteq \overline{A \cap B}$.

Therefore, $\overline{A \cap B} = \overline{A} \cap \overline{B}$. □

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

Proof. If $A \trianglelefteq G$ then

$$\begin{aligned} gag^{-1} &= a && [\text{for some } a \in A \text{ and for all } g \in G] \\ \implies (gag^{-1})N &= (a)N && [N \trianglelefteq G, N \leq A] \\ \implies gNaNg^{-1}N &= aN && [N \text{ is normal - kernel of a homomorphism - well defined}] \end{aligned}$$

$$\implies \overline{A} \trianglelefteq \overline{G}$$

Conversely, if $\overline{A} \trianglelefteq \overline{G}$ then

$$\begin{aligned} & gNaNg^{-1}N = aN \\ \implies & (gag^{-1})N = (a)N && [N \text{ is normal - kernel of a homomorphism - well defined}] \\ \implies & gag^{-1} = a && [\text{for some } a \in A \text{ and for all } g \in G] \\ \implies & A \trianglelefteq G \end{aligned}$$

Therefore, $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$. □

3. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either

(i) $K \leq H$ or

(ii) $G = HK$ and $|K \ : \ K \cap H| = p$.

Proof. Since H is a normal subgroup of G we know that for any $K \leq G$ that HK is a subgroup of G.

(i) If $G \neq HK$ then since $\dfrac{|G|}{|H|} = \dfrac{|G|}{|HK|}\dfrac{|HK|}{|H|} = p$ we see that

$$\frac{|G|}{|HK|} \neq 1 \implies \frac{|HK|}{|H|} = 1 \implies HK = H \implies K \subseteq H \implies K \leq H.$$

(ii) If $G = HK$ then since $|G \ : \ H| = p$, we have $|HK \ : \ H| = p$ and from The Second or Diamond Isomorphism Theorem we know that $HK/H \cong K/(K \cap H)$ which implies $|HK \ : \ H| \cong |K \ : \ K \cap H| = p$. If $G \neq HK$, since H is normal in G we know that HK is a subgroup of G. Therefore, $|G \ : \ HK|$ must be a number that is less than p. □

4. Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.

Proof. Since the Cartesian product is component wise we see that for $(a, b) \in A \times B$ and $(c, d) \in C \times D$ that

$$\begin{aligned} (a,b)(c,d)(a,b)^{-1} &= (a,b)(c,d)(a^{-1},b^{-1}) \\ &= (aca^{-1}, bdb^{-1}) \\ &= (c', d') \in (C \times D) && [\text{for some } c' \in C \text{ and } d' \in D] \end{aligned}$$

Showing that $(C \times D) \trianglelefteq (A \times B)$.

Let $\varphi : (A \times B)/(C \times D) \to (A/C) \times (B/D)$ such that $\varphi((a, b)/(c, d)) = (a/c, b/d)$. This is a homomorphism since

$$\begin{aligned} \varphi\left(\frac{(a_1,b_1)}{(c_1,d_1)} \cdot \frac{(a_2,b_2)}{(c_2,d_2)}\right) &= \varphi\left(\frac{(a_1a_2, b_1b_2)}{(c_1c_2, d_1d_2)}\right) \\ &= \left(\frac{a_1a_2}{c_1c_2}, \frac{b_1b_2}{d_1d_2}\right) \\ &= \left(\frac{a_1}{c_1}, \frac{b_1}{d_1}\right)\left(\frac{a_2}{c_2}, \frac{b_2}{d_2}\right) \end{aligned}$$

$$= \varphi\left(\frac{(a_1, b_1)}{(c_1, d_1)}\right)\varphi\left(\frac{(a_2, b_2)}{(c_2, d_2)}\right)$$

It is easy to see that this is also an isomorphism since the coordinates of the tuples are elements from the groups so injectivity and surjectivity follow easily.

Therefore, we see that $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$. □

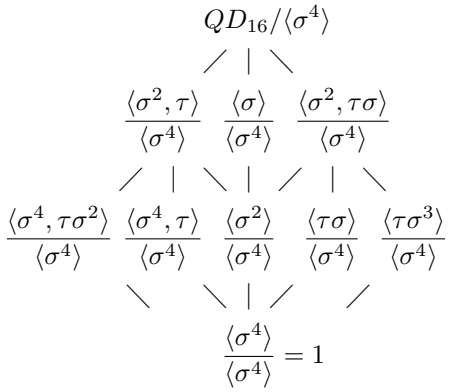
5. Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group described in Exercise 11 of Section 2.5. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $QD_{16}/\langle \sigma^4 \rangle$ to decide the isomorphism type of this group.

Proof. $QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$

It is easy to manually verify $\langle \sigma^4 \rangle$ is normal in QD_{16} since the generators are τ and σ.

$$\begin{aligned}
\sigma\sigma^4\sigma^{-1} &= \sigma^4 \\
\tau\sigma^4\tau^{-1} &= \tau\sigma^3\tau\sigma^3 && [\tau = \tau^{-1}, \sigma\tau = \tau\sigma^3] \\
&= \tau\sigma^2\tau\sigma^6 \\
&= \tau\sigma\sigma^9 \\
&= \tau\tau\sigma^1 2 \\
&= \sigma^4 \in \langle \sigma^4 \rangle
\end{aligned}$$

Therefore, $\langle \sigma^4 \rangle \trianglelefteq QD_{16}$.



The group of order 8 that has the same lattice as this quotient is D_8. The generators and relations for $QD_{16}/\langle \sigma^4 \rangle = \langle \overline{\sigma}, \overline{\tau} \mid \overline{\sigma}^4 = \overline{\tau}^2 = 1, \overline{\sigma\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^{-1}} \rangle$ which is isomorphic to D_8. □

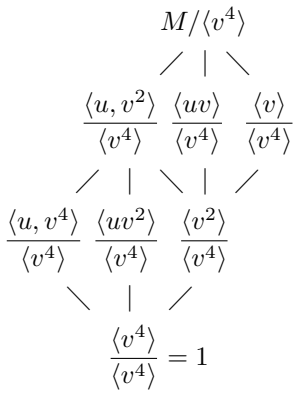
6. Let $M = \langle u, v \rangle$ be the modular group of order 16 described in Exercise 14 of Section 2.5. Prove that $\langle v^4 \rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/\langle v^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $M/\langle v^4 \rangle$ to decide the isomorphism type of this group.

