MATH 6121: selected solutions

Written and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

Exercise 1.1. If $\vec{u} \in \mathbb{C}^n$ and $M\vec{u} = \vec{0}_{\mathbb{C}^m}$, then show that $T(L_{\mathcal{B}}^{-1}(\vec{u})) = \vec{0}_W$.

Solution 1.2. Suppose that $\vec{u} \in \mathbb{C}^n$ and $M\vec{u} = \vec{0}_{\mathbb{C}^m}$, with $M = {}_{\mathcal{C}}[T]_{\mathcal{B}}$. Let $\vec{u}$ be denoted as follows:

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \in \mathbb{C}^n.$$

Now, since $M = {}_{\mathcal{C}}[T]_{\mathcal{B}}$, we have that:

$$M = \left[L_{\mathcal{C}}\left(T\left(\vec{b}_1\right)\right),\ L_{\mathcal{C}}\left(T\left(\vec{b}_2\right)\right), \ldots, L_{\mathcal{C}}\left(T\left(\vec{b}_n\right)\right)\right],$$

letting $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$. Since $M\vec{u} = \vec{0}_{\mathbb{C}^m}$, we have that:

$$L_{\mathcal{C}}\left(T\left(\vec{b}_1\right)\right) u_1 + \cdots + L_{\mathcal{C}}\left(T\left(\vec{b}_n\right)\right) u_n = \vec{0}_{\mathbb{C}^m}.$$

By linearity of $L_{\mathcal{C}}$ and T, we have that:

$$L_{\mathcal{C}}\left(T\left(u_1\vec{b}_1 + \cdots + u_n\vec{b}_n\right)\right) = \vec{0}_{\mathbb{C}^m}.$$

Since $L_{\mathcal{C}}$ is a linear isomorphism, from the above equality, we have that:

$$T\left(u_1\vec{b}_1 + \cdots + u_n\vec{b}_n\right) = \vec{0}_W.$$

Equivalently, $T(L_{\mathcal{B}}^{-1}(\vec{u})) = \vec{0}_W$. □

Exercise 1.3. Show that $V \oplus W$ forms a vector space.

Solution 1.4. Given $(\vec{v}, \vec{w}), (\vec{x}, \vec{y}) \in V \oplus W$, we have that

$$(\vec{v}, \vec{w}) +_{\oplus} (\vec{x}, \vec{y}) \in V \oplus W,$$

since $+_V$ is a binary operation on V and $+_W$ is a binary operation on W, with $\vec{v} +_V \vec{x} \in V$ and $\vec{w} +_W \vec{y} \in W$.

The commutativity of $+_{\oplus}$ is inherited from the commutativity of $+_V$ and $+_W$ in an obvious manner, as indicated below.

$$\begin{aligned}(\vec{v}_1, \vec{w}_1) +_{\oplus} (\vec{v}_2, \vec{w}_2) &= (\vec{v}_1 +_V \vec{v}_2, \vec{w}_1 +_W \vec{w}_2) \\ &= (\vec{v}_2 +_V \vec{v}_1, \vec{w}_2 +_W \vec{w}_1) \\ &= (\vec{v}_2, \vec{w}_2) +_{\oplus} (\vec{v}_1, \vec{w}_1).\end{aligned}$$

The associativity of $+_{\oplus}$ is inherited from the associativity of $+_V$ and $+_W$ in an obvious manner, as indicated below.

$$(\vec{v}_1, \vec{w}_1) +_{\oplus} \Big((\vec{v}_2, \vec{w}_2) +_{\oplus} (\vec{v}_3, \vec{w}_3) \Big) = (\vec{v}_1, \vec{w}_1) +_{\oplus} (\vec{v}_2 +_V \vec{v}_3, \vec{w}_2 +_W \vec{w}_3)$$

$$
\begin{aligned}
&= (\vec{v}_1 +_V (\vec{v}_2 +_V \vec{v}_3), \vec{w}_1 +_W (\vec{w}_2 +_W \vec{w}_3)) \\
&= ((\vec{v}_1 +_V \vec{v}_2) +_V \vec{v}_3, (\vec{w}_1 +_W \vec{w}_2) +_W \vec{w}_3) \\
&= (\vec{v}_1 +_V \vec{v}_2, \vec{w}_1 +_W \vec{w}_2) +_\oplus (\vec{v}_3, \vec{w}_3) \\
&= \Big((\vec{v}_1, \vec{w}_1) +_\oplus (\vec{v}_2, \vec{w}_2)\Big) +_\oplus (\vec{v}_3, \vec{w}_3).
\end{aligned}
$$

Given $(\vec{v}, \vec{w}) \in V \oplus W$, we have that

$$(\vec{v}, \vec{w}) +_\oplus (-\vec{v}, -\vec{w}) = (\vec{0}, \vec{0})$$

and

$$(\vec{v}, \vec{w}) +_\oplus (\vec{0}, \vec{0}) = (\vec{0}, \vec{0}) +_\oplus (\vec{v}, \vec{w}) = (\vec{v}, \vec{w}).$$

The domain of the operation $\cdot_\oplus$ is from the Cartesian product of the underlying field of V and W with the direct sum $V \oplus W$. It is clear that the codomain of this operation is $V \oplus W$, since we have that

$$c \cdot_\oplus (\vec{v}, \vec{w}) = (c\vec{v}, c\vec{w}) \in V \oplus W$$

since $c\vec{v} \in V$ and $v\vec{w} \in W$. The properties concerning the operation $\cdot_\oplus$ given below show that $V \oplus W$ forms a vector space with respect to the operations $+_{V \oplus W}$ and $\cdot_{V \oplus W}$.

$$
\begin{aligned}
(c+d) \cdot_\oplus (\vec{v}, \vec{w}) &= ((c+d) \cdot_V \vec{v}, (c+d) \cdot_W \vec{w}) \\
&= (c \cdot_V \vec{v} + d \cdot_V \vec{v}, c \cdot_W \vec{w} + d \cdot_W \vec{w}) \\
&= (c \cdot_V \vec{v}, c \cdot_W \vec{w}) +_\oplus (d \cdot_V \vec{v}, d \cdot_W \vec{w}) \\
&= c \cdot_\oplus (\vec{v}, \vec{w}) +_\oplus d \cdot_\oplus (\vec{v}, \vec{w}), \\
c \cdot_\oplus \big((\vec{v}, \vec{w}) +_\oplus (\vec{x}, \vec{y})\big) &= c \cdot_\oplus (\vec{v} +_V \vec{x}, \vec{w} +_W \vec{y}) \\
&= (c \cdot_V (\vec{v} +_V \vec{x}), c \cdot_W (\vec{w} +_W \vec{y})) \\
&= (c \cdot_V \vec{v} +_V c \cdot_V \vec{x}, c \cdot_W \vec{w} +_W c \cdot_W \vec{y}) \\
&= (c \cdot_V \vec{v}, c \cdot_W \vec{w}) +_\oplus (c \cdot_V \vec{x}, c \cdot_W \vec{y}) \\
&= c \cdot_\oplus (\vec{v}, \vec{w}) +_\oplus c \cdot_\oplus (\vec{x}, \vec{y}), \\
(cd) \cdot_\oplus (\vec{v}, \vec{w}) &= ((cd) \cdot_V \vec{v}, (cd) \cdot_W \vec{w}) \\
&= (c \cdot_V (d \cdot_V \vec{v}), c \cdot_W (d \cdot_W \vec{w})) \\
&= c \cdot_\oplus (d \cdot_V \vec{v}, d \cdot_W \vec{w}) \\
&= c \cdot_\oplus (d \cdot_\oplus (\vec{v}, \vec{w})), \\
1 \cdot_\oplus (\vec{v}, \vec{w}) &= (1 \cdot_V \vec{v}, 1 \cdot_W \vec{w}) \\
&= (\vec{v}, \vec{w}).
\end{aligned}
$$

Exercise 1.5. Let $\dim(V) = n$, $\dim(W) = m$, $\dim(X) = r$, and $\dim(Y) = s$. Prove that ${}_{\mathcal{B}_{X \oplus Y}}[T \oplus Q]_{\mathcal{B}_{V \oplus W}}$ is equal to the following $(r+s) \times (n+m)$ matrix.

$$
\begin{array}{cc}
 & \begin{array}{cc} \quad n \quad & \quad m \quad \end{array} \\
\begin{array}{c} r \\ s \end{array} & \left[\begin{array}{c|c} {}_{\mathcal{B}_X}[T]_{\mathcal{B}_V} & 0 \\ \hline 0 & {}_{\mathcal{B}_Y}[Q]_{\mathcal{B}_W} \end{array}\right]
\end{array}
$$

Solution 1.6. By definition, the transition matrix

$${}_{\mathcal{B}_{X \oplus Y}}[T \oplus Q]_{\mathcal{B}_{V \oplus W}}$$

is equal to the following matrix:

$$\Big[L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{v}_1,\vec{0})), L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{v}_2,\vec{0})), \dots, L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{v}_n,\vec{0})),$$
$$L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{0},\vec{w}_1)), L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{0},\vec{w}_2)), \dots, L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{0},\vec{w}_m))\Big].$$

The matrix in the upper-right $r \times n$ quadrant of

$$_{\mathcal{B}_{X\oplus Y}}[T\oplus Q]_{\mathcal{B}_{V\oplus W}}$$

must be $_{\mathcal{B}_X}[T]_{\mathcal{B}_V}$, because the first r entries in

$$L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{v}_1,\vec{0}))$$

must be the first r entries in $L_{\mathcal{B}_X}(T(\vec{v}_i))$ for all indices i, since $\mathcal{B}_{X\oplus Y}$ is given by the direct sum of the bases $\mathcal{B}_X$ and $\mathcal{B}_Y$, i.e. $\mathcal{B}_{X\oplus Y}$ consists of expressions of the form $(\vec{x}_j,\vec{0})$ and $(\vec{0},\vec{y}_k)$. Similarly, the last s entries in

$$L_{\mathcal{B}_{X\oplus Y}}((T\oplus Q)(\vec{v}_i,\vec{0}))$$

all must be 0 since $Q(\vec{0}) = \vec{0}$. Symmetric arguments may be used to evaluate the remaining quadrants.

Exercise 1.7. Let $V = \mathbb{R}^2$, and let $W = \mathbb{R}^2$. With respect to the tensor product $V \otimes W$, show that:

$$\begin{aligned}(1,1)\otimes(1,4) + (1,-2)\otimes(-1,2) = {} & 0\,(1,0)\otimes(1,0) + \\ & 6\,(1,0)\otimes(0,1) + \\ & 3\,(0,1)\otimes(1,0) + \\ & 0\,(0,1)\otimes(0,1)\,.\end{aligned}$$

With respect to the direct sum $V \oplus W$, show that

$$((1,1),(1,4)) + ((1,-2),(-1,2)) = ((2,-1),(0,6))\,.$$

Solution 1.8. Recall that the tensor product $M \otimes N$ of two modulues M and N over a ring R may informally be defined as the set of expressions of the form $m \otimes n$ for $m \in M$ and $n \in N$, subject to the following relations:

(i) $x \otimes (y + y') = x \otimes y + x \otimes y'$;

(ii) $(x + x') \otimes y = x \otimes y + x' \otimes y$;

(iii) $(x \cdot r) \otimes y = x \otimes (r \cdot y)$.

Expand the expression

$$(1,1)\otimes(1,4) + (1,-2)\otimes(-1,2)$$

using the above relations as follows.

$$\begin{aligned}&(1,1)\otimes(1,4) + (1,-2)\otimes(-1,2)\\ &= (1,0)\otimes(1,4) + (1,-2)\otimes(-1,2) + (0,1)\otimes(1,4)\\ &= (1,0)\otimes(1,0) + (1,-2)\otimes(-1,2) + (0,1)\otimes(1,4) + (1,0)\otimes(0,4)\\ &= (1,0)\otimes(1,0) + (1,-2)\otimes(-1,2) + (0,1)\otimes(1,4) + 4(1,0)\otimes(0,1)\end{aligned}$$

$$\begin{aligned}
&= (1,0)\otimes(1,0) + (1,-2)\otimes(-1,2) + (0,1)\otimes(1,0) + 4(1,0)\otimes(0,1) + (0,1)\otimes(0,4)\\
&= (1,0)\otimes(1,0) + (1,-2)\otimes(-1,2) + (0,1)\otimes(1,0) + 4(1,0)\otimes(0,1) + 4(0,1)\otimes(0,1)\\
&= (1,0)\otimes(1,0) + (1,0)\otimes(-1,2) + (0,1)\otimes(1,0) + 4(1,0)\otimes(0,1) + 4(0,1)\otimes(0,1)\\
&+ (0,-2)\otimes(-1,2)\\
&= (1,0)\otimes(1,0) - (1,0)\otimes(1,-2) + (0,1)\otimes(1,0) + 4(1,0)\otimes(0,1) + 4(0,1)\otimes(0,1) - 2(0,1)\otimes(-1,2)\\
&= (0,1)\otimes(1,0) + 4(1,0)\otimes(0,1) + 4(0,1)\otimes(0,1) + 2(0,1)\otimes(1,-2) + 2(1,0)\otimes(0,1)\\
&= (0,1)\otimes(1,0) + 6(1,0)\otimes(0,1) + 2(0,1)\otimes(1,0)\\
&= 3(0,1)\otimes(1,0) + 6(1,0)\otimes(0,1).
\end{aligned}$$

Using componentwise addition, we have that $(1,1)+(1,-2)=(2,-1)$ and $(1,4)+(-1,2)=(0,6)$, so $((1,1),(1,4))+((1,-2),(-1,2))=((2,-1),(0,6))$.