Proof. $M = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$ It is easy to manually verify $\langle v^4 \rangle$ is normal in M since the generators are u and v.

$$vv^4v^{-1} = v^4$$

$$\begin{aligned} uv^4u^{-1} &= uv^3uv^5 && [u = u^{-1}, vu = uv^5] \\ &= uv^2uv^{10} \\ &= uvuv^{15} \\ &= uuv^{20} \\ &= v^4 \in \langle v^4 \rangle \end{aligned}$$

Therefore, $\langle v^4 \rangle \trianglelefteq M$.



The group of order 8 that has the same lattice as this quotient is $Z_2 \times Z_4$. The generators and relations for $M/\langle v^4 \rangle = \langle \overline{u}, \overline{v} \mid \overline{v}^4 = \overline{u}^2 = 1, \overline{vu} = \overline{uv^5} = \overline{uv} \rangle$ which is isomorphic to $Z_2 \times Z_4$. □

7. Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$. [Draw the lattice.]

Proof. If we draw the lattice, similar to Figure 6 in the text, we see that since M and N are both normal in G, both sides of the lattice give $MN/M \cong M/(M \cap N)$ and $MN/N \cong N/(M \cap N)$ from the Second Isomorphism Theorem. Therefore, multiplying these together we see that

$$\begin{aligned} M/(M \cap N) \cdot N/(M \cap N) &\cong MN/M \times MN/N \\ G/(M \cap N) &\cong G/M \times G/N && \text{[can combine similar cosets]} \end{aligned}$$

□

8. Let p be a prime and let G be the group of p-power roots of 1 in $\mathbb{C}$ (cf. Exercise 18, Section 2.4). Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.

Proof. $G = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+ \text{ and } p \text{ prime}\}$ and let φ be the map $z \mapsto z^p$ such that $\varphi : G \to G$ and $\varphi(z) = z^p$. φ is a homomorphism since

$$\begin{aligned} \varphi(z_1z_2) &= (z_1z_2)^p \\ &= z_1^p z_2^p \\ &= \varphi(z_1)\varphi(z_2) \end{aligned}$$

To show that φ is surjective we will need to show that for any element $z \in G$ that there exists another $z \in G$ such that the criteria $z^{p^n} = 1$ is still held. Let $z \in \text{im}\varphi$ so that

$$\begin{aligned} &\varphi(z_1) = z \\ \implies\ &z_1 = z^{1/p} && [\varphi^{-1}(z) = z^{1/p}] \end{aligned}$$

For z_1 to be an element in G it must be a p-power root of unity in $\mathbb{C}$. Therefore, for some $k \in \mathbb{Z}^+$, we must have that $(z_1)^{p^k} = 1$. Therefore

$$\begin{aligned} (z_1)^{p^k} &= (z^{1/p})^{p^k} \\ &= (z^{1/p})^{p^{n+1}} && [k = n+1] \\ &= (z^{1/p})^{pp^n} \\ &= (z)^{p^n} = 1 \end{aligned}$$

showing that $z_1^{p^k} = 1$ and therefore is in G. Thus, φ is surjective.

Since φ is surjective and $\ker\varphi$ is the p-roots of unity (i.e., the kernel is not trivial and therefore φ is not injective), by the First Isomorphism Theorem we can deduce that there is a *proper* quotient of G that is isomorphic to G. □

9. Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)

Proof. Since $P \leq G$ and $N \trianglelefteq G$ we know that $PN \leq G$. From Proposition 13 we know that $|PN| = |P||N|/|P \cap N| \implies |P \cap N| = |P||N|/|PN|$. The order of PN is the number of elements that are in P and N, but those that are not in both. Since $|G| = p^a m, |P| = p^a$, and $|N| = p^b n$, we know from Cauchy's Theorem that G, P, and N all have elements that have order p. Additionally, from Lagrange's Theorem we know that the order of the elements of a group must divide the order of the group, which shows that every element in P must be a power of p. Therefore, the elements in N that are also in P are the elements that are a power of p. Thus, the order of PN is $p^a n$ (i.e., the p^b elements in N are also in P so they were not counted) so we then see that

$$|P \cap N| = |P||N|/|PN| = \frac{p^a p^b n}{p^a n} = p^b$$

From this it is easy to see that

$$|PN/N| = \frac{p^a n}{p^b n} = p^{a-b}$$

□

10. Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Proof. If H is a Hall subgroup of G and $N \trianglelefteq G$, to show that $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N, we will show that the indexes and orders of these subgroups divide $|G : H|$ and $|H|$ respectively. This will show that these divisors must also be relatively prime to each other.

First, to show that $(|N : H \cap N|, |H \cap N|) = 1$ we will show that $|N : H \cap N|$ divides $|G : H|$ and $|H \cap N|$ divides $|H|$, respectively. From Second Isomorphism Theorem we see that

$$H/(H \cap N) \cong HN/N$$

so therefore $|H \cap N|$ is a divisor of $|H|$ (isomorphism is injective, hence they have the same order). Since HN is a subgroup of G we know that it divides the order of G and from Proposition 13 we see that

$$\frac{|N|}{|H \cap N|} = \frac{|HN|}{|H|}$$
$$\implies \frac{|HN|}{|H|} \cdot \frac{|G|}{|HN|} = \frac{|G|}{|H|}$$

showing use that $|N|/|H \cap N|$ is a divisor of $|G|/|H|$. Therefore, $(|N : H \cap N|, |H \cap N|) = 1$

Second, to show that $(|G/N : HN/N|, |HN/N|) = 1$ we will show that $|G/N : HN/N|$ divides $|G : H|$ and $|HH/N|$ divides $|H|$, respectively. We see from the above that since

$$H/(H \cap N) \cong HN/N$$

that $|HN/N|$ is a divisor of $|H|$. Then for $|G/N|/|HN/N| \implies |G|/|HN|$ which we already showed divides $|G : H|$. Therefore, $(|G/N : HN/N|, |HN/N|) = 1$. □

3.4 COMPOSITION SERIES AND THE HÖLDER PROGRAM

1. Prove that if G is an abelian simple group then $G \cong Z_p$ for some prime p (do not assume G is a finite group).

Proof. Since G is abelian, any subgroup of G is normal. However, since G is a simple group we know that its only normal subgroups are 1 and G. Therefore, since its only normal subgroups are 1 and G, it therefore, does not contain any other subgroups.

We will now show that it must also be finite. Assume that G is infinite and that $x \in G$ such that $x \neq 1$. Then we must have that $H = \langle x \rangle$ is a subgroup of G. If $H \neq G$, then we have a proper subgroup of G, which is a contradiction, since G is a simple group. If $H = G$, then we have an infinite cyclic group, which we know is isomorphic to $\mathbb{Z}$ but $\mathbb{Z}$ contains proper subgroups, which is also a contradiction. Therefore, G must be finite.

Since G is finite, and its only subgroups are 1 and G, then by Lagrange's Theorem it must be of prime order since it doesn't contain any other subgroups. Since G is of prime order, by Cauchy's Theorem we know that G must contain an element of prime order and therefore G must be generated by this element. Therefore G is a cyclic group of prime order, $G \cong Z_p$. □

2. Exhibit all 3 composition series for Q_8 and all 7 composition series for D_8. List the composition factors in each case.

D_8:

$$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle rs \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^3 s \rangle \trianglelefteq \langle rs, r^2 \rangle \trianglelefteq D_8$$

Q_8:

$$1 \trianglelefteq \langle i \rangle \trianglelefteq Q_8$$
$$1 \trianglelefteq \langle j \rangle \trianglelefteq Q_8$$
$$1 \trianglelefteq \langle k \rangle \trianglelefteq Q_8$$

3. Find a composition series for the quasidihedral group of order 16 (cf. Exercise 11, Section 2.5). Deduce that QD_{16} is solvable.

Since r commutes with all of QD_{16} we know that the subgroups generated from this are all normal. Additionally, looking at the composition factors of the subgroups generated from r we see that they are all simple. Therefore, a composition series for the quasidihedral group of order 16 is:

$$1 \trianglelefteq \langle r^4 \rangle \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq QD_{16}$$

Since each of these composition factors are abelian we see that G is solvable.

4. Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.

Proof. Let G be a finite abelian group.

base case: $|G| = 1$, which is trivial.

induction hypothesis: $|G| = n - 1$. Suppose that subgroups of G exist for all $k, 1 \leq k \leq n-1$, where $k \mid n-1$.

induction step: $|G| = n$. Let m be a divisor of n. If m is prime, then by Cauchy's Theorem there exists an element of order m and thus a subgroup of order m. If m is not prime, then m is a composite number. Let $m = kp$ for some prime p. By Cauchy's Theorem there is $g \in G$ such that $|g| = p$ and therefore $|\langle g \rangle| = p$. Since G is abelian, all of its subgroups are normal so we have $\langle g \rangle \trianglelefteq G \implies G/\langle g \rangle$ and by the induction hypothesis we have $|G/\langle g \rangle| = k$ (since $p \neq 1$ we know that we are in the range $1 \leq k \leq n-1$).

Therefore, for $\overline{x} \in G/\langle g \rangle$ we have that

$$|\overline{x}| = k \implies (\overline{x})^k = (x\langle g \rangle)^k = x^k \langle g \rangle \implies x^k \in \langle g \rangle$$

There are two possibilities for the value of x^k. One is that $x^k = 1 \in \langle g \rangle$ and the other is $x^{kp} = 1 \in \langle g \rangle$ for $x^k \neq 1$. If it is the later, we are done since $|x| = kp = m$, which shows that there is a subgroup of order m. If it is the former then we have that $\langle x \rangle \cap \langle g \rangle = 1$, since the order of g is prime. Therefore,

$$|\langle x\rangle\langle g\rangle| = \frac{|\langle x\rangle||\langle g\rangle|}{|\langle x\rangle \cap \langle g\rangle|} = \frac{kp}{1} = kp = m$$

Thus, $\langle x, g\rangle = \langle x\rangle\langle g\rangle$ is a subgroup of G of order m. □

5. Prove that subgroups and quotient groups of a solvable group are solvable.

Proof. A group G is solvable if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$.

For $N \leq G$ let $N_i = G_i \cap N$. Since $G_i \trianglelefteq G_{i+1}$ we see that for $x \in N_i$ and $y \in N_{i+1}$ we have $yxy^{-1} \in N$. We also have $yxy^{-1} \in G_i$ since $G_i \trianglelefteq G_{i+1}$. Therefore, $yxy^{-1} \in G_i \cap N = N_i$. Thus, $N_i \trianglelefteq N_{i+1}$ and therefore we have a chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_s = N$$

Now we need to show that N_{i+1}/N_i is abelian. Note that

$$N_i = G_i \cap N = G_i \cap (G_{i+1} \cap N) = G_i \cap N_{i+1}.$$

and then by the Second Isomorphism Theorem we have that

$$\frac{N_{i+1}}{N_i} = \frac{N_{i+1}}{G_i \cap N_{i+1}} \cong \frac{G_i N_{i+1}}{G_i} \leq \frac{G_i + 1}{G_i}$$

since G_i and N_{i+1} are both subgroups of G_{i+1}. Therefore, since G_{i+1}/G_i is abelian, all of its subgroups are as well so we see that N_{i+1}/N_i is abelian. Therefore, subgroups of a solvable group are solvable.