Exercise 1.9. Let $\mathcal{B}_V = \{\vec{v}_1,\vec{v}_2,\vec{v}_3\}$ and $\mathcal{B}_W = \{\vec{w}_1,\vec{w}_2\}$. Let $\phi\colon V\to V$ be such that

$$\phi\left(a\vec{v}_1 + b\vec{v}_2 + c\vec{v}_3\right) = c\vec{v}_1 + 2a\vec{v}_2 - 3b\vec{v}_3,$$

and let $\psi\colon W\to W$ be such that

$$\psi\left(a\vec{w}_1 + b\vec{w}_2\right) = (a+3b)\,\vec{w}_1 + (4b-2a)\,\vec{w}_2.$$

Compute ${}_{\mathcal{B}_V}[\phi]_{\mathcal{B}_V}$, ${}_{\mathcal{B}_W}[\psi]_{\mathcal{B}_W}$, and

$${}_{\mathcal{B}_{V\otimes W}}[\phi\otimes\psi]_{\mathcal{B}_{V\otimes W}}.$$

Note that $\mathcal{B}_{V\otimes W}$ consists of six elements that have a specific order.

Solution 1.10. Begin by computing ${}_{\mathcal{B}_V}[\phi]_{\mathcal{B}_V}$ and ${}_{\mathcal{B}_W}[\psi]_{\mathcal{B}_W}$ as follows.

$$\begin{aligned}
{}_{\mathcal{B}_V}[\phi]_{\mathcal{B}_V} &= \left[L_{\mathcal{B}_V}(\phi(\vec{v}_1)), L_{\mathcal{B}_V}(\phi(\vec{v}_2)), L_{\mathcal{B}_V}(\phi(\vec{v}_3))\right]\\
&= \begin{bmatrix} c & 0 & 0\\ 0 & 2a & 0\\ 0 & 0 & -3b\end{bmatrix},\\
{}_{\mathcal{B}_W}[\psi]_{\mathcal{B}_W} &= \left[L_{\mathcal{B}_W}(\psi(\vec{w}_1)), L_{\mathcal{B}_W}(\psi(\vec{w}_2))\right]\\
&= \begin{bmatrix} a+3b & 0\\ 0 & 4b-2a\end{bmatrix}.
\end{aligned}$$

The matrix

$${}_{\mathcal{B}_{V\otimes W}}\left[\phi\otimes\psi\right]_{\mathcal{B}_{V\otimes W}}$$

may be evaluated as the Kronecker product of ${}_{\mathcal{B}_V}[\phi]_{\mathcal{B}_V}$ and ${}_{\mathcal{B}_W}[\psi]_{\mathcal{B}_W}$. Write $A = {}_{\mathcal{B}_V}[\phi]_{\mathcal{B}_V}$, and write $B = {}_{\mathcal{B}_W}[\psi]_{\mathcal{B}_W}$. Also, let the entries of A be denoted as follows: $A = [a_{ij}]_{1\le i,j\le 3}$. Then the matrix

$${}_{\mathcal{B}_{V\otimes W}}\left[\phi\otimes\psi\right]_{\mathcal{B}_{V\otimes W}}$$

is equal to the Kronecker product of A and B, which is equal to the following matrix:

$$\begin{bmatrix} a_{1,1}B & a_{1,2}B & a_{1,3}B\\ a_{2,1}B & a_{2,2}B & a_{2,3}B\\ a_{3,1}B & a_{3,2}B & a_{3,3}B\end{bmatrix}.$$

Explicitly, we have that the matrix

$$_{\mathcal{B}_{V\otimes W}}[\phi \otimes \psi]_{\mathcal{B}_{V\otimes W}}$$

is equal to the following matrix:

$$\begin{bmatrix} ac+3bc & 0 & 0 & 0 & 0 & 0 \\ 0 & 4bc-2ac & 0 & 0 & 0 & 0 \\ 0 & 0 & 2a^2+6ab & 0 & 0 & 0 \\ 0 & 0 & 0 & 8ab-4a^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3ab-9b^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -12b^2+6ab \end{bmatrix}.$$

Exercise 1.11. Prove that if $\phi\colon G \to H$ is a homomorphism, then $\text{im}(\phi) \leq H$ with respect to $\circ_H$, where $\text{im}(\phi) = \{\phi(g) : g \in G\}$.

Solution 1.12. Given a subset S of the underlying set of a group T, to prove that S forms a subgroup of T, it suffices to prove that S is closed under the underlying binary operation of T and that S is closed under inverses with respect to this operation. This property concerning subgroups is sometimes referred to as the Two-Step Subgroup Test (see Joseph A. Gallian's *Contemporary Abstract Algebra*).

So, let g_1 and g_2 be arbitrary elements in G, so that $\phi(g_1)$ and $\phi(g_2)$ are arbitrary elements in $\text{im}(\phi)$. Since $\phi\colon G \to H$ is a homomorphism, we have that

$$\phi(g_1) \circ_H \phi(g_2) = \phi(g_1 \circ_G g_2) \in \text{im}(\phi),$$

thus proving that $\text{im}(\phi)$ is closed with respect to $\circ_H$. Similarly, we have that

$$(\phi(g))^{-1} = \phi(g^{-1}) \in \text{im}(\phi)$$

for $g \in G$, since

$$(\phi(g))^{-1}\phi(g) = e_H = \phi(e_G) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$$

since a group homomorphism must map a group identity element to another group identity element, since $\phi(e_G g) = \phi(g) = \phi(e_G)\phi(g)$, and thus $\phi(e_G) = e_H$ from the equality $\phi(g) = \phi(e_G)\phi(g)$.

Exercise 1.13. Prove that $\ker(\phi) \trianglelefteq G$, where $\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$.

Solution 1.14. We begin by proving that $\ker(\phi) \leq G$, using the Two-Step Subgroup Test described above.

Let $g_1, g_2 \in G$ be such that $\phi(g_1) = e_H$ and $\phi(g_2) = e_H$, so that g_1 and g_2 are arbitrary elements in the kernel $\ker(\phi)$ of the group homomorphism $\phi\colon G \to H$. We thus have that

$$\phi(g_1) \circ \phi(g_2) = \phi(g_1 \circ g_2) = e_H \circ e_H = e_H,$$

thus proving that $g_1 \circ g_2 \in \ker(\phi)$. Similarly, since for $g \in G$ we have that $(\phi(g))^{-1} = \phi(g^{-1})$ as discussed above, we have that

$$(\phi(g))^{-1} = e_H^{-1} = e_H$$

if $g \in \ker(\phi)$ and thus $\phi(g^{-1}) = e_H$ if $g \in \ker(\phi)$, thus proving that $\ker(\phi) \leq G$.

Now, let $k \in \ker(\phi)$, and let $i \in G$. It remains to prove that: $iki^{-1} \in \ker(\phi)$. Equivalently, it remains to prove that $\phi(iki^{-1}) = e_H$. Using the fact that $k \in \ker(\phi)$, we have that

$$\phi(iki^{-1}) = \phi(i)\phi(k)\phi(i^{-1}) = \phi(i)\phi(i^{-1}) = \phi(i \circ i^{-1}) = \phi(e_G) = e_H,$$

thus proving that $\ker(\phi) \trianglelefteq G$.

Exercise 1.15. Prove Cayley's theorem.

Solution 1.16. Let ψ denote the mapping which maps $g \in G$ to the permutation in S_G given by the mapping $h \mapsto g \bullet h$, letting the codomain of ψ be equal to $\text{im}(\psi)$.

First, we begin by proving that ψ is well-defined in the sense that for $g \in G$, $\psi(g)$ is indeed an element in the codomain of ψ. For $g \in G$, let σ_g denote the mapping $\sigma_g\colon G \to G$ whereby

$$\sigma_g(h) = g \bullet h = g \circ h \in G$$

for all $h \in G$. The mapping σ_g must be injective, since

$$\sigma_g(h_1) = \sigma_g(h_2) \Longrightarrow gh_1 = gh_2 \Longrightarrow h_1 = h_2,$$

and the mapping $\sigma_g\colon G \to G$ must be surjective, since for $k \in G$, we have that: $\sigma_g(g^{-1}k) = g \circ g^{-1} \circ k = k \in G$, thus proving that $\sigma_g \in S_G$, and thus proving that σ_g is in the codomain of ψ.

Now let $g_1, g_2 \in G$, and let $\sigma_{g_1}\colon G \to G$ and $\sigma_{g_2}\colon G \to G$ be such that $\sigma_{g_1}(h) = g_1 h \in G$ and $\sigma_{g_2}(h) = g_2 h \in G$ for all $h \in G$. Suppose that $\psi(g_1) = \psi(g_2)$. That is, $\sigma_{g_1} = \sigma_{g_2}$. That is, $g_1 h = g_2 h$ for all $h \in G$. Letting $h = e$, we thus have that $\psi(g_1) = \psi(g_2) \Longrightarrow g_1 = g_2$, thus proving that ψ is injective.

Since we constructed ψ so that the codomain of ψ is equal to the image of ψ, we have that ψ is surjective by definition. Since ψ is bijective, it remains to prove that ψ is a group homomorphism.

Again let $g_1, g_2 \in G$. We thus have that $\psi(g_1 g_2)$ is the mapping $\sigma_{g_1 g_2}\colon G \to G$ which maps h to $g_1 g_2 h$. But it is clear that the composition $\psi(g_1) \circ \psi(g_2)$ maps h to $g_1(g_2 h) = g_1 g_2 h$, thus proving that ψ is an isomorphism.

Exercise 1.17. For all $g_1, g_2 \in G$, show that either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \varnothing$.

Solution 1.18. Let $g_1, g_2 \in G$. Our strategy is to show that if $g_1 H \cap g_2 H$ is nonempty, then $g_1 H = g_2 H$. We remark that we are using the logical equivalence whereby $(\neg p) \to q \equiv q \vee p$.

Suppose that $g_1 H \cap g_2 H$ is nonempty. Note that we are letting $H \leq G$. So there exists an element in the following intersection:

$$\{g_1 h : h \in H\} \cap \{g_2 h : h \in H\}.$$

We thus have that there exist elements h_1 and h_2 in H such that

$$g_1 h_1 = g_2 h_2 \in g_1 H \cap g_2 H.$$

Therefore,

$$g_1 h_1 h_2^{-1} = g_2.$$

Writing $h_3 = h_1 h_2^{-1} \in H$, we thus have that $g_1 h_3 = g_2$. We thus have that the left coset $g_2 H$ is equal to $\{g_1 h_3 h : h \in H\}$. But since the mapping from H to H which maps $h \in H$ to $h_3 h$ is bijective (see previous exercise), we have that

$$g_2 H = \{g_1 h_3 h : h \in H\} = \{h_1 i : i \in H\} = g_1 H$$

as desired.

Exercise 1.19. Show that the canonical mapping $\phi_g\colon H \to gH$ is a bijection, so that, as a consequence, we have that $|gH| = |H|$. Another consequence of this result is that $|H|$ divides $|G|$ (*Lagrange's theorem*).

Solution 1.20. Let $H \leq G$, and let $g \in G$, and let $\phi_g : H \to gH$ be such that $\phi_g(h) = gh \in gH$ for all $h \in H$. We have that

$$\phi_g(h_1) = \phi_g(h_2) \Longrightarrow gh_1 = gh_2 \Longrightarrow h_1 = h_2,$$

thus proving the injectivity of ϕ_g. Similarly, it is clear that ϕ_g is surjective, since for $gh \in gH$ we have that $\phi_g(h) = gh$. We thus have that $|gH| = |H|$ as desired.

We now use this result to prove Lagrange's theorem. We have previously shown that two cosets g_1H and g_2H are either disjoint or equal. Therefore, since $g \in gH$ for all $g \in G$, we have that G may be written as a disjoint union of cosets, say

$$G = g_1H \cup g_2H \cup \cdots \cup g_nH$$

where $n \in \mathbb{N}$. But since $|gH| = |H|$ for $g \in G$, we have that $|G| = n|H|$, thus proving Lagrange's theorem.

Exercise 1.21. For $g \in G$, let order(g) denote the smallest $n \in \mathbb{N}$ such that $g^n = e$. Show that order(g) divides $|G|$.

Solution 1.22. It is easily seen that the set

$$\{1, g, g^2, \ldots, g^{\text{order}(g)-1}\}$$

forms a cyclic subgroup of G. By Lagrange's theorem, proven above, we have that the order of this cyclic subgroup divides $|G|$, and we thus have that order(g) divides $|G|$ as desired.

Exercise 1.23. Prove that Stab(x) is a subgroup of G.

Solution 1.24. We again make use of the Two-Step Subgroup Test described above.

Let $g_1, g_2 \in G$ be such that $g_1 \bullet x = x$ and $g_2 \bullet x = x$, so that g_1 and g_2 are arbitrary elements in Stab(x). Now consider the following expression: $(g_1g_2) \bullet x$. By definition of a group action, we have that

$$(g_1g_2) \bullet x = g_1 \bullet (g_2 \bullet x) = g_1 \bullet x = x,$$

thus proving that Stab(x) is closed under the underlying binary operation of G. Letting $g \in G$ be such that $g \bullet x = x$, since $(g^{-1}g) \bullet x = e \bullet x = x$ by definition of a group action, we have that $g^{-1} \bullet (g \bullet x) = x$, thus proving that $g^{-1} \bullet x = x$ as desired, with Stab$(x) \leq G$.

Exercise 1.25. Prove that a G-set X is a disjoint union of orbits.

Solution 1.26. Let x be a G-set, and let $\bullet : G \times X \to X$ denote a group action. Let $x, y \in X$, so that Orbit(x) and Orbit(y) are arbitrary orbits. Suppose that Orbit$(x) \cap$ Orbit$(y) \neq \varnothing$. Let

$$g_1 \bullet x = g_2 \bullet y \in X$$

denote an element in the nonempty intersection Orbit$(x) \cap$ Orbit(y). We thus have that

$$(g_2^{-1}g_1) \bullet x = y.$$

Therefore,

$$\text{Orbit}(y) = \{g \bullet (g_2^{-1}g_1 \bullet x) \mid g \in G\}.$$

Equivalently,

$$\text{Orbit}(y) = \{g(g_2^{-1}g_1) \bullet x \mid g \in G\}.$$

Since the mapping whereby $g \mapsto g(g_2^{-1}g_1)$ is a permutation of G, we thus have that

$$\text{Orbit}(y) = \{h \bullet x \mid h \in G\},$$

thus proving that two orbits are either equal or disjoint. Since $x \in \text{Orbit}(x)$ for $x \in X$, we thus have that X may be written as a disjoint union of orbits.