Let N be a normal subgroup of G so that G/N is a quotient group. Then we have the chain of subgroups

$$1 \trianglelefteq N \trianglelefteq G$$

But we know that G is solvable so we know that we also have the chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

therefore N must be one of these subgroups. Let $N = G_k$. Then, since N is normal we know that G/N is a quotient group and from the Fourth Isomorphism Theorem we know that there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. Therefore, we know that we will have the chain of subgroups

$$1 = G_k/N \trianglelefteq G_{k+1}/N \trianglelefteq \cdots \trianglelefteq G_s/N = G/N$$

Furthermore, from the Third Isomorphism Theorem we have that

$$\frac{G_{i+1}/N}{G_i/N} \cong \frac{G_{i+1}}{G_i} \text{ for all } k \leq i \leq s$$

so that each factor of this chain of subgroups is also abelian. Therefore, quotient groups of a solvable group are solvable. □

6. Prove part (1) of the Jordan-Hölder Theorem by induction on $|G|$.

Part (1) of the Jordan-Hölder Theorem states that for a finite group G with $G \neq 1$ that

$$G \text{ has a composition series.}$$

A composition series is a sequence of subgroups in G such that

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

where $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i a simple group for $0 \leq i \leq k-1$.

Proof. Since $G \neq 1$ then $|G| > 1$.

base case: $|G| = 2$. Any group of order 2 has the composition series

$$1 = 1 \trianglelefteq G = G$$

induction hypothesis: Assume all groups $|G| < n$ have a composition series.

induction step: $|G| = n$. G is either simple or it is not. If G is simple, then from the same argument as the base case we see that it has a composition series. If G is not simple then it *has* a normal subgroup other than 1 and G, say N. Then G/N is a quotient group and since its order is less than the order of G, by the induction hypothesis, it has a composition series

$$1 = \overline{G_0} \leq \overline{G_1} \leq \cdots \leq \overline{G_s} = \overline{G}$$

From the Fourth Isomorphism Theorem we know that this composition series corresponds to

$$N = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

and also that $G_i \trianglelefteq G_{i+1}$ if and only if $\overline{G_i} \trianglelefteq \overline{G_{i+1}}$ so that by the Third Isomorphism Theorem we see that

$$\frac{\overline{G_{i+1}}}{\overline{G_i}} \cong \frac{G_{i+1}}{G_i}$$

So that the composition factors are simple. Thus, $N = G_0 \leq G_1 \leq \cdots \leq G_s = G$ is a composition series for $\overline{G}$.

The order of N is also less than the order of G and it too, by the induction hypothesis, has a composition series

$$1 = N_0 \leq N_1 \leq \cdots \leq N_k = N$$

Putting these two composition series together we get the composition series for G

$$1 = N_0 \leq N_1 \leq \cdots \leq N \leq G_1 \leq \cdots \leq G_s = G$$

Therefore, by induction, all finite groups have a composition series. □

7. If G is a finite group and $H \trianglelefteq G$ prove that there is a composition series of G, one of whose terms is H.

Proof. From the proof of Exercise 6 we can see that in the composition series for G that the normal subgroup N was one of the terms. In the same manner and derivation, we see that H is a term in the composition series of G. □

8. Let G be a *finite* group. Prove that the following are equivalent:

(i) G is solvable

(ii) G has a chain of subgroups: $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is cyclic, $0 \leq i \leq s = 1$

(iii) all composition factors of G are of prime order

(iv) G has a chain of subgroups: $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t-1$.

[For (iv), prove that a minimal nontrivial normal subgroup M of G is necessarily abelian and then use induction. To see that M is abelian, let $N \trianglelefteq M$ be of prime index (by (iii)) and show that $x^{-1}y^{-1}xy \in N$ for all $x, y \in M$ (cf. Exercise 40, Section 1). Apply the same argument to gNg^{-1} to show that $x^{-1}y^{-1}xy$ is in the intersection of all G-conjugates of N, and use the minimality of M to conclude that $x^{-1}y^{-1}xy = 1$.]

Proof.
(i) $\rightarrow$ (ii): If G is solvable then there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$. Since G_{i+1}/G_i is abelian, we know that if its order can be divided, that a subgroup exists. If its order cannot be divided then we know that the quotients G_{i+1}/G_i are cyclic since they are of prime order [Corollary 10]. If it can be divided then we know that the quotients G_{i+1}/G_i have a normal subgroup, say H. Then we must have the series

$$\overline{1} \trianglelefteq \overline{H} \trianglelefteq \overline{G_{i+1}}$$

and from the Fourth Isomorphism Theorem we know that there then exists the series

$$G_i \trianglelefteq H \trianglelefteq G_{i+1}$$

Since G is finite, this process can be repeated until G_{i+1}/H_i do not contain anymore subgroups for all of G_{i+1}/G_i in the series. Then, we will have a series such that all quotients are cyclic as desired.

(ii) $\rightarrow$ (iii): If G has a chain of subgroups: $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is cyclic, $0 \leq i \leq s = 1$, then all quotients are either of prime order or they aren't. If they are, we are done. If not,

then for the quotients not of prime order, since the quotients are cyclic they are also abelian (since taking powers of an element is commutative). From Exercise 4 we know that there exist subgroups for any divisor of the quotients. Therefore in the same manner as (i) $\rightarrow$ (ii), using the Fourth Isomorphism Theorem, we can construct a series were all the quotients are of prime order.

(iii) $\rightarrow$ (iv): If all composition factors of G are of prime order then they must be cyclic [Corollary 10] and therefore abelian (since taking powers of an element is commutative). Let $N \trianglelefteq M$ be of prime index, where M is assumed to be a minimal nontrivial subgroup of G. Therefore, in the quotient group M/N we have

$$\begin{gathered}\overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x}^{-1}\overline{xy}^{-1}\overline{y} = \overline{1} \\ \iff x^{-1}y^{-1}xy \in N\end{gathered}$$

gNg^{-1}, for any $g \in G$ is obviously a subgroup of G but it is also a subgroup of M since M is normal (i.e. $gNg^{-1} \subseteq M$). We will show that it is is normal in M. For it to be normal in M, for $n \in N$ and $m \in M$, we need to have

$$\begin{gathered}m(gng^{-1})m^{-1} \in gNg^{-1} \\ (g^{-1}mg)n(g^{-1}m^{-1}g) \in N\end{gathered}$$

which we know is true since N is normal in M. Thus, gNg^{-1} is a normal subgroup of M and by the same argument above, we see that for all $g \in G$

$$x^{-1}y^{-1}xy \in gNg^{-1}$$

Which shows that $x^{-1}y^{-1}xy$ is in the intersection of all G-conjugates of N. However

$$I = \bigcap_{g \in G} gNg^{-1}$$

is a normal subgroup of G since if $x \in I$ and $g \in G$, then we must have that $x \in N$ so that gxg^{-1} and it must be the trivial subgroup because if it wasn't this would contradict the minimality of M. Therefore, I must be the trivial subgroup and

$$x^{-1}y^{-1}xy = 1 \in I$$

so that $xy = yx$ for $x, y \in M$. This shows that a minimal normal subgroup M must be abelian (we could have shown this with $M/N \cong M/1 \cong M$, since M is minimal and $N \trianglelefteq M$ is of prime index, which shows that M is abelian since the composition factors of prime index are abelian).

Now that we have shown that M is abelian, we will show by induction that there is a chain of normal subgroups where the composition factors are abelian. Suppose that M_1 is a the minimal normal subgroup of G. Then we have the chain

$$1 \trianglelefteq M_1 \trianglelefteq G$$

Using the same argument as above, we must have that there is a minimal nontrivial normal subgroup of G/M_1, say $\overline{M_2}$, which is also abelian. Then we have

$$\overline{1} \trianglelefteq \overline{M_2} \trianglelefteq \overline{G} = G/M_1$$

By the Fourth Isomorphism Theorem, there then exists the series

$$M_1 \trianglelefteq M_2 \trianglelefteq G$$

From the two series above we see that $\overline{M_2} = M_2/M_1$ is abelian and also that M_2 is normal. Therefore, since G is finite, we can continue this same process a finite number of steps, say n, to get the series

$$1 \trianglelefteq M_1 \trianglelefteq M_2 \trianglelefteq \cdots \trianglelefteq M_n = G$$

Which shows that was required.

(iv) $\to$ (i): This is the definition of a solvable group. □

9. Prove the following special case of part (2) of the Jordan-Hölder Theorem: assume the finite group G has two composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G \text{ and } 1 = M_0 \trianglelefteq M_1 \trianglelefteq M_2 = G.$$

Show that $r = 2$ and that the list of composition factors is the same. [Use the Second Isomorphism Theorem.]

Proof. If $M_1 = N_{r-1}$ then we see that the two composition series match up and we are done. Let's assume that $M \neq N_{r-1}$ and let $H = N_{r-1} \cap M$. From the composition series we see that the composition factor $M/1 \cong M$ is simple, so therefore M does not have any nontrivial normal subgroups. It is easy to see that H is normal in M and therefore it must be trivial.

Then, by the Second Isomorphism Theorem we have that

$$\frac{N_{r-1}}{N_{r-1} \cap M} \cong \frac{N_{r-1}M}{M}$$

where the left hand side evaluates to N_{r-1}. Now, on the right hand side, we see that $N_{r-1}M$ must be normal as the join of two normal subgroups is normal. Also, since N_{r-1} is nontrivial (from its composition series), we see that $N_{r-1}M$ is larger than M. Assume that $N_{r-1}M \neq G$ so that

$$M \trianglelefteq N_{r-1}M \trianglelefteq G$$

and if we divide this out with M we see that

$$\overline{1} \trianglelefteq \overline{N_{r-}M} \trianglelefteq \overline{G} = G/M$$

However, we know that G/M is simple as it is a composition factor and therefore it doesn't have any nontrivial normal subgroups. Therefore, we have a contradiction. Therefore, we must have that $N_{r-1}M = G$ so that we have

$$N_{r-1} \cong \frac{N_{r-1}M}{M} \cong G/M$$

which we know doesn't have any nontrivial normal subgroups. Therefore, we must have that $r = 2$. The composition factors for $N_{r-1} \neq M$ between the two composition series are $G/N_{r-1} \cong M$ and $N_{r-1}/1 \cong G/M$. □

10. Prove part (2) of the Jordan-Hölder Theorem by induction on $\min\{r, s\}$. [Apply the inductive hypothesis to $H = N_{r-1} \cap M_{s-1}$ and use the preceding exercises.]

Proof. Let G be a finite group with $G \neq 1$.

base case: From Exercise 9 we have already proven part (2) of the Jordan-Hölder Theorem for $\min\{r, s\} = 2$.

induction hypothesis: Assume part (2) of the Jordan-Hölder Theorem holds for $n < \min\{r, s\}$.

induction step: Suppose there are two composition series for G

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G$$
$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_s = G$$

Let $H = N_{r-1} \cap M_{s-1}$. The composition series for G contain sub-composition series for N_{r-1} and M_{s-1} from the induction hypothesis. If we have $H = N_{r-1} = M_{s-1}$ then by the induction hypothesis we must have that

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{r-1}$$
$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_{s-1}$$

are both of the same length, which shows that $r = s$ and the composition factors for G are the composition factors in the series plus $G/N_{r-1} \cong G/M_{s-1}$. On the other hand, if $N_{r-1} \neq M_{s-1}$ then similar to the argument used in the proof of Exercise 9 we must have that $N_{r-1}M_{s-1}$ is normal and larger than M_{s-1} as N_{r-1} can't be trivial as it is part of the composition series. Then we must have a chain

$$M_{s-1} \trianglelefteq N_{r-1}M_{s-1} \trianglelefteq G$$

which we can divide by M_{s-1} to get the chain

$$\overline{1} \trianglelefteq \overline{N_{r-1}M_{s-1}} \trianglelefteq \overline{G} = G/M_{s-1}$$

which is a contradiction since G/M_{s-1} is a composition factor of the series and must therefore be simple. Thus, we must have that $N_{r-1} = M_{s-1}$ showing that $r = s$ and that the two composition series are equivalent with composition factors $G/N_{r-1} \cong G/M_{s-1}$. □

11. Prove that if H is a nontrivial normal subgroup of the solvable group G then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.