Exercise 1.27. Show that the map

$$\phi_x\colon \text{Orbit}(x) \to G/\text{Stab}(x)$$

given by the mapping

$$g \bullet x \mapsto g\text{Stab}(x) \in G/\text{Stab}(x)$$

is a well-defined, bijective G-set homomorphism.

Solution 1.28. Suppose that $g_1 \bullet x = g_2 \bullet x$. Equivalently, $g_2^{-1}g_1 \bullet x = x$. Therefore, $g_2^{-1}g_1 \in \text{Stab}(x)$, so $g_1 \in g_2\text{Stab}(x)$, so $g_1\text{Stab}(x) = g_2\text{Stab}(x)$, since two given cosets must be disjoint or equal. We thus have the mapping ϕ_x is well-defined in the sense that $g_1 \bullet x = g_2 \bullet x$ implies that $\phi_x(g_1 \bullet x) = \phi_x(g_2 \bullet x)$.

Letting $g_1, g_2 \in G$ so that $g_1 \bullet x$ and $g_2 \bullet x$ are arbitrary elements in the domain of ϕ_x, we have that

$$\phi_x(g_1 \bullet x) = \phi_x(g_2 \bullet x) \Longrightarrow g_1\text{Stab}(x) = g_2\text{Stab}(x).$$

We thus have that there exist elements $g_3, g_4 \in \text{Stab}(x)$ such that

$$g_1g_3 = g_2g_4.$$

We thus have that

$$(g_1g_3) \bullet x = (g_2g_4) \bullet x,$$

which implies that

$$g_1 \bullet x = g_2 \bullet x,$$

thus proving the injectivity of ϕ_x. It is obvious that ϕ_x is surjective, since given a coset $g\text{Stab}(x)$ in the codomain of ϕ_x, we have that $\phi_x(g) = g\text{Stab}(x)$.

Since

$$\phi_x((hg) \bullet x) = (hg)\text{Stab}(x) = h(g\text{Stab}(x)) = h\phi_x(g \bullet x),$$

we have that ϕ_x is a G-set homomorphism.

Exercise 1.29. Prove that if $H \trianglelefteq G$, then G/H forms a group with respect to the operation $\circ_{G/H}$ on G/H whereby $g_1H \circ_{G/H} g_2H = g_1g_2H$ for all $g_1, g_2 \in G$.

Solution 1.30. Assume that $H \trianglelefteq G$. We begin by showing that the operation $\circ_{G/H} = \circ$ is *well-defined* in the sense that the expression $g_1H \circ_{G/H} g_2H$ does not depend on the coset representatives of the cosets g_1H and g_2H. So, suppose that $g_1H = g_3H$ and $g_2H = g_4H$, letting $g_1, g_2, g_3, g_4 \in G$. To prove that the operation $\circ_{G/H}$ is well-defined, it thus remains to prove that:

$$g_1g_2H = g_3g_4H.$$

Since $g_1H = g_3H$, let $g_3 = g_1h_1$, where $h_1 \in H$. Similarly, since $g_2H = g_4H$, let $g_4 = g_2h_2$, with $h_2 \in H$. So, it remains to prove that

$$g_1g_2H = g_1h_1g_2h_2H.$$

But since $H \trianglelefteq G$, we have that $gH = Hg$ for all $g \in G$. Since $h_1g_2 \in Hg_2 = g_2H$, let $h_1g_2 = g_2h_3$, where $h_3 \in H$. We thus have that

$$g_1h_1g_2h_2H = g_1g_2h_3h_2H.$$

But it is clear that

$$g_1g_2h_3h_2H = g_1g_2H$$

since the mapping $h \mapsto h_3h_2h$ is a bijection on H. We thus have that

$$g_3g_4H = g_1g_2H$$

as desired, thus proving that $\circ_{G/H}$ is well-defined.

Since $\circ_{G/H}$ maps elements in $(G/H) \times (G/H)$ to G/H, we have that G/H is a binary operation on G/H. So we have thus far shown that $\circ_{G/H}$ is a well-defined binary operation on G/H.

The binary operation $\circ_{G/H} = \circ$ inherits the associativity of the underlying binary operation of G in a natural way:

$$\begin{aligned} g_1H \circ (g_2H \circ g_3H) &= g_1H \circ ((g_2g_3)H) \\ &= g_1(g_2g_3)H \\ &= (g_1g_2)g_3H \\ &= (g_1g_2)H \circ g_3H \\ &= (g_1H \circ g_2H) \circ g_3H. \end{aligned}$$

We have thus far shown that $\circ_{G/H}$ is a well-defined associative binary operation on G/H.

Letting $g \in G$ be arbitrary, and letting $e = e_G$ denote the identity element in G, we have that:

$$\begin{aligned} (eH)(gH) &= (eg)H \\ &= eH \\ &= (ge)H \\ &= (gH)(eH). \end{aligned}$$

Again letting $g \in G$ be arbitrary, we have that:

$$\begin{aligned} (gH)(g^{-1}H) &= (g \cdot g^{-1})H \\ &= eH \\ &= (g^{-1}g)H \\ &= (g^{-1}H)(gH). \end{aligned}$$

We thus have that if $H \trianglelefteq G$, then G/H forms a group under the operation $\circ_{G/H}$ given above.

Exercise 1.31. Show that $\phi: G \to G/H$ is a group homomorphism, where $g \mapsto gH$, and $\ker(\phi) = H$.

Solution 1.32. Since $\ker(\phi) \trianglelefteq G$ as shown above, from our results given in the previous exercise, we have that G/H is a group with respect to the binary operation $\circ_{G/H}$.

Now let $g_1, g_2 \in G$. We thus have that

$$\phi(g_1g_2) = (g_1g_2)H = (g_1H) \circ_{G/H} (g_2H) = \phi(g_1) \circ_{G/H} \phi(g_2)$$

by definition of the well-defined group operation $\circ_{G/H}$.

Exercise 1.33. If N is normal in G, then $\forall g \in G\ \exists g' \in G\ gN = Ng'$.

Solution 1.34. Our strategy is to prove the following much stronger statement: "N is normal in G if and only if $\forall g \in G\ gN = Ng$."

We are using the following definition of the term *normal subgroup* given in class: "H is a normal subgroup of G if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, denoted by $H \trianglelefteq G$."

($\Longrightarrow$) First suppose that $N \trianglelefteq G$, i.e. with respect to the above definition. We thus have that $hnh^{-1} \in N$ for all $h \in G$ and $n \in N$. Now consider the left coset gN, letting $g \in G$ be arbitrary:

$$gN = \{gn\ :\ n \in N\}.$$

Now, for $gn \in gN$, we have that $gng^{-1} \in N$ by assumption that $N \trianglelefteq G$, according to the above definition of the term *normal subgroup*. So, letting g be "fixed" (and arbitrary), for *each* choice of an element $n \in N$, we have that there exists a corresponding element $n' \in N$ such that $gng^{-1} = n'$. That is, for each $n \in N$, we have that $gn = n'g$ for some $n' \in N$. So it is clear that

$$gN = \{gn\ :\ n \in N\} = \{n'g\ :\ n' \in M \subseteq N\} \subseteq Ng$$

for some subset $M \subseteq N$. Similarly, for each element ng in the right coset Ng, since $g^{-1}ng = n''$ for some $n'' \in N$ by the above definition of the term *normal subgroup*, we have that $ng = g(n'')$, so it is clear that

$$Ng = \{ng\ :\ n \in N\} = \{g(n'')\ :\ n'' \in M' \subseteq N\} \subseteq gN$$

for some subset $M' \subseteq N$. So since $gN \subseteq Ng$ and $gN \supseteq Ng$, by *mutual inclusion*, we have that $gN = Ng$ as desired.

($\Longleftarrow$) Conversely, suppose that $\forall g \in G\ gN = Ng$. So, let $g \in G$ and $n \in N$ be arbitrary. Since $gN = Ng$, we have that there exists some element $n' \in N$ such that $gn = (n')g$. Therefore, $gng^{-1} = n' \in N$, as desired.

Exercise 1.35. Let $M_G(A) = \{g \in G \mid gag^{-1} \in G \text{ for all } a \in A\}$, then show that $M_G(A)$ is not a group in general. Hint: Take G to be the group of permutations of the set of integers and show that for $A = \{\sigma \in G : \sigma(i) = i, \text{ for } i < 0\}$ that $g(x) = x + 1 \in M_G(A)$, but $g^{-1}(x) = x - 1 \notin M_G(A)$.

Solution 1.36. Let G denote the permutation group $S_{\mathbb{Z}}$ of the set $\mathbb{Z}$ of all integers. Let

$$g = \sigma : \mathbb{Z} \to \mathbb{Z}$$

denote the bijection whereby $\sigma(z) = z + 1$ for $z \in \mathbb{Z}$. Let A denote the collection of all permutations in $\tau \in G$ such that $\tau(z) = z$ if $z < 0$.

We claim that $M_G(A)$ does not form a subgroup of G in this case. Letting $\sigma : \mathbb{Z} \to \mathbb{Z}$ be as given above, we have that $\sigma \in M_G(A)$. But is it true that σ^{-1} is in $M_G(A)$?

The mapping $\sigma^{-1} : \mathbb{Z} \to \mathbb{Z}$ is such that $\sigma^{-1}(z) = z - 1$ for all $z \in \mathbb{Z}$. We have that $\sigma^{-1} \in G$, but it is not true that

$$\forall a \in A\ \sigma^{-1}a(\sigma^{-1})^{-1} \in A,$$

since for $z < 0$ and $a \in A$, we have that

$$\sigma^{-1}a\sigma(z) = \sigma a(z + 1),$$

but since $a \in A$ and $z < 0$, it is not necessarily true that "$a(z+1) = z+1$", i.e. it is not necessarily true "$a(-1+1) = -1+1$", so it is not necessarily true that that

$$\sigma^{-1} a \sigma(z) = a.$$

For example, if $a \in A$ is such that

$$a(0) = 31415,$$

then we have that

$$\sigma^{-1} a \sigma(-1) = \sigma^{-1} a(0) = \sigma^{-1}(31415) = 31414.$$

So we have shown that $M_G(A)$ is not necessarily closed under inverses with respect to the underlying binary operation of G, thus proving that $M_G(A)$ is not a subgroup of G.

Exercise 1.37. Show that if G is finite then $N_G(A) = M_G(A)$. Where does the proof fail if G is infinite?

Solution 1.38. The normalizer $N_G(A)$ of a subset A of a group G is almost always defined as

$$N_G(A) = \{g \in G \mid gA = Ag\}$$

or equivalently as

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

This appears to be the standard definition of the normalizer of a subset. Writing

$$M_G(A) := \{g \in G \mid gag^{-1} \in A \text{ for all } a \in A\},$$

we claim that if G is finite, then $M_G(A) = N_G(A)$. So, suppose that G is finite. Letting g be in $N_G(A)$, we have that $gA = Ag$. So for all a in A, we have that $ga = (a')g$ for some a' in A. So, for all a in A, gag^{-1} is in A. So, $N_G(A)$ is a subset of $M_G(A)$. Conversely, let g be in $M_G(A)$. So for all a in A, gag^{-1} is in A. So, for all a in A, $ga = (a'')g$ for some a'' in A. This just shows that gA is contained in Ag. But since G is finite, we know that $|gA| = |Ag|$. This is easily seen bijectively. But since $gA \subseteq Ag$, and since $|gA| = |Ag|$, and since G is finite, we may thus deduce that $gA = Ag$. But then g must be in $N_G(A)$, thus completing our proof.

Now, observe that if G is infinite, it is still true that $N_G(A) \subseteq M_G(A)$, since if $g \in N_G(A)$, $ga = (a')g$ for some a' in A, so gag^{-1} is in A for all a in A. But for the infinite group G, the above proof fails in its latter part in the following sense. For g in $M_G(A)$, we have that: for all a in A, gag^{-1} is in A. So, for all a in A, $ga = (a'')g$ for some a'' in A. But this just shows that gA is contained in Ag. Using the previous exercise, it is easily seen that it is not in general true that $gA \subseteq Ag$ implies $gA = Ag$, given that G is infinite. Since it is not in general true that $gA \subseteq Ag$ implies $gA = Ag$, we thus have that g may or may not be in $N_G(A)$, so $M_G(A)$ may or may not be contained in $N_G(A)$, given that G is infinite.

Exercise 1.39. Show that $C_G(A) \leq N_G(A) \leq G$.

Solution 1.40. We are using the definition of the normalizer of a subset whereby $N_G(A) = \{g \in G \mid gA = Ag\}$. Since $eA = Ae$, we thus have that $N_G(A)$ is nonempty.

Now let $g, h \in G$ be such that $gA = Ag$ and $hA = Ah$ so that g and h are arbitrary elements in $N_G(A)$. Consider the expression ghA:

$$ghA = \{gha \ : \ a \in A\}.$$

Now, let $a \in A$ be arbitrary, so that gha is an arbitrary element in ghA. Since $hA = Ah$, we have that

$$ha = a'h$$

for some $a' \in A$, and we thus have that

$$gha = g(a')h.$$

Since $gA = Ag$, we have that

$$ga' = a''g$$

for some $a'' \in A$. Therefore,

$$gha = a''gh \in Agh.$$

We thus have that

$$ghA \subseteq Agh.$$

An obvious symmetric argument may be used to prove the reverse inclusion

$$ghA \supseteq Agh.$$

We thus have that $N_G(A)$ is closed with respect to the underlying binary operation of G.

As above, let $g \in N_G(A)$ be arbitrary. We thus have that $gA = Ag$. Now let $a \in A$ be arbitrary. So

$$ga = a'g$$

for some $a' \in A$. Therefore,

$$ag^{-1} = g^{-1}a'$$

for some $a' \in A$. This shows that each element in Ag^{-1} is in $g^{-1}A$. An obvious symmetric argument may be used to prove the reverse inclusion whereby

$$Ag^{-1} \supseteq g^{-1}A.$$

By the Two-Step Subgroup Test, we thus have that $N_G(A) \leq G$ as desired.

Now recall that the centralizer $C_G(A)$ of A is given as follows:

$$C_G(A) = \{g \in G \mid \forall a \in A \ ag = ga\}.$$

Now let $g \in G$ be such that $\forall a \in A \ ag = ga$, so that g is an arbitrary element in $C_G(A)$. Then it is clear that

$$gA = \{ga \ : \ a \in a\} = \{ag \ : \ a \in a\} = Ag,$$

thus proving that $C_G(A) \subseteq N_G(A)$. Also observe that $C_G(A)$ is nonempty $ae = ea$ for $a \in A$.

Now let $g, h \in C_G(A)$ be arbitrary, and let $a \in A$ be arbitrary. Since $h \in C_G(A)$, we have that

$$ha = ah,$$

and we thus have that

$$gha = gah$$

Since $g \in C_G(A)$, from the equality $gha = gah$, we thus obtain the equality

$$(gh)\,a = a\,(gh)\,,$$

thus proving that $C_G(A)$ is closed under the underlying binary operation of the subgroup $N_G(A)$.

Again let $g \in C_G(A)$ be arbitrary, and again let $a \in A$ be arbitrary. From the equality

$$ga = ag$$

we obtain the equality

$$ag^{-1} = g^{-1}a,$$

thus proving that $C_G(A)$ is closed with respect to inverses. We thus have that

$$C_G(A) \leq N_G(A) \leq G$$

as desired.

Exercise 1.41. State and prove the four isomorphism theorems for groups.

Solution 1.42. The First Isomorphism Theorem for groups may be formulated in the following manner.

The First Isomorphism Theorem: Let H and G be groups. Then for a morphism $\phi\colon G \to H$, we have that $\ker(\phi) \trianglelefteq G$, and furthermore, we have that $G/\ker(\phi) \cong \mathrm{im}(\phi)$.

Proof: We have proven in a previous exercise that $\ker(\phi) \trianglelefteq G$. As suggested in class, to prove the First Isomorphism Theorem, one may use the canonical morphism

$$\psi_\phi = \psi\colon G/\ker(\phi) \to \mathrm{im}(\phi)$$

given by the mapping $g\ker(\phi) \mapsto \phi(g)$ for a coset $g\ker(\phi)$ in the domain of ψ, with $g \in G$. To prove the First Isomorphism Theorem using this canonical morphism, one must show that ψ is a well-defined, bijective, group homomorphism.

Letting $g \in G$, so that $g\ker(\phi)$ is an arbitrary element in the domain of ψ, we have that

$$\psi(g\ker(\phi)) = \phi(g),$$

and $\phi(g) \in \mathrm{im}(\phi)$ since $\phi\colon G \to H$. The mapping ψ is well-defined in the sense that $\psi(d)$ is in the given codomain of ψ for each element d in the comain of ψ. But we also must prove that ψ is well-defined in the sense that an expression of the form $\psi(d)$ does not depend on a given coset representative for an element d in the domain of ψ.

So, let $g, h \in G$, so that $g\ker(\phi)$ and $h\ker(\phi)$ are elements in the domain $G/\ker(\phi)$ of $\psi_\phi = \psi$. Now, suppose that $g\ker(\phi) = h\ker(\phi)$. To prove that ψ is well-defined, it thus remains to prove that $\psi(g\ker(\phi)) = \psi(h\ker(\phi))$.

Now, under the above assumption whereby $g\ker(\phi) = h\ker(\phi)$, since $e \in \ker(\phi)$, we may thus deduce that

$$ge = hk$$

for some element $k \in \ker(\phi)$. We thus have that

$$g = hk$$

for some element $k \in \ker(\phi)$. Now apply the morphism $\phi\colon G \to H$ to both sides of the equality $g = hk$:

$$\begin{aligned} g = hk &\Longrightarrow \phi(g) = \phi(hk) \\ &\Longrightarrow \phi(g) = \phi(h)\,\phi(k) \\ &\Longrightarrow \phi(g) = \phi(h)\,e \\ &\Longrightarrow \phi(g) = \phi(h) \\ &\Longrightarrow \psi(g\ker(\phi)) = \psi(h\ker(\phi)). \end{aligned}$$

So we have shown that

$$g\ker(\phi) = h\ker(\phi) \Longrightarrow \psi(g\ker(\phi)) = \psi(h\ker(\phi))$$

for cosets $g\ker(\phi)$ and $h\ker(\phi)$ in the domain $G/\ker(\phi)$ of $\psi_\phi = \psi$, thus concluding our proof that ψ is well-defined.

We claim that ψ is injective. Again letting $g, h \in G$, we have that:

$$\begin{aligned} \psi(g\ker(\phi)) = \psi(h\ker(\phi)) &\Longrightarrow \phi(g) = \phi(h) \\ &\Longrightarrow \phi(g)\left(\phi(h)\right)^{-1} = e_H = e \\ &\Longrightarrow \phi(g)\phi(h^{-1}) = e \\ &\Longrightarrow \phi(g \cdot (h^{-1})) = e \\ &\Longrightarrow g \cdot (h^{-1}) \in \ker(\phi) \\ &\Longrightarrow \exists k \in \ker(\phi)\ g \cdot (h^{-1}) = k \\ &\Longrightarrow \exists k \in \ker(\phi)\ g = k \cdot h. \end{aligned}$$

Now, using the fact that $\ker(\phi)$ is a normal subgroup, we have that $(\ker(\phi))\,h = h\,(\ker(\phi))$. Since there exists an element k in $\ker(\phi)$ such that $g = k \cdot h$, and since $(\ker(\phi))\,h = h\,(\ker(\phi))$, we may deduce that there exists an element $\ell \in \ker(\phi)$ such that $g = h \cdot \ell$. So for $m \in \ker(\phi) \trianglelefteq G$, we have that

$$g \cdot m = h \cdot (\ell \cdot m) \in h\,(\ker(\phi)),$$

and we thus have that each element $g \cdot m$ in $g\,(\ker(\phi))$ is in $h\,(\ker(\phi))$, thus proving the following inclusion:

$$g\ker(\phi) \subseteq h\ker(\phi).$$

We have already shown that:

$$\psi(g\ker(\phi)) = \psi(h\ker(\phi)) \Longrightarrow \exists k \in \ker(\phi)\ g = k \cdot h.$$

Under the assumption that $\psi(g\ker(\phi)) = \psi(h\ker(\phi))$, we thus have that there exists an element k^{-1} in $\ker(\phi)$ such that

$$h = k^{-1}g.$$

Note that we are using the fact that $\ker(\phi)$ forms a subgroup of the domain of ϕ in the sense that we are using the fact that $\ker(\phi)$ must be closed under inverses. From the equality

$$h = k^{-1}g,$$

it is easily seen that

$$g\ker(\phi) \supseteq h\ker(\phi)$$

by repeating the above argument which was used to prove that

$$(\exists k \in \ker(\phi)\ g = k \cdot h) \Longrightarrow g\ker(\phi) \subseteq h\ker(\phi).$$

By mutual inclusion, we thus have that

$$\psi(g\ker(\phi)) = \psi(h\ker(\phi)) \Longrightarrow g\ker(\phi) = h\ker(\phi),$$

thus proving the injectivity ψ.

So, we have thus far shown that ψ is a well-defined injective mapping from $G/\ker(\phi)$ to $\mathrm{im}(\phi)$. Now, let $g \in G$, so that $\phi(g)$ is an arbitrary element in the codomain $\mathrm{im}(\phi)$ of ψ. Since

$$\psi(g\ker(\phi)) = \phi(g) \in \mathrm{im}(\phi),$$

it is thus clear that ψ is surjective.

So, we have thus far shown that ψ is well-defined and bijective. It thus remains to prove that ψ is a group homomorphism. Again let $g, h \in G$, so that the left cosets $g\ker(\phi)$ and $h\ker(\phi)$ are arbitrary elements in the domain $G/\ker(\phi)$ of $\psi_\phi = \psi$. Now consider the evaluation of ψ at the product $(g\ker(\phi)) \cdot (h\ker(\phi))$:

$$\begin{aligned}\psi\left((g\ker(\phi)) \cdot (h\ker(\phi))\right) &= \psi\left((g \cdot h)\ker(\phi)\right)\\ &= \phi(g \cdot h)\\ &= \phi(g) \cdot \phi(h)\\ &= \psi(g\ker(\phi)) \cdot \psi(h\ker(\phi)).\end{aligned}$$

We thus have that

$$\psi_\phi = \psi \colon G/\ker(\phi) \to \mathrm{im}(\phi)$$

is a well-defined, bijective group homomorphism, thus proving that $G/\ker(\phi) \cong \mathrm{im}(\phi)$. □

The Second Isomorphism Theorem may be formulated in the following manner:

The Second Isomorphism Theorem: Let G be a group, and let $H, K \leq G$ be such that $H \leq N_G(K)$. Then $H \cap K \trianglelefteq H$, and $HK/K \cong H/(H \cap K)$.

Proof: We begin by defining a mapping

$$\tau \colon H \to HK/K$$

whereby $h \mapsto hK$ for $h \in H$.

We claim that τ is a group homomorphism. To show this, we begin be demonstrating that HK forms a subgroup of G. Let $h_1, h_2 \in H$ and let $k_1, k_2 \in K$, so that h_1k_1 and h_2k_2 are arbitrary elements in HK. Consider the product

$$h_1k_1h_2k_2.$$

Now, since $H \leq N_G(K)$. We thus have that $hK = Kh$ for all $h \in H$. In particular, we have that $k_1h_2 = h_2k_3$ for some element k_3 in K. We thus have that

$$h_1k_1h_2k_2 = h_1\left(k_1h_2\right)k_2 = h_1\left(h_2k_3\right)k_2 = \left(h_1h_2\right)\left(k_3k_2\right) \in HK,$$

thus proving that the product HK is closed with respect to the underlying binary operation of G. Similarly, since $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1}$, and since $hK = Kh$ for all $h \in H$, we thus have that

$$k_1^{-1}h_1^{-1} = h_3k_1^{-1} \in HK,$$

thus effectively proving that $HK \leq G$.

Moreover, we claim that $K \trianglelefteq HK$. Consider the coset k_1HK. But recall that $hK = Kh$ for all $h \in H$. Given an element

$$k_1h_1k_2 \in k_1HK$$

in the left coset k_1HK, we have that

$$k_1h_1k_2 = h_1k_3k_2 = h_1\left(k_3k_2k_1^{-1}\right)k_1 \in HKk_1$$

for some $k_3 \in K$, thus proving the inclusion whereby

$$k_1HK \subseteq HKk_1.$$

Conversely, given an element

$$h_1k_2k_1 \in HKk_1,$$

we have that

$$h_1k_2k_1 = h_1k_3 = k_4h_1 = k_1\left(k_1^{-1}k_4\right)h_1 = k_1k_5h_1 = k_1h_1k_6 \in k_1HK,$$

the proving the reverse inclusion whereby

$$k_1HK \supseteq HKk_1.$$

We thus have that $K \trianglelefteq HK$ as desired.

So, we have shown that the given codomain

$$\operatorname{cod}(\tau) = HK/K$$

of the mapping $\tau\colon H \to HK/K$ forms a group, in the sense that $K \trianglelefteq HK$.

To prove that τ is a group homomorphism, begin by letting $h_1, h_2 \in H$. Consider the expression $\tau(h_1h_2)$:

$$\tau(h_1h_2) = (h_1h_2)K.$$

We have shown that $K \trianglelefteq HK$. We thus have that

$$\tau(h_1h_2) = h_1h_2K = (h_1K)(h_2K) = \tau(h_1\tau(h_2)),$$

thus proving that τ is a group homomorphism.

Now consider the kernel of the group homomorphism $\tau\colon H \to HK/K$:

$$\begin{aligned}\ker(\tau) &= \{h_1 \in H : \tau(h_1) = K\} \\ &= \{h_1 \in H : h_1K = K\}.\end{aligned}$$

We claim that the above set is equal to $H \cap K$. Letting $x \in H \cap K$, we have that $x \in H$, and we have that

$$xK = K$$

since $x \in K$, thus proving the inclusion whereby:

$$H \cap K \subseteq \ker(\tau).$$

Conversely, let $h_1 \in H$ be such that $h_1 K = K$. Since $e \in K$, we thus have that $h_1 e = k$ for some $k \in K$, and we thus have that $h_1 = k$ for some $k \in K$. So it is clear that $h_1 \in H \cap K$, thus proving the desired inclusion given below:

$$H \cap K \supseteq \ker(\tau).$$

We thus have that

$$\ker(\tau) = H \cap K,$$

as desired.

So, since

$$\tau \colon H \to HK/K$$

is a group homomorphism whereby

$$\ker(\tau) = H \cap K,$$

by the First Isomorphism Theorem, we thus have that:

$$H/\left(H \cap K\right) \cong \operatorname{im}\left(\tau\right).$$

We claim that τ is surjective. To show this, let $h_1 \in H$ and $k_1 \in K$, so that $h_1 k_1 K$ is an arbitrary element in the codomain

$$\operatorname{cod}(\tau) = HK/K$$

of τ. It is clear that $h_1 k_1 K = h_1 K$. We thus have that

$$\tau(h_1) = h_1 K = h_1 k_1 K \in HK/K,$$

thus proving the surjectivity of τ. So, by the First Isomorphism Theorem, we thus have that

$$H/\left(H \cap K\right) \cong HK/K$$

as desired. □

The Third Isomorphism Theorem may be formulated in the following manner:

The Third Isomorphism Theorem: Let G be a group and let $H, K \trianglelefteq G$, with $H \trianglelefteq K$. Then K/H is normal in G/H, and furthermore, we have that $(G/H)/(K/H) \cong G/K$.