Proof. Since $H \trianglelefteq G$ and G is solvable we must have that G/N is abelian. Therefore for $x, y \in G$ we have that

$$\begin{aligned} &(xH)(yH) = (yH)(xH) \\ \iff &[xH, yH] = H \\ \iff &[x, y]H = H \end{aligned}$$

$$\iff [x, y] \in H$$

which shows that $A \leq H$ is the *commutator subgroup* of G. It was proved in Exercise 41, Section 3.1 that this group is a normal subgroup of G. For $x, y \in G$ we have

$$\begin{aligned} &(xH)(yH) = (yH)(xH) && [G/H \text{ is abelian}] \\ \iff &xyH = yxH && [H \text{ is normal}] \\ \iff &xy = yx \in H \end{aligned}$$

and therefore for $[x_1, y_1], [x_2, y_2] \in H$ we have

$$\begin{aligned} &([x_1, y_1]H)([x_2, y_2]H) = ([x_2, y_2]H)([x_1, y_1]H) && [G/H \text{ is abelian}] \\ \iff &[x_1, y_1][x_2, y_2] = [x_2, y_2][x_1, y_1] \end{aligned}$$

showing that A is abelian. □

12. Prove (without using the Feit-Thompson Theorem) that the following are equivalent:

(i) every group of odd order is solvable

(ii) the only simple groups of odd order are those of prime order.

Proof.
(i) → (ii): If every group of odd order is solvable then let G be of odd order and simple. Then, since G is simple we have the chain

$$1 \trianglelefteq G$$

which shows that the quotient group $G/1 \cong G$ must be abelian. Yet, all subgroups of an abelian group are normal so this shows that the only subgroups of G are 1 and G. Therefore, by Lagrange's Theorem we know that the group must be of prime order.

(ii) → (i): If the only simple groups of odd order are those of prime order then let G be a simple group of odd and prime order. Then, since G is simple and of odd and prime order we see from Lagrange's Theorem that its only subgroups are the 1 and G itself so that we have the chain

$$1 \trianglelefteq G$$

Additionally, we know that since G is of prime order that G is cyclic and $G \cong Z_p$ [Corollary 10]. Thus, G must be abelian since taking powers of an element is commutative. Hence, $G \cong G/1$ is also abelian, showing that G and thus every group of odd order is solvable. □

3.5 TRANSPOSITIONS AND THE ALTERNATING GROUP

1. In Exercises 1 and 2 of Section 1.3 you were asked to find the cycle decomposition of some permutations. Write each of these permutations as a product of transpositions. Determine which of these is an even permutation and which is an odd permutation.

Proof.
Exercise 1:

$$\sigma = (1\ 3\ 5)(2\ 4) \implies (2\ 4)(1\ 5)(1\ 3),\ \epsilon(\sigma) = -1$$

$$\begin{aligned}
\tau &= (1\ 5)(2\ 3) \implies \text{already a product of transpositions, } \epsilon(\tau) = 1 \\
\sigma^2 &= (1\ 5\ 3) \implies (1\ 3)(1\ 5),\ \epsilon(\sigma^2) = 1 \\
\sigma\tau &= (2\ 5\ 3\ 4) \implies (2\ 4)(2\ 3)(2\ 5),\ \epsilon(\sigma\tau) = -1 \\
\tau\sigma &= (1\ 2\ 4\ 3) \implies (1\ 3)(1\ 4)(1\ 2),\ \epsilon(\tau\sigma) = -1 \\
\tau^2\sigma &= (1\ 3\ 5)(2\ 4) \implies (2\ 4)(1\ 5)(1\ 3),\ \epsilon(\tau^2\sigma) = -1
\end{aligned}$$

Exercise 2:

$$\begin{aligned}
\sigma &= (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) \implies (1\ 10)(1\ 5)(1\ 13)(3\ 8)(3\ 15)(4\ 9)(4\ 12)(4\ 7)(4\ 11)(4\ 14),\ \epsilon(\sigma) = 1 \\
\tau &= (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11) \implies (1\ 14)(2\ 4)(2\ 13)(2\ 15)(2\ 9)(3\ 10)(5\ 7)(5\ 12)(8\ 11), \epsilon(\tau) = -1 \\
\sigma^2 &= (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13) \implies (1\ 5)(3\ 15)(3\ 8)(4\ 12)(4\ 11)(7\ 14)(7\ 9)(10\ 13),\ \epsilon(\sigma^2) = 1 \\
\sigma\tau &= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14) \implies (1\ 3)(1\ 11)(2\ 4)(5\ 15)(5\ 10)(5\ 7)(5\ 8)(5\ 9)(13\ 14),\ \epsilon(\sigma\tau) = -1 \\
\tau\sigma &= (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14) \implies (1\ 4)(2\ 9)(3\ 5)(3\ 11)(3\ 15)(3\ 12)(3\ 13)(8\ 14)(8\ 10),\ \epsilon(\tau\sigma) = -1 \\
\tau^2\sigma &= (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10) \implies \\
&\quad (1\ 10)(1\ 5)(1\ 7)(1\ 13)(1\ 12)(1\ 11)(1\ 14)(1\ 4)(1\ 3)(1\ 8)(1\ 15)(1\ 2),\ \epsilon(\tau^2\sigma) = 1
\end{aligned}$$

□

2. Prove that σ^2 is an even permutation for every permutation σ.

Proof. $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism. Therefore, for any permutation σ we have that

$$\begin{aligned}
\epsilon(\sigma^2) &= \epsilon(\sigma \cdot \sigma) \\
&= \epsilon(\sigma)\epsilon(\sigma) \\
&= (\pm 1)(\pm 1) = 1
\end{aligned}$$

□

3. Prove that S_n is generated by $\{(i\ i+1) \mid 1 \le i \le n-1\}$. [Consider conjugates, viz. $(2\ 3)(1\ 2)(2\ 3)^{-1}$.]