Proof: Define $\gamma \colon G/H \to G/K$ so that

$$\gamma(gH) = gK$$

for each coset gH in the domain of γ. We begin by showing that γ is a well-defined group homomorphism. To show that γ is well-defined, begin by letting $g_1, g_2 \in G$, and suppose that $g_1 H = g_2 H$. Let $k_1 \in K$ be arbitrary, so that $g_1 \cdot k_1$ is an arbitrary element in $g_1 K$. Since

$$g_1 \cdot e \cdot k_1 = g_1 \cdot k_1,$$

and since $g_1 H = g_2 H$, we have that

$$g_1 \cdot k_1 = g_1 \cdot e \cdot k_1 = g_2 \cdot h_1 \cdot k_1 \in g_2 K$$

for some $h_1 \in H$. An obvious symmetric argument shows that $g_1 K \supseteq g_2 K$. We thus have that γ is well-defined in the sense that

$$g_1 H = g_2 H \Longrightarrow \gamma(g_1 H) = \gamma(g_2 H).$$

Letting g_1 and g_2 be as given above, since $H, K \trianglelefteq G$

$$\begin{aligned}\gamma(g_1H \cdot g_2H) &= \gamma(g_1g_2H)\\ &= g_1g_2K\\ &= g_1K \cdot g_2K\\ &= \gamma(g_1H) \cdot \gamma(g_2H).\end{aligned}$$

We thus have that γ is a group homomorphism. We claim that the kernel of γ is K/H. If gH is in the kernel of γ, where $g \in G$, then $gK = eK = K$. So g must be in K. That is, $gH \in K/H$ since $g \in K$. Conversely, given an element kH in K/H, we have that $\gamma(kH) = kK = K$, and we thus have that kH is in $\ker(\gamma)$. We thus have that $\ker(\gamma) = K/H$ as desired. It is clear that γ is surjective, since for $gK \in G/K$, we have that $\gamma(gH) = gK$, with $gH \in G/H$. So, by the first isomorphism theorem, we have that

$$(G/H)\,/\ker(\gamma) \cong \operatorname{im}(\gamma),$$

and we thus have that

$$(G/H)\,/\,(K/H) \cong G/K,$$

as desired. □

The Fourth Isomorphism Theorem may be formulated in the following manner:

The Fourth Isomorphism Theorem: Let G be a group and let $H \trianglelefteq G$. Then the canonical projection morphism $\pi\colon G \to G/H$ whereby

$$g \mapsto gH$$

induces the bijections indicated below:

$$\begin{aligned}\{K : H \trianglelefteq K \leq G\} &\longleftrightarrow \{\overline{K} : \overline{K} \leq G/H\},\\ \{K : H \trianglelefteq K \trianglelefteq G\} &\longleftrightarrow \{\overline{K} : \overline{K} \trianglelefteq G/H\}.\end{aligned}$$

Let

$$f\colon \{K : H \trianglelefteq K \leq G\} \to \{\overline{K} : \overline{K} \leq G/H\}$$

denote the mapping whereby

$$f(K) = \pi(K) = \{kH : k \in K\} = K/H$$

for a subgroup K of G such that $H \trianglelefteq K$. We claim that f is well-defined in the sense that $f(K)$ is indeed an element in the given codomain of f for $K \in \operatorname{dom}(f)$. Letting $K \in \operatorname{dom}(f)$, we have that $H \trianglelefteq K \leq G$. Since $K \subseteq G$, we have that $K/H \subseteq G/H$, and since $H \trianglelefteq K$, we have that K/H forms a group under the operation $\cdot$ whereby $k_1H \cdot k_2H = (k_1k_2)H$ for $k_1, k_2 \in K$. But furthermore, since $H \trianglelefteq G$, G/H forms a group with respect to the operation $\cdot$ whereby $g_1H \cdot g_2H = (g_1g_2)H$ for $g_1, g_2 \in g$, thus showing that K/H is a subgroup of G/H.

Conversely, consider the mapping

$$f'\colon \{\overline{K} : \overline{K} \leq G/H\} \to \{K : H \trianglelefteq K \leq G\}$$

such that: given an element

$$\overline{K} = \left\{g_1H, g_2H, \ldots, g_{|\overline{K}|}H\right\} \leq G/H$$

in the domain of f', where $g_1, g_2, \ldots, g_{|\overline{K}|} \in G$, we have that

$$f'\left(\overline{K}\right) = \bigcup_{i=1}^{|\overline{K}|} g_i H = \bigcup_{k \in \overline{K}} k.$$

We claim that f' is well-defined in the sense that $f'(\overline{K}) \in \operatorname{cod}(f')$ for $\overline{K} \in \operatorname{dom}(f')$. Again let

$$\overline{K} = \{g_1 H, g_2 H, \ldots, g_{|\overline{K}|} H\} \leq G/H$$

be an element in the domain of f'. We thus have that $f'(\overline{K})$ consists precisely of all expressions of the form $g_i h$ where

$$i \in \left\{1, 2, \ldots, \left|\overline{K}\right|\right\}$$

and $h \in H$. We thus have that $f'(\overline{K}) \subseteq G$. We know that $\overline{K} \leq G/H$, so $g_{i_1} H g_{i_2} H = g_{i_1} g_{i_2} H \in \overline{K}$ for all indices i_1 and i_2. So given elements $h_1, h_2 \in H$, we have that

$$g_{i_1} h_1 g_{i_2} h_2 = g_{i_3} h_3$$

for some index $i_3 \in \{1, 2, \ldots, |\overline{K}|\}$ and some element $h_3 \in H$. We thus have that $f'(\overline{K})$ is closed under the underlying binary operation of G. Similarly, given an index

$$i_1 \in \left\{1, 2, \ldots, \left|\overline{K}\right|\right\},$$

and letting $h_1 \in H$, since $\overline{K} \leq G/H$, we have that

$$(g_{i_1} H)^{-1} = g_{i_2} H \in \overline{K}$$

for some index

$$i_2 \in \left\{1, 2, \ldots, \left|\overline{K}\right|\right\},$$

so

$$g_{i_1} h_1 = g_{i_2} h_2$$

for some $h_2 \in H$, thus proving that $f'(\overline{K}) \leq G$.

Since $\overline{K} \leq G/H$, we have that $eH = H \in \overline{K}$. So it is clear that $H \subseteq f'(\overline{K}) \leq G$. Since $H \leq G$, we have that $H \leq f'(\overline{K}) \leq G$. Given an element

$$g_i h \in g(\overline{K})$$

where $i \in \{1, 2, \ldots, |\overline{K}|\}$ and $h \in H$, since $H \trianglelefteq G$, we have that

$$(g_i h) H = H (g_i h),$$

so it is clear that $H \trianglelefteq f'(\overline{K}) \leq G$. We thus have that $f'(\overline{K}) \in \operatorname{cod}(f')$, as desired, thus proving that f' is well-defined.

Since

$$f\colon \{K : H \trianglelefteq K \leq G\} \to \{\overline{K} : \overline{K} \leq G/H\}$$

and

$$f'\colon \{\overline{K} : \overline{K} \leq G/H\} \to \{K : H \trianglelefteq K \leq G\}$$

are both well-defined, we may thus consider the composition

$$f \circ f' \colon \{\overline{K} : \overline{K} \leq G/H\} \to \{\overline{K} : \overline{K} \leq G/H\}.$$

Let $\overline{K}$ be an element in the domain of f'. As above, write:

$$\overline{K} = \left\{g_1 H, g_2 H, \ldots, g_{|\overline{K}|} H\right\} \leq G/H,$$

where $g_1, g_2, \ldots, g_{|\overline{K}|} \in G$. Now evaluate the expression $(f \circ f')(\overline{K})$ in the following manner:

$$\begin{aligned}
(f \circ f')(\overline{K}) &= f(f'(\overline{K})) \\
&= f\left(\bigcup_{i=1}^{|\overline{K}|} g_i H\right) \\
&= \pi\left(\bigcup_{i=1}^{|\overline{K}|} g_i H\right) \\
&= \pi\left(g_1 H \uplus g_2 H \uplus \cdots \uplus g_{|\overline{K}|} H\right) \\
&= \pi\left(g_1 H\right) \uplus \pi\left(g_2 H\right) \uplus \cdots \uplus \pi\left(g_{|\overline{K}|} H\right) \\
&= \pi\left(\{g_1 h : h \in H\}\right) \uplus \pi\left(\{g_2 h : h \in H\}\right) \uplus \cdots \uplus \pi\left(\left\{g_{|\overline{K}|} h : h \in H\right\}\right) \\
&= \{g_1 h H : h \in H\} \uplus \{g_2 h H : h \in H\} \uplus \cdots \uplus \left\{g_{|\overline{K}|} h H : h \in H\right\} \\
&= \{g_1 H\} \uplus \{g_2 H\} \uplus \cdots \uplus \left\{g_{|\overline{K}|} H\right\} \\
&= \left\{g_1 H, g_2 H, \ldots, g_{|\overline{K}|} H\right\} \\
&= \overline{K}.
\end{aligned}$$

Conversely, consider the composition

$$f' \circ f \colon \{K : H \trianglelefteq K \leq G\} \to \{K : H \trianglelefteq K \leq G\}.$$

Now, let K be such that $H \trianglelefteq K \leq G$, those that K is an arbitrary element in the domain of the product $f' \circ f$. Since $H \trianglelefteq K$, we have that K/H forms a group. Write

$$K/H = \{k_1 H, k_2 H, \ldots, k_n H\}$$

letting $n \in \mathbb{N}$. Now evaluate the expression $(f' \circ f)(K)$ as follows.

$$\begin{aligned}
(f' \circ f)(K) &= f'(f(K)) \\
&= f'(\pi(K)) \\
&= f'\left(\{kH : k \in K\}\right) \\
&= f'\left(\{k_1 H, k_2 H, \ldots, k_n H\}\right) \\
&= \bigcup_{i=1}^{n} k_i H \\
&= K.
\end{aligned}$$

We thus have that f and f' are inverses of one another. This essentially proves that f is bijective, which proves that

$$\{K : H \trianglelefteq K \leq G\}$$

and

$$\{\overline{K} : \overline{K} \leq G/H\}$$

are bijectively equivalent, as desired. More explicitly, for elements $x_1, x_2 \in \operatorname{dom}(f)$, we have that:

$$\begin{aligned} f(x_1) = f(x_2) &\implies f'(f(x_1)) = f'(f(x_2)) \\ &\implies (f' \circ f)(x_1) = (f' \circ f)(x_2) \\ &\implies x_1 = x_2. \end{aligned}$$

We thus have that f is injective. Somewhat similarly, letting $y \in \operatorname{cod}(f)$, we have that:

$$\begin{aligned} y \in \operatorname{cod}(f) &\implies y \in \operatorname{dom}(f') \\ &\implies f'(y) \in \operatorname{cod}(f') \\ &\implies f'(y) \in \operatorname{dom}(f) \\ &\implies \exists z \in \operatorname{dom}(f)\ z = f'(y) \\ &\implies \exists z \in \operatorname{dom}(f)\ f(z) = f(f'(y)) \\ &\implies \exists z \in \operatorname{dom}(f)\ f(z) = (f \circ f')(y) \\ &\implies \exists z \in \operatorname{dom}(f)\ f(z) = y. \end{aligned}$$

We thus have that f is surjective, as desired.

We apply a similar strategy to show that $\{K : H \trianglelefteq K \trianglelefteq G\}$ and $\{\overline{K} : \overline{K} \trianglelefteq G/H\}$ are bijectively equivalent.

We have already shown that

$$f\colon \{K : H \trianglelefteq K \leq G\} \to \{\overline{K} : \overline{K} \leq G/H\}$$

is bijective. Now, observe that the set

$$\{K : H \trianglelefteq K \leq G\}$$

is contained in the set

$$\{K : H \trianglelefteq K \trianglelefteq G\}.$$

Similarly, the set

$$\{\overline{K} : \overline{K} \leq G/H\}$$

is contained in the set

$$\{\overline{K} : \overline{K} \trianglelefteq G/H\}.$$

Now, let f denote the mapping obtained by restricting the domain of f to $\{K : H \trianglelefteq K \trianglelefteq G\}$. Since f is injective, we have that f is injective. Now, let K be such that $H \trianglelefteq K \trianglelefteq G$. Since $H \trianglelefteq K \leq G$, we have that $\pi(K) \leq G/H$, since f is well-defined. We claim that $\pi(K) \trianglelefteq G/H$. We know that $gK = Kg$ for all $g \in G$. It remains to prove that

$$(gH)\{kH : k \in K\} = \{kH : k \in K\}(gH)$$

for all $g \in G$. Since

$$(gH)\{kH : k \in K\} = \{gHkH : k \in K\} = \{(gk)H : k \in K\},$$

and since $gK = Kg$ for all $g \in G$, we have that

$$(gH)\{kH : k \in K\} = \{(kg)H : k \in K\} = \{kHgH : k \in K\} = \{kH : k \in K\}(gH),$$

thus proving that $\pi(K) \trianglelefteq G/H$, as desired. So, we know that the mapping

$$\mathsf{f} = f\Big|_{\{K:H\trianglelefteq K\trianglelefteq G\}} : \{K : H \trianglelefteq K \trianglelefteq G\} \to \{\overline{K} : \overline{K} \leq G/H\}$$

obtained by restricting the domain of f to the subset

$$\{K : H \trianglelefteq K \trianglelefteq G\} \subseteq \{K : H \trianglelefteq K \leq G\}$$

is injective. But furthermore, we have shown that if K is such that $H \trianglelefteq K \trianglelefteq G$, then $f(K) \trianglelefteq G/H$. That is,

$$K \in \operatorname{dom}(\mathsf{f}) \Longrightarrow \mathsf{f}(K) \in \{\overline{K} : \overline{K} \trianglelefteq G/H\}.$$

We thus have that the image of f is contained in $\{\overline{K} : \overline{K} \trianglelefteq G/H\}$. Now let

$$\mathsf{g} : \{K : H \trianglelefteq K \trianglelefteq G\} \to \{\overline{K} : \overline{K} \trianglelefteq G/H\}$$

denote the mapping obtained by restricting the codomain of f to $\{\overline{K} : \overline{K} \trianglelefteq G/H\}$. Since f is injective, we have that g is injective. We claim that g is also surjective. Let

$$\{k_1, k_2, \ldots, k_n\} \subseteq G$$

be such that

$$\{k_1H, k_2H, \ldots, k_nH\} \trianglelefteq G/H,$$

so that the collection $\{k_1H, k_2H, \ldots, k_nH\}$ is an arbitrary element in the codomain of g. Consider the union

$$\bigcup_{i=1}^{n} k_iH \subseteq G.$$

Given two elements $k_{i_1}h_1$ and $k_{i_2}h_2$ in the above union, since

$$k_{i_1}Hk_{i_2}H = k_{i_1}k_{i_2}H$$

we have that

$$k_{i_1}h_1k_{i_2}h_2 = k_{i_1}k_{i_2}h_3 \in \bigcup_{i=1}^{n} k_iH$$

for some element $h_3 \in H$. We thus have that $\bigcup_{i=1}^{n} k_iH$ is closed with respect to the underlying multiplicative binary operation of G. Similarly, since

$$(k_{i_1}H)^{-1} = k_{i_4}H$$

for some index i_4, it is clear that

$$\bigcup_{i=1}^{n} k_iH \leq G.$$

But since H is also a subgroup of G, it is clear that:

$$H \leq \bigcup_{i=1}^{n} k_iH \leq G.$$

Since

$$\{k_1H, k_2H, \dots, k_nH\} \trianglelefteq G/H,$$

we have that

$$gH\{k_1H, k_2H, \dots, k_nH\} = \{k_1H, k_2H, \dots, k_nH\}gH$$

for all $g \in G$. To prove that

$$\bigcup_{i=1}^{n} k_iH \trianglelefteq G,$$

it remains to prove that

$$g\bigcup_{i=1}^{n} k_iH = \left(\bigcup_{i=1}^{n} k_iH\right)g$$

for all $g \in G$. Let $g \in G$ be arbitrary. Letting $gk_{i_1}h_1$ be an arbitrary element in $g\bigcup_{i=1}^{n} k_iH$, since

$$gHk_{i_1}H = k_{i_2}HgH = (k_{i_2}H)(Hg) = k_{i_2}Hg,$$

we have that

$$g\bigcup_{i=1}^{n} k_iH \subseteq \left(\bigcup_{i=1}^{n} k_iH\right)g,$$

and a symmetric argument may be used to prove the reverse inclusion. Similarly, it is clear that

$$H \trianglelefteq \bigcup_{i=1}^{n} k_iH,$$

since $k_{i_1}h_1H = Hk_{i_1}h_1$ since $H \trianglelefteq G$. So, we have thus far shown that

$$H \trianglelefteq \bigcup_{i=1}^{n} k_iH \trianglelefteq G.$$

So, given that

$$\{k_1H, k_2H, \dots, k_nH\} \trianglelefteq G/H,$$

we have that:

$$\bigcup_{i=1}^{n} k_iH \in \mathrm{dom}(\mathsf{g}).$$

Now evaluate the expression

$$\mathsf{g}\left(\bigcup_{i=1}^{n} k_iH\right)$$

as follows:

$$\begin{aligned} \mathsf{g}\left(\bigcup_{i=1}^{n} k_iH\right) &= \pi\left(\bigcup_{i=1}^{n} k_iH\right) \\ &= \{k_ihH : i \in \{1, 2, \dots, n\}, h \in H\} \\ &= \{k_iH : i \in \{1, 2, \dots, n\}\} \\ &= \{k_1H, k_2H, \dots, k_nH\} \trianglelefteq G/H. \end{aligned}$$

We thus have that the mapping

$$\mathsf{g}\colon \{K : H \trianglelefteq K \trianglelefteq G\} \to \{\overline{K} : \overline{K} \trianglelefteq G/H\}$$

is bijective, thus completing our proof.

Exercise 1.43. Recall that A_n is simple for $n \geq 5$. However, it is not true that A_4 is a simple group. Prove that A_4 is not a simple group using a counterexample, and write out all 12 elements in A_4.

Solution 1.44. We defined the alternating group A_n using permutation matrices in class. This group also may be defined as the group under composition consisting of all even permutations in S_n. With respect to the definition of A_n given in class, we have that A_n consists precisely of the following 12 matrices:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

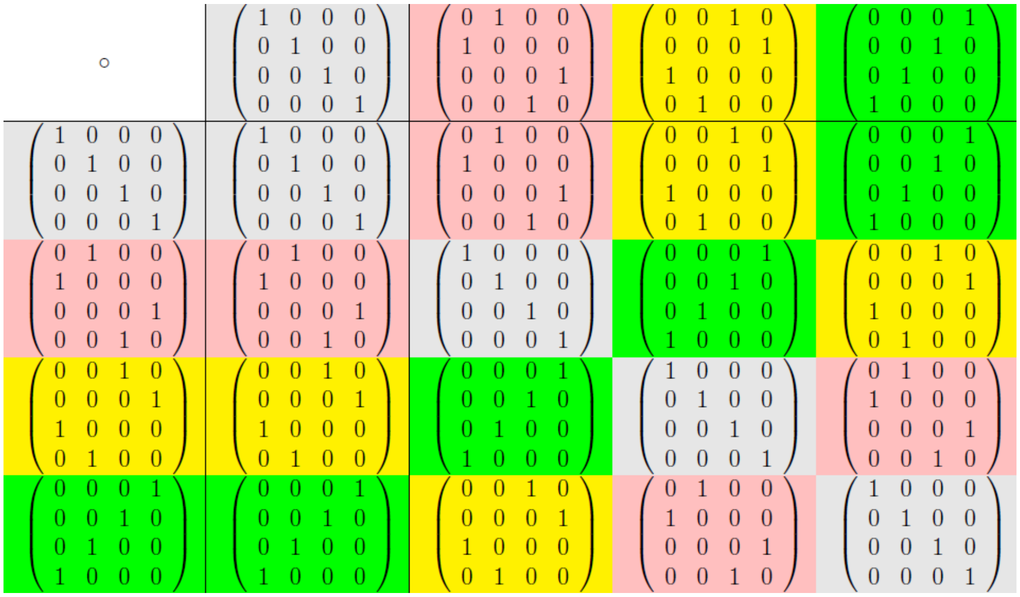
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

We claim that there is a normal subgroup of A_4 which is isomorphic to the Klein four-group $C_2 \times C_2$. Consider the following multiplication table.



$\circ$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$
$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$
$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$
$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$
$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$

Let H denote the subset of A_4 consisting of the matrices illustrated in the above multiplication table. From the above multiplication table, it is clear that H forms a subgroup of A_4, and that H is isomorphic to the Klein four-group $C_2 \times C_2$.

Our strategy to prove that $H \trianglelefteq A_4$ is simply to use a "brute-force" computational approach, by computationally verifying that $aH = Ha$ for $a \in A_4$. A Mathematica program which may be used for these computations is illustrated below.

```
row1 = {1, 0, 0, 0} ;
row2 = {0, 1, 0, 0} ;
row3 = {0, 0, 1, 0} ;
row4 = {0, 0, 0, 1} ;
rowlist = {row1, row2, row3, row4} ;

permutation = Permutations[{1, 2, 3, 4}][[24]] ;

testmatrix1 = {rowlist[[permutation[[1]]]],
 rowlist[[permutation[[2]]]], rowlist[[permutation[[3]]]],
 rowlist[[permutation[[4]]]]} ;

groupelement1 = {rowlist[[1]], rowlist[[2]], rowlist[[3]],
 rowlist[[4]]} ;
groupelement2 = {rowlist[[2]], rowlist[[1]], rowlist[[4]],
 rowlist[[3]]} ;
groupelement3 = {rowlist[[3]], rowlist[[4]], rowlist[[1]],
 rowlist[[2]]} ;
groupelement4 = {rowlist[[4]], rowlist[[3]], rowlist[[2]],
 rowlist[[1]]} ;

Print[Sort[{testmatrix1.groupelement1 // MatrixForm,
 testmatrix1.groupelement2 // MatrixForm,
 testmatrix1.groupelement3 // MatrixForm,
 testmatrix1.groupelement4 // MatrixForm}]] ;
Print[Sort[{groupelement1.testmatrix1 // MatrixForm,
 groupelement2.testmatrix1 // MatrixForm,
 groupelement3.testmatrix1 // MatrixForm,
 groupelement4.testmatrix1 // MatrixForm}]] ;

If[Signature[permutation] == 1,
 Print[Sort[{testmatrix1.groupelement1, testmatrix1.groupelement2,
 testmatrix1.groupelement3, testmatrix1.groupelement4}] ==
 Sort[{groupelement1.testmatrix1, groupelement2.testmatrix1,
 groupelement3.testmatrix1, groupelement4.testmatrix1}]] ;,
 Print["The given permutation must be even."]]
```

Using the above program, we obtain the following computational results which show that $\forall a \in A \; aH = Ha$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} H = H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} H = H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} H = H \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$

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

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} H = H \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} =$$

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

Exercise 1.45. Let G be a group, and suppose that there exists a nontrivial proper normal subgroup N of G. So, there is a composition series for N and G/N, as illustrated below:

$$\boxed{\begin{array}{lccccccccccc} \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_\ell = & N & \trianglelefteq & H_{\ell+1} & \trianglelefteq & H_{\ell+2} & \trianglelefteq & \cdots & \trianglelefteq & G \\ & \updownarrow & & \updownarrow & & \updownarrow & & & & \updownarrow \\ & N/N & \trianglelefteq & \overline{H}_{\ell+1} & \trianglelefteq & \overline{H}_{\ell+2} & \trianglelefteq & \cdots & \trianglelefteq & G/N \end{array}}$$

By the fourth isomorphism theorem, we have that there is a bijection between the set of expressions of the form $\overline{H}_{\ell+i} \trianglelefteq G/N$ and the set of expressions of the form $H_{\ell+i} \trianglelefteq G$. If $\overline{H}_{\ell+i} \trianglelefteq G/N$, then $H_{\ell+i} \trianglelefteq G$. Check that since $\overline{H}_{\ell+i} \trianglelefteq \overline{H}_{\ell+i+1}$ then $H_{\ell+i} \trianglelefteq H_{\ell+i+1}$.

Solution 1.46. We know that the canonical projection morphism

$$\pi : G \to G/N$$

whereby

$$g \mapsto gN$$

induces the bijection indicated below:

$$\{K : N \trianglelefteq K \trianglelefteq G\} \longleftrightarrow \{\overline{K} : \overline{K} \trianglelefteq G/N\}.$$

Now suppose that $\overline{H}_{\ell+i} \trianglelefteq \overline{H}_{\ell+i+1} \trianglelefteq G/N$. Write

$$\overline{H}_{\ell+i} = \{g_1N, g_2N, \dots, g_nN\}.$$

Note that cosets of N must all be of the same cardinality. Write:

$$\overline{H}_{\ell+i+1} = \{h_1N, h_2N, \dots, h_nN\}.$$

We thus have that

$$H_{\ell+i} = \bigcup_{i=1}^{n} g_iN$$

and

$$H_{\ell+i+1} = \bigcup_{i=1}^{n} h_iN,$$

since the projection morphism π induces bijections according according to the Fourth Isomorphism Theorem. Since

$$\overline{H}_{\ell+i} \trianglelefteq \overline{H}_{\ell+i+1},$$

we have that

$$h_iN\{g_1N, g_2N, \dots, g_nN\} = \{g_1N, g_2N, \dots, g_nN\}h_iN$$

for all indices i. So, given an element

$$h_{i_1}n_1 \in h_{i_1}N \subseteq H_{\ell+i+1}$$

and an element

$$g_{i_2}n_2 \in g_{i_2}N \subseteq H_{\ell+i},$$

we have that

$$h_{i_1}n_1g_{i_2}n_2 \in h_{i_1}n_1H_{\ell+i},$$

i.e., $h_{i_1}n_1g_{i_2}n_2$ is an arbitrary element in $h_{i_1}n_1H_{\ell+i}$. But since

$$h_iN\{g_1N, g_2N, \dots, g_nN\} = \{g_1N, g_2N, \dots, g_nN\}h_iN$$

for all indices i, we have that

$$h_{i_1}n_1g_{i_2}n_2 = g_{i_3}n_3h_{i_1}n_4$$

for some index i_3, and some elements $n_3, n_4 \in N$. Rewrite this equality as

$$h_{i_1}n_1g_{i_2}n_2 = g_{i_3}n_3h_{i_1}n_1n_1^{-1}n_4.$$

Since $N \trianglelefteq G$, we have that

$$h_{i_1}n_1g_{i_2}n_2 = g_{i_3}n_3n_5h_{i_1}n_1$$

for some $n_5 \in N$, and we thus have that

$$(h_{i_1}n_1)g_{i_2}n_2 = g_{i_3}n_6(h_{i_1}n_1)$$

for some $n_6 \in N$. So, for an arbitrary element

$$h_{i_1} n_1 g_{i_2} n_2 \in (h_{i_1} n_1) H_{\ell+i},$$

we thus have that

$$(h_{i_1} n_1) g_{i_2} n_2 = g_{i_3} n_6 (h_{i_1} n_1) \in H_{\ell+i} (h_{i_1} n_1),$$

thus proving the inclusion whereby

$$(h_{i_1} n_1) H_{\ell+i} \subseteq H_{\ell+i} (h_{i_1} n_1).$$

A symmetric argument may be used to prove the reverse inclusion, in order to prove that $H_{\ell+i} \trianglelefteq H_{\ell+i+1}$.

Exercise 1.47. State the Jordan-Hölder theorem, and write a sketch of a proof of this theorem, by filling in the details of the proof sketch of this theorem given in class.

Solution 1.48. The Jordan-Hölder theorem states that any two composition series of a given group are equivalent in the sense that they have the same composition length and the same composition factors, up to permutation and isomorphism. Recall that a subnormal series of a group G is a finite sequence of the following form:

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

Recall that a subnormal series

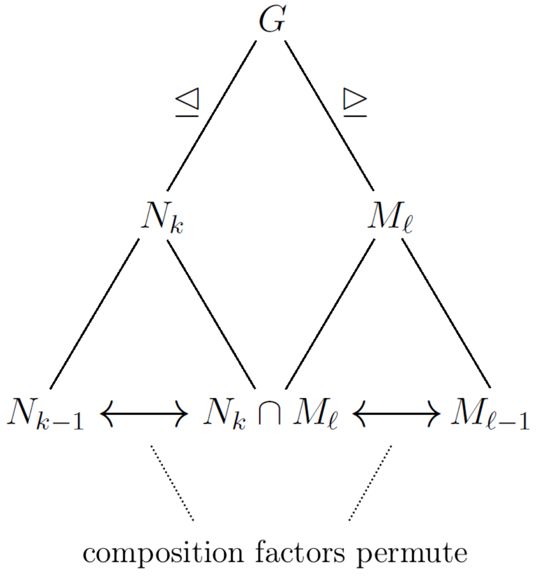
$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

of a group G is a composition series if all the factor groups H_{i+1}/H_i are simple.