Proof. The text shows that S_n is generated from its transpositions, $S_n = \langle (i\ j) \mid 1 \le i < j \le n \rangle$. Here we will prove that S_n is generated from the $n-1$ transpositions

$$(1\ 2), (2\ 3), \ldots, (n-1\ n)$$

by showing that they produce each transposition $(a\ b)$ in S_n. Since $(a\ b) = (b\ a)$, without loss of generality let $a < b$. We will show with induction on $b - a$ that $(a\ b)$ is a product of transpositions $(i\ i+1)$.

base case: For $b - a = 1$ we see that

$$(a\ b) = (a\ a+1)$$

is one of the transpositions of the generating set so it is trivially included.

induction hypothesis: Assume that $(1\ 2), (2\ 3), \ldots, (n-1\ n)$ is a generating set for transpositions with a difference up to, $b - a = k - 2 > 1$.

induction step: Now we will show that $(1\ 2), (2\ 3), \ldots, (n-1\ n)$ is a generating set for all of S_n by showing that it generates all transpositions $\{(i\ j) \mid 1 \leq i < j \leq n\}$. The induction hypothesis takes care of all transpositions up to a difference of $k-2$. With conjugation we have

$$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1)^{-1}$$

and in order to generate all of S_n we need that $b-a = k-1$. Suppose that $b-a = k-1$. The first and third transpositions on the right hand side are handled by the base case. The middle transposition on the right hand side has a difference of

$$b-(a+1) = b-a-1 = k-1-1 = k-2$$

and is handled by the induction hypothesis.

Therefore, S_n is generated by $\{(i\ i+1) \mid 1 \leq i \leq n-1\}$. □

4. Show that $S_n = \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$ for all $n > 2$.

Proof. From Exercise 3, it suffices to show that $\langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$, for all $n > 2$, will produce $\{(i\ i+1) \mid 1 \leq i \leq n-1\}$. Let $\sigma \in S_n$ and note that for an n-cycle, say $(1\ 2\ 3\ \ldots n)$ we have that

$$\sigma(1\ 2\ 3\ \ldots\ n)\sigma^{-1}$$

If we let $\sigma(x)$ represent the number that is to the right of x in the permutation σ then x will be the number to the left of the number $\sigma(x)$ in the permutation σ^{-1} since σ^{-1} cycles in the opposite direction as σ. Looking at the cycle decomposition above, let us see how the numbers are permuted. Starting on the right, choose a number in σ^{-1}, say $\sigma(x)$. This will then point to the left, which by our convention would be, at x. Then, the next step is to go to the n-cycle to the left and starting at x, we see that this would point to the right at $x+1$ (unless $x = n$, in which case this would point to 1). The next step is to then go this number in the permutation σ and then this would point to $\sigma(x+1)$, to the right of $x+1$. Therefore, we would have that the above cycle decomposition is equal to the

$$\sigma(1\ 2\ 3\ \ldots\ n)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \ldots\ \sigma(n))$$

With this in mind, now let's take a look at the conjugation of the generators

$$(1\ 2\ 3\ \ldots\ n)(1\ 2)(1\ 2\ 3\ \ldots\ n)^{-1} = (\sigma(1)\ \sigma(2)) = (2\ 3)$$

and continuing in this fashion we can see that we can generate the rest of $\{(i\ i+1) \mid 1 \leq i \leq n-1\}$ with

$$(1\ 2\ 3\ \ldots\ n)^k(1\ 2)(1\ 2\ 3\ \ldots\ n)^{-k} = (\sigma^k(1)\ \sigma^k(2)) = (k+1\ k+2)$$

which we can see is true for all $n > 2$.

Therefore, $S_n = \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$ for all $n > 2$. □

5. Show that if p is prime, $S_p = \langle \sigma, \tau \rangle$ where σ is any transposition and τ is any p-cycle.

Proof. Let us denote the transposition as $\sigma = (a\ b)$, with $1 \leq a < b \leq p$. If $b - a = 1$ then from Exercise 4, with a relabeling of the n elements to coincide with a and b we would have

$$S_p = \langle (a\ b), (a\ b\ \dots) \rangle$$

If $b - a > 1$ let $\tau = (1\ 2\ 3\ \dots\ p)$ and note that the powers of τ give

$$\begin{aligned} \tau &= (1\ 2\ \dots\ p) \\ \tau^2 &= (1\ 3\ \dots\ p-1) \\ \tau^3 &= (1\ 4\ \dots\ p-2) \\ &\dots \\ \tau^{p-1} &= (1\ p\ \dots 2) \\ \tau^p &= 1 \end{aligned}$$

What this shows that there exists a p-cycle that will have a difference of b and a amongst its entries. Note that we would not have a p-cycle for every power of τ if p were not prime (for example $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$). Therefore, relabeling the power of τ so that it is the p-cycle that coincides with a and b we have

$$S_p = \langle (a\ b), (a\ b\ \dots) \rangle$$

Therefore, if p is prime, $S_p = \langle \sigma, \tau \rangle$ where σ is any transposition and τ is any p-cycle. □

6. Show that $\langle (1\ 3), (1\ 2\ 3\ 4) \rangle$ is a proper subgroup of S_4. What is the isomorphism type of this subgroup?