Letting G be a finite group, assume that there are two composition series for G:

$$\begin{array}{ccccccccc}
\{1\} = N_0 & \trianglelefteq & N_1 & \trianglelefteq & \cdots & \trianglelefteq & N_k & \trianglelefteq & N_{k+1} \\
 & & & & & & & & \shortparallel \\
 & & & & & & & & G \\
 & & & & & & & & \shortparallel \\
\{1\} = M_0 & \trianglelefteq & M_1 & \trianglelefteq & \cdots & \trianglelefteq & M_\ell & \trianglelefteq & M_{\ell+1}
\end{array}$$

We want to show that the above composition factors are permuted. We may assume without loss of generality that $M_\ell \neq N_k$. To prove that the composition factors given by each of the above series are permutations of each other, we make use of an inductive approach, illustrated by the following diagram.



We need to verify that $N_k \cap M_\ell \trianglelefteq N_k$ and that $N_k \cap M_\ell \trianglelefteq M_\ell$.

To verify this, we apply the Second Isomorphism Theorem.

Recall that the Second Isomorphism Theorem may be formulated in the following manner.

The Second Isomorphism Theorem: Let G be a group, and let $H, K \leq G$ be such that $H \leq N_G(K)$. Then $H \cap K \trianglelefteq H$, and $HK/K \cong H/(H \cap K)$.

By the Second Isomorphism Theorem, since $N_k, M_\ell \leq G$, to prove that $N_k \cap M_\ell \trianglelefteq N_k$, it suffices to prove that $N_k \leq N_G(M_\ell)$, i.e.,

$$N_k \leq \{g \in G : gM_\ell = M_\ell g\}.$$

But since $M_\ell \trianglelefteq G$, we have that

$$\forall g \in G \; gM_\ell = M_\ell g,$$

and we thus have that

$$N_G(M_\ell) = \{g \in G : gM_\ell = M_\ell g\} = G,$$

so since $N_k \leq G$, we thus have that $N_k \leq N_G(M_\ell)$, as desired. An identical argument may be used to prove that $N_k \cap M_\ell \trianglelefteq M_\ell$.

So, by the Second Isomorphism Theorem, we have that:

$$N_k/(N_k \cap M_\ell) \cong N_k M_\ell / M_\ell.$$

We need to show that:

(i) $N_k M_\ell$ forms a subgroup;

(ii) $N_k M_\ell$ is normal in G; and

(iii) $N_k M_\ell$ contains N_k and M_ℓ.

To show that $N_k M_\ell$ forms a subgroup, we begin by letting $n_1, n_2 \in N_k$ and $m_1, m_2 \in M_\ell$, so that $n_1 m_1$ and $n_2 m_2$ are arbitrary elements in $N_k M_\ell$. Now consider the following expression:

$$n_1 m_1 n_2 m_2.$$

Since $N_k \trianglelefteq G$, we have that

$$m_1 N_k = N_k m_1,$$

and we thus have that

$$n_1 n_3 m_1 m_2 \in N_k M_\ell,$$

for some $n_3 \in N_k$, thus proving that $N_k M_\ell$ is closed with respect to the underlying binary operation of G. Similarly, since

$$(n_1 m_1)^{-1} = m_1^{-1} n_1^{-1},$$

and since $N_k \trianglelefteq G$, we have that

$$(n_1 m_1)^{-1} = n_4 m_1^{-1}$$

for some $n_4 \in N$, thus proving that $N_k M_\ell$ is closed under inverses. We thus have that $N_k M_\ell \leq G$, as desired.

Now, let $g \in G$ be arbitrary. Again let $n_1 \in N_k$ and $m_1 \in M_\ell$, and consider the following expression:

$$gn_1m_1 \in gN_kM_\ell.$$

Since $N_k \trianglelefteq G$, we have that

$$gn_1m_1 = n_2gm_1.$$

Since $M_\ell \trianglelefteq G$, we have that

$$gn_1m_1 = n_2m_2g \in N_kM_\ell g$$

for some $m_2 \in M_\ell$, thus proving the inclusion whereby

$$gN_kM_\ell \subseteq N_kM_\ell g.$$

A symmetric argument may be used to prove the reverse inclusion, in order to prove that $N_kM_\ell \trianglelefteq G$. It is obvious that the product N_kM_ℓ contains both N_k and M_ℓ, since expressions of the form $e_{N_k}m$ are in N_kM_ℓ for $m \in M_\ell$, and expressions of the form $n \cdot e_{M_\ell}$ are in N_kM_ℓ for $n \in N_k$.

Since $N_kM_\ell \trianglelefteq G$, and since N_kM_ℓ contains both N_k and M_ℓ, we thus arrive at the subnormal series given below:

$$N_k \trianglelefteq N_kM_\ell \trianglelefteq G$$
$$M_\ell \trianglelefteq N_kM_\ell \trianglelefteq G.$$

But recall that the subnormal series

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k \trianglelefteq N_{k+1} = G$$

is, in fact, a composition series. We thus have that the quotient group G/N_k is simple. From the subnormal series

$$N_k \trianglelefteq N_kM_\ell \trianglelefteq G,$$

we are thus lead to consider the following quotient groups: N_k/N_k, N_kM_ℓ/N_k, and G/N_k. By the Fourth Isomorphism Theorem, we know that there exists a bijection between normal subgroups of G containing N_k and normal subgroups of G/N_k.

But G/N_k is simple. Since

$$N_kM_\ell/N_k \trianglelefteq G/N_k,$$

we have that N_kM_ℓ/N_k is either trivial or is equal to G/N_k. By the fourth isomorphism theorem, N_kM_ℓ is either equal to G or N_k. Since $N_k \neq M_\ell$ by assumption, we have that $N_kM_\ell = G$.

Using the Second Isomorphism Theorem, we have shown that

$$N_k/(N_k \cap M_\ell) \cong N_kM_\ell/M_\ell.$$

We thus have that:

$$N_k/(N_k \cap M_\ell) \cong G/M_\ell.$$

A symmetric argument shows that:

$$M_\ell/(N_k \cap M_\ell) \cong G/N_k.$$

Inductively, this effectively completes our proof.

Exercise 1.49. Prove that for abelian groups, the composition series is such that the quotient between consecutive terms is given by a prime order.

Solution 1.50. Let G be an abelian group, and let $x \in G$. Let $x \neq e$ be of order n. If n is not prime then $x^{n/p}$ is of order p. We thus have that there exists a subgroup of G of order p. Let

$$\{\langle x^{n/p}\rangle\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G/\langle x^{n/p}\rangle$$

be a composition series for $G/\langle x^{n/p}\rangle$. Inductively, we may assume that the composition factors in the above composition series are all of prime order. By the Fourth Isomorphism Theorem, we know that there is a bijection of the form

$$\{\overline{K} : \overline{K} \trianglelefteq G/\langle x^{n/p}\rangle\} \longleftrightarrow \{K : \langle x^{n/p}\rangle \trianglelefteq K \trianglelefteq G\}$$

so there exists a composition series for G of the form

$$\overline{H}_0 \trianglelefteq \overline{H}_1 \trianglelefteq \cdots \trianglelefteq \overline{H}_n = G.$$

But since $\overline{H}_{i+1}/\overline{H}_i \cong H_{i+1}/H_i$ for all indices i, we have that all of the composition factors in the above composition series are all of prime order.

Exercise 1.51. There are 5 groups of order $8 = 2^3$. Find all the possible composition series.

Solution 1.52. Recall that a subnormal series of a group G is a finite sequence of the form

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

Recall that a subnormal series

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

is a composition series if each factor group of the form H_{i+1}/H_i is simple. Also recall that a group is simple if it is nontrivial and has no proper nontrivial normal subgroups. Also recall that a finite simple abelian group is necessarily isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Begin by considering a composition series for $\mathbb{Z}/8\mathbb{Z}$. Given a subgroup H of $\mathbb{Z}/8\mathbb{Z}$, we have that $(\mathbb{Z}/8\mathbb{Z})/H$ is simple if and only if it is of prime order. So it is clear that $(\mathbb{Z}/8\mathbb{Z})/H$ is simple if and only if it is of order 2. We thus have that the latter part of a composition series for $\mathbb{Z}/8\mathbb{Z}$ must be of the form

$$\{0, 2, 4, 6\} \trianglelefteq \mathbb{Z}/8\mathbb{Z}.$$

Similarly, since a finite simple abelian group must be isomorphic to a group of the form $\mathbb{Z}/p\mathbb{Z}$ for a prime p, we thus find that a composition series for $\mathbb{Z}/8\mathbb{Z}$ must be of the following form:

$$\{0\} \trianglelefteq \{0, 2\} \trianglelefteq \{0, 2, 4, 6\} \trianglelefteq \mathbb{Z}/8\mathbb{Z}.$$

Now consider a composition series for $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Given a subgroup H of this group, we know that $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}))/H$ is simple if and only if it is of prime order. In particular, $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}))/H$ is simple if and only if it is of order 2. Now observe that the direct product $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ has precisely three subgroups of order 4:

$$\{(0,0), (0,1), (0,2), (0,3)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}),$$
$$\{(0,0), (1,1), (0,2), (1,3)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}),$$

$$\{(0,0),(0,2),(1,0),(1,2)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}).$$

We thus arrive at the following compositions series:

$$\begin{gathered}
\{(0,0)\} \trianglelefteq \{(0,0),(0,2)\} \trianglelefteq \{(0,0),(0,1),(0,2),(0,3)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \\
\{(0,0)\} \trianglelefteq \{(0,0),(0,2)\} \trianglelefteq \{(0,0),(1,1),(0,2),(1,3)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \\
\{(0,0)\} \trianglelefteq \{(0,0),(0,2)\} \trianglelefteq \{(0,0),(0,2),(1,0),(1,2)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \\
\{(0,0)\} \trianglelefteq \{(0,0),(1,0)\} \trianglelefteq \{(0,0),(0,2),(1,0),(1,2)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \\
\{(0,0)\} \trianglelefteq \{(0,0),(1,2)\} \trianglelefteq \{(0,0),(0,2),(1,0),(1,2)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}).
\end{gathered}$$

Now consider a composition series for $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. There are several subgroups of order 4 of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, namely:

$$\begin{gathered}
\{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})
\end{gathered}$$

We thus arrive at the following composition series:

$$\begin{gathered}
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,0,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,0)\} \trianglelefteq \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,0,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,0)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,0,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,0)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,1)\} \trianglelefteq \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,0)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,0)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,0)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,0)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,1)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,1)\} \trianglelefteq \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,0)\} \trianglelefteq \{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,1)\} \trianglelefteq \{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,1)\} \trianglelefteq \{(0,0,0),(1,0,0),(0,1,1),(1,1,1)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\
\{(0,0,0)\} \trianglelefteq \{(0,0,0),(0,1,1)\} \trianglelefteq \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})
\end{gathered}$$

$$\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,0,1)\} \trianglelefteq \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$
$$\{(0,0,0)\} \trianglelefteq \{(0,0,0),(1,1,0)\} \trianglelefteq \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\} \trianglelefteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Now consider composition series for the following dihedral group:

$$D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}.$$

It is easily seen that there are precisely three different subgroups of order 4 of D_4, namely:

$$\begin{aligned} \{1, a, a^2, a^3\} &\trianglelefteq D_4 \\ \{1, a^2, b, ba^2\} &\trianglelefteq D_4 \\ \{1, a^2, ba, ba^3\} &\trianglelefteq D_4. \end{aligned}$$

It is clear that the set $\{1, a, a^2, a^3\}$ of rotational isometries forms a subgroup of D_4. It may be less clear as to why $\{1, a^2, b, ba^2\}$ forms a subgroup, or why $\{1, a^2, ba, ba^3\}$ forms a subgroup. To illustrate why $\{1, a^2, b, ba^2\}$ and $\{1, a^2, ba, ba^3\}$ both form subgroups, we evaluate the Cayley tables for both $\{1, a^2, b, ba^2\}$ and $\{1, a^2, ba, ba^3\}$, using the dihedral relations whereby $a^4 = b^2 = (ab)^2 = 1$. We remark that from these relations, we have that $ab = ba^3$, since:

$$\begin{aligned} b^2 = (ab)^2 &\implies bb = abab \\ &\implies b = aba \\ &\implies ba^3 = ab. \end{aligned}$$

$\circ$	1	a^2	b	ba^2
1	1	a^2	b	ba^2
a^2	a^2	1	ba^2	b
b	b	ba^2	1	a^2
ba^2	ba^2	b	a^2	1

Entries in the above Cayley table may be evaluated using dihedral relations in the manner illustrated below.

$$\begin{aligned} a^2 b &= aab \\ &= a(ab) \\ &= a(ba^3) \\ &= (ab)a^3 \\ &= (ba^3)a^3 \\ &= ba^6 \\ &= ba^2. \end{aligned}$$

$$\begin{aligned} a^2 ba^2 &= ba^2 a^2 \\ &= b. \end{aligned}$$

$$\begin{aligned} ba^2 ba^2 &= baabaa \\ &= ba(ab)aa \end{aligned}$$

$$\begin{aligned} &= ba(ba^3)aa \\ &= baba \\ &= b(ab)a \\ &= b(ba^3)a \\ &= b^2a^4 \\ &= 1. \end{aligned}$$

$\circ$	1	a^2	ba	ba^3
1	1	a^2	ba	ba^3
a^2	a^2	1	ba^3	ba
ba	ba	ba^3	1	a^2
ba^3	ba^3	ba	a^2	1

Entries in the above Cayley table may be evaluated using dihedral relations in the manner illustrated below.