Proof. From the previous exercises, we know that in order to generate all of S_4 we need to be be able to produce all transpositions that differ by 1. Therefore, in order to be able to generate all of S_4 with the transposition of $(1\ 3)$ we would need a power of $(1\ 2\ 3\ 4)$ to sequentially have a difference of 2 between each number of the cycle. However, if we let $\sigma = (1\ 2\ 3\ 4)$ we see that this is impossible as its powers are

$$\begin{aligned} \sigma &= (1\ 2\ 3\ 4) \\ \sigma^2 &= (1\ 3)(2\ 4) \\ \sigma^3 &= (1\ 4\ 3\ 2) \\ \sigma^4 &= 1 \end{aligned}$$

Therefore, $\langle (1\ 3), (1\ 2\ 3\ 4) \rangle$ must be a proper subgroup of S_4. $\langle (1\ 3), (1\ 2\ 3\ 4) \rangle \cong D_8$ since $(1\ 3)$ has order 2 and $(1\ 2\ 3\ 4)$ has order 4, similar to s and r respectively. □

7. Prove that the group of rigid motions of a tetrahedron is isomorphic to A_4. [Recall Exercise 20 in Section 1.7.]

Proof. From Exercise 20 in Section 1.7 we saw that the group of rigid motions of a tetrahedron are the permutations

$$\{1,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 4)(2\ 3),\ (1\ 3)(2\ 4),\ (1\ 2)(3\ 4)\}$$

and that they were a subgroup of S_4. For this to be isomorphic to A_4 we need that each of these 12 permutations are even. Thus, we need that $\epsilon(\sigma) = 1$, which the identity permutation obviously maps to 1. For the other permutations, note that an m-cycle is an odd permutation if and only if m is even and that $\epsilon(\sigma) = 1$ if σ is a product of an even number of transpositions, which shows that these are all even permutations.

Therefore, the group of rigid motions of a tetrahedron is isomorphic to A_4. □

8. Prove the lattice of subgroups of A_4 given in the text is correct. [By the preceding exercise and the comments following Lagrange's Theorem, A_4 has no subgroup of order 6.]

Proof. From Exercise 7 we can see that all of the permutations of A_4 are accounted for in graph. In the graph we can also see that the edges for the 3-cycles between 1 and A_4 are correct since the order of the 3-cycles is 3 and $|A_4| = 12$. For $\langle(1\ 2)(3\ 4)\rangle, \langle(1\ 3)(2\ 4)\rangle, \langle(1\ 4)(2\ 3)\rangle$ it is easy to verity they each have order two. For $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ we see that $(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$ so $|\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle| = 4$ and all edges between subgroups is correct.

Thereofore, the lattice of subgroups of A_4 given in the text is correct. □

9. Prove that the (unique) subgroup of order 4 in A_4 is normal and is isomorphic to V_4.

Proof. To show that $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is a normal subgroup of A_4 will see if any of the generators from the subgroups of order 3 normalize it (no need to check the subgroups of order 2 as they are already subgroups of this group).

$$
\begin{aligned}
(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} &= (1\ 4)(2\ 3)\\
(1\ 2\ 4)(1\ 2)(3\ 4)(1\ 2\ 4)^{-1} &= (1\ 3)(2\ 4)\\
(1\ 3\ 4)(1\ 2)(3\ 4)(1\ 3\ 4)^{-1} &= (1\ 4)(2\ 3)\\
(2\ 3\ 4)(1\ 2)(3\ 4)(2\ 3\ 4)^{-1} &= (1\ 3)(2\ 4)\\
(1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} &= (1\ 2)(3\ 4)\\
(1\ 2\ 4)(1\ 3)(2\ 4)(1\ 2\ 4)^{-1} &= (1\ 4)(2\ 3)\\
(1\ 3\ 4)(1\ 3)(2\ 4)(1\ 3\ 4)^{-1} &= (1\ 2)(3\ 4)\\
(2\ 3\ 4)(1\ 3)(2\ 4)(2\ 3\ 4)^{-1} &= (1\ 4)(2\ 3)
\end{aligned}
$$

Therefore, $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is normal in A_4. This group is isomorphic to V_4 since its a group of order 4 and each of its nontrivial elements have order 2. □

10. Find a components series for A_4. Deduce that A_4 is solvable.

Proof. From Exercise 9 we see that $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is normal in A_4 with order 4. Let us denote this subgroup as N. We see that the component series

$$1 \trianglelefteq N \trianglelefteq A_4$$

has composition factors A_4/N and $N/1 \cong N$. The former has prime order and is isomorphic to Z_3, which is abelan. The latter is isomorphic to V_4, as we saw in Exercise 9, which is also abelian.

Therefore, A_4 is solvable. □

11. Prove that S_4 has no subgroup isomorphic to Q_8.

Proof. Q_8 has 3 cyclic subgroups of order 4. In Exercise 4 of section 1.3 we saw that S_4 has 6 4-cycles and all 6 of these 4-cycles are generated by the 3 subgroups of Q_8. Therefore, if Q_8 was a subgroup of S_4 it would need to contain all of these permutations. However, the square of a 4-cycle is a double transposition and this two would need to be part of the group (closure under multiplication). This means Q_8 would also need to contain V_4 as we saw from Exercise 10 that it was generated from two double transpositions. This would be an additional 4 permutations to the previous 6 which is 10 and therefore more than the 8 elements of Q_8.

Therefore, S_4 has no subgroup isomorphic to Q_8. □

12. Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.

Proof. **base case:** For $n = 3$, we see that A_3 has a subgroup that is isomorphic to S_1, namely the identity element.

induction hypothesis: Assume that A_n contains a subgroup isomorphic to S_{n-2} for each $n = k - 1 \geq 3$.

induction step: Suppose that we have A_n for $n = k \geq 3$. Then □

13. Prove that every element of order 2 in A_n is the square of an element of order 4 in S_n. [An element of order 2 in A_n is a product of $2k$ commuting transpositions.]

Proof. □

14. Prove that the subgroup of A_4 generated by any element of order 2 and any element of order 3 is all of A_4.

Proof. □

15. Prove that if x and y are distinct 3-cycles in S_4 with $x \neq y^{-1}$, then the subgroup of S_4 generated by x and y is A_4.

Proof. □

16. Let x and y be distinct 3-cycles in S_5 with $x \neq y^{-1}$.

(a) Prove that is x and y fix a common element of $\{1, \ldots, 5\}$, then $\langle x, y \rangle \cong A_4$.

Proof. □

(b) Prove that if x and y do not fix a common element of $\{1, \ldots, 5\}$, then $\langle x, y \rangle \cong A_5$.

Proof. □

17. If x and y are 3-cycles in $S - n$, prove that $\langle x, y \rangle$ is isomorphic to Z_3, A_4, A_5 or $Z_3 \times Z_3$.

Proof. □