$$\begin{aligned} a^2ba &= aaba \\ &= a(ab)a \\ &= a(ba^3)a \\ &= aba^4 \\ &= ab \\ &= ba^3. \end{aligned}$$

$$\begin{aligned} baba &= b(ab)a \\ &= b(ba^3)a \\ &= 1. \end{aligned}$$

So, since $\{1, a, a^2, a^3\}$, $\{1, a^2, b, ba^2\}$, and $\{1, a^2, ba, ba^3\}$ are the only subgroups of D_4 of order 4, it is easily seen that the only possible composition series for the dihedral group of order 8 are the subnormal series given below:

$$\begin{gathered} \{1\} \trianglelefteq \{1, a^2\} \trianglelefteq \{1, a, a^2, a^3\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, a^2\} \trianglelefteq \{1, a^2, b, ba^2\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, b\} \trianglelefteq \{1, a^2, b, ba^2\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, ba^2\} \trianglelefteq \{1, a^2, b, ba^2\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, a^2\} \trianglelefteq \{1, a^2, ba, ba^3\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, ba\} \trianglelefteq \{1, a^2, ba, ba^3\} \trianglelefteq D_4 \\ \{1\} \trianglelefteq \{1, ba^3\} \trianglelefteq \{1, a^2, ba, ba^3\} \trianglelefteq D_4. \end{gathered}$$

So, it remains to consider composition series for the quaternion group. Recall that the quaternion group is an 8-element group on the set

$$\{1, -1, i, -i, j, -j, k, -k\}$$

with a presentation of the following form:

$$\langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

It is known that there are precisely 3 subgroups of order 4 of Q_8, namely the subgroups given below, which are all isomorphic to the cyclic group $\mathbb{Z}/4\mathbb{Z}$[1] It is also known that all of these subgroups of order 4 are normal.

$$\begin{aligned}\{1, i, -1, -i\} &\trianglelefteq Q_8\\ \{1, j, -1, -j\} &\trianglelefteq Q_8\\ \{1, k, -1, -k\} &\trianglelefteq Q_8.\end{aligned}$$

We thus find that the only composition series for the quaternion group are the following series:

$$\begin{aligned}\{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{1, i, -1, -i\} \trianglelefteq Q_8\\ \{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{1, j, -1, -j\} \trianglelefteq Q_8\\ \{1\} \trianglelefteq \{1, -1\} \trianglelefteq \{1, k, -1, -k\} \trianglelefteq Q_8.\end{aligned}$$

Exercise 1.53. Let A and B be groups, and for $b \in B$, let ϕ_b be an automorphism of A, so that

$$\phi: B \to \text{Aut}(A)$$

is a group homomorphism. Define $A \rtimes_\phi B$ as the set

$$\{(a, b) : a \in A, b \in B\}$$

endowed with the binary operation $\circ_{A\rtimes_\phi B}$ on $A \rtimes_\phi B$ whereby

$$(a, b) \circ_{A\rtimes_\phi B} (a', b') = (a\phi_b(a'), b(b'))$$

for $a, a' \in A$ and $b, b' \in B$. Show that $A \rtimes B$ forms a group, and show that $A \rtimes_\phi B = A \times B$ if $\phi_b(a) = a$ for all $b \in B$, i.e. ϕ_b is the identity automorphism on A for all $b \in B$.

Solution 1.54. Let $a_1, a_2 \in A$ and let $b_1, b_2 \in B$. By definition of the operation $\circ = \circ_{A\rtimes_\phi B}$, we have that

$$(a, b) \circ_{A\rtimes_\phi B} (a', b') = (a\phi_b(a'), b(b')),$$

and since

$$\phi_b: A \to A$$

must be an automorphism of A for $b \in B$, we thus find that

$$(a, b) \circ_{A\rtimes_\phi B} (a', b') = (a\phi_b(a'), b(b')) \in \{(a, b) : a \in A, b \in B\}$$

for $a, a' \in A$ and $b, b' \in B$, thus proving that $\circ_{A\rtimes_\phi B}$ is a binary operation on $\{(a, b) : a \in A, b \in B\}$. We claim that this binary operation is associative. To prove this, begin by letting $a_1, a_2, a_3 \in A$ and $b_1, b_2, b_3 \in B$. Evaluate the product $(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3))$:

$$\begin{aligned}(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3)) &= (a_1, b_1) \circ (a_2\phi_{b_2}(a_3), b_2b_3)\\ &= (a_1\phi_{b_1}(a_2\phi_{b_2}(a_3)), b_1(b_2b_3)).\end{aligned}$$

Now evaluate the product $((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3)$:

$$((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3) = (a_1\phi_{b_1}(a_2), b_1b_2) \circ (a_3, b_3)$$

[1] See `http://groupprops.subwiki.org/wiki/Subgroup_structure_of_quaternion_group`.

$$= (a_1\phi_{b_1}(a_2)\phi_{b_1b_2}(a_3), (b_1b_2)b_3)\,.$$

Now recall that

$$\phi\colon B \to \mathrm{Aut}(A)$$

is a group homomorphism. Also observe that ϕ_b is a group homomorphism for all $b \in B$. We thus find that the product $(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3))$ may be rewritten in the following manner, making use of the associativity of the underlying binary operation of B:

$$\begin{aligned}(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3)) &= (a_1, b_1) \circ (a_2\phi_{b_2}(a_3), b_2b_3)\\ &= (a_1\phi_{b_1}(a_2\phi_{b_2}(a_3)), b_1(b_2b_3))\\ &= (a_1\phi_{b_1}(a_2\phi_{b_2}(a_3)), (b_1b_2)b_3)\\ &= (a_1\phi_{b_1}(a_2)\phi_{b_1}(\phi_{b_2}(a_3)), (b_1b_2)b_3)\\ &= (a_1\phi_{b_1}(a_2)\phi_{b_1b_2}(a_3), (b_1b_2)b_3)\,.\end{aligned}$$

We thus find that

$$(a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3)) = ((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3)$$

for $a_1, a_2, a_3 \in A$ and $b_1, b_2, b_3 \in B$. We have thus far shown that the operation $\circ_{A\rtimes_\phi B}$ is an associative binary operation on the set $\{(a, b) : a \in A, b \in B\}$. In other words, we have that the collection of all pairs of the form (a, b) for $a \in A$ and $b \in B$ forms a semigroup. Recall that a semigroup is an algebraic structure consisting of a set together with an assocaitive binary operation [2].

Now, let e_A and e_B respectively denote the identity elements for A and B. Consider the ordered pair (e_A, e_B) in the codomain of the binary operation $\circ = \circ_{A\rtimes_\phi B}$. Letting $a \in A$ and $b \in B$ be artbirary, observe that $\phi_b(e_A) = e_A$ since ϕ_b must be an automorphism of A. Also observe that since

$$\phi\colon B \to \mathrm{Aut}(A)$$

is a group homomorphism, we have that

$$\phi_{e_B} = \mathrm{id} = \mathrm{id}_{\mathrm{Aut}(A)} = e_{\mathrm{Aut}(A)},$$

letting

$$\mathrm{id} = \mathrm{id}_{\mathrm{Aut}(A)} = e_{\mathrm{Aut}(A)}\colon A \to A$$

denote the identity automorphism on A whereby

$$\mathrm{id}(a) = a$$

for all $a \in A$. We thus have that:

$$\begin{aligned}(e_A, e_B) \circ (a, b) &= (e_A\phi_{e_B}(a), e_Bb)\\ &= (e_A\phi_{e_B}(a), b)\\ &= (e_A\mathrm{id}(a), b)\\ &= (e_Aa, b)\\ &= (a, b).\end{aligned}$$

[2] See https://en.wikipedia.org/wiki/Semigroup.

Similarly, we have that:

$$\begin{aligned}(a,b)\circ(e_A,e_B) &= (a\phi_b(e_A), b\cdot e_B)\\ &= (a\phi_b(e_A), b)\\ &= (a\cdot e_A, b)\\ &= (a,b).\end{aligned}$$

We thus have that the identity axiom holds with respect to the semigroup obtained by endowing the set $\{(a,b) : a \in A, b \in B\}$ with the binary operation $\circ = \circ_{A\rtimes_\phi B}$. In other words, the set $\{(a,b) : a \in A, b \in B\}$ forms a monoid with respect to this binary operation. Recall that a monoid is an algebraic structure with a single associative binary operation and an identity element [3]. Again letting $a \in A$ and $b \in B$ be arbitrary, let a^{-1} and b^{-1} respectively denote the inverses of a and b. We claim that the right inverse of (a,b) is $(\phi_{b^{-1}}(a^{-1}), b^{-1})$:

$$\begin{aligned}(a,b)\circ(\phi_{b^{-1}}(a^{-1}), b^{-1}) &= (a\phi_b(\phi_{b^{-1}}(a^{-1})), b\cdot b^{-1})\\ &= (a\phi_b(\phi_{b^{-1}}(a^{-1})), e_B)\\ &= (a\phi_{b\cdot b^{-1}}(a^{-1}), e_B)\\ &= (a\phi_{e_B}(a^{-1}), e_B)\\ &= (a\cdot \mathrm{id}(a^{-1}), e_B)\\ &= (a\cdot a^{-1}, e_B)\\ &= (e_A, e_B).\end{aligned}$$

Similarly, we find that the left inverse of (a,b) is also equal to $(\phi_{b^{-1}}(a^{-1}), b^{-1})$:

$$\begin{aligned}(\phi_{b^{-1}}(a^{-1}), b^{-1})\circ(a,b) &= (\phi_{b^{-1}}(a^{-1})\phi_{b^{-1}}(a), b^{-1}b)\\ &= (\phi_{b^{-1}}(a^{-1})\phi_{b^{-1}}(a), e_B)\\ &= (\phi_{b^{-1}}(a^{-1}a), e_B)\\ &= (\phi_{b^{-1}}(e_A), e_B)\\ &= (e_A, e_B).\end{aligned}$$

We thus find that the monoid obtained by endowing the set $\{(a,b) : a \in A, b \in B\}$ with the operation $\circ$ forms a group.

Exercise 1.55. Construct morphisms α and β such that the sequence

$$\{1\} \longrightarrow A \xrightarrow{\alpha} A \rtimes_\phi B \xrightarrow{\beta} B \longrightarrow \{1\}.$$

is an exact sequence.

Solution 1.56. Recall that a sequence

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} G_n$$

of groups and group homomorphisms is said to be exact if the image of each homomorphism is equal to the kernel of the next, i.e.,

$$\mathrm{im}(f_i) = \ker(f_{i+1})$$

[3] See https://en.wikipedia.org/wiki/Monoid.

for all indices i[4]. It is natural to consider the mapping

$$\alpha\colon A \to A \rtimes_{\phi} B$$

whereby

$$\alpha(a) = (a, e_B)$$

for all $a \in A$. Letting $a_1, a_2 \in A$, we have that:

$$\begin{aligned}
\alpha(a_1) \cdot \alpha(a_2) &= (a_1, e_B) \cdot (a_2, e_B) \\
&= (a_1 \phi_{e_B}(a_2), e_B e_B) \\
&= (a_1 \phi_{e_B}(a_2), e_B) \\
&= (a_1 \mathrm{id}(a_2), e_B) \\
&= (a_1 a_2, e_B) \\
&= \alpha(a_1 a_2).
\end{aligned}$$

We thus have that α is a group homomorphism in this case. Observe that the image $\mathrm{im}(\alpha)$ of the morphism

$$\alpha\colon A \to A \rtimes_{\phi} B$$

is the set of all expressions of the form (a, e_B) where $a \in A$. Now define

$$\beta\colon A \rtimes_{\phi} B \to B$$

so that

$$\beta(a, b) = b$$

for all $a \in A$ and $b \in B$. Letting $a_1, a_2 \in A$ and $b_1, b_2 \in B$, we have that:

$$\begin{aligned}
\beta((a_1, b_1) \cdot (a_2, b_2)) &= \beta((a_1 \phi_{b_1}(a_2), b_1 b_2)) \\
&= b_1 b_2 \\
&= \beta(a_1, b_1) \cdot \beta(a_2, b_2).
\end{aligned}$$

Now observe that the kernel $\ker(\beta)$ of the morphism β is precisely the set of all expressions in $A \rtimes_{\phi} B$ of the form (a, e_B) for $a \in A$. So, we have that $\mathrm{im}(\alpha) = \ker(\beta)$, thus establishing an exact sequence of the desired form.

Exercise 1.57. Letting G be a group of prime power order, with $|G| = p^a$, prove that if $H \leq G$, then $N_G(H) \neq H$.

Solution 1.58. Find a proper normal subgroup $K \lhd G$ and $K \trianglelefteq H$ such that K is maximal and that G/K is not trivial. Since

$$K \trianglelefteq H \leq G,$$

we have that

$$H/K \leq G/K.$$

Now, since G is of prime power order, we have that the quotient group G/K is also of prime power order. So the center $Z(G/K)$ of G/K is nontrivial. So there exists a non-identity element zK in the center $Z(G/K)$ of G/K, with $z \notin K$ since $zK \neq eK$.

[4] See `https://en.wikipedia.org/wiki/Exact_sequence`.

Now, observe that for $h \in H$, we have that $hK \in H/K$. Since

$$H/K \leq G/K,$$

we are thus lead to consider the product

$$(zK)(hK) \in G/K.$$

Since z is in the center of G/K, we have that:

$$zhK = (zK)(hK) = (hK)(zK) = hzK \in G/K.$$

So, since

$$zhK = hzK \in G/K,$$

we have that

$$hK = z^{-1}hzK.$$

Therefore,

$$z^{-1}hz \in hK \subseteq hH = H.$$

But recall that $h \in H$ is arbitrary. We thus find that

$$zhz^{-1} \in H$$

for all $h \in H$. Since G is finite, we have that $N_G(H) = M_G(H)$. So, we have shown that $z \in N_G(H)$.

But furthermore, we claim that z cannot be in H. By way of contradiction, suppose that $z \in H$. We thus have that $z \notin K$ and $z \in H$. We claim that this contradicts the maximality of K.

To show this, let L denote the smallest subgroup of G containing z and containing the elements in K. Since $z \notin K$, we have that $K \subsetneq L$. We have that $L \leq G$ by definition of L. Using the fact that $zK \in Z(G/K)$ together with the fact that $K \lhd G$, it is easily seen that each element in L must be of the form $z^n k$ for some $k \in K$ and some power z_n of z. Letting $g \in G$, consider the coset Lg. Let $z^n kg$ be an element in this coset. But then this element is equal to

$$z^n gk'$$

for some $k' \in K$, and this element is equal to

$$gz^n k''$$

for some $k'' \in K$, since powers of zK are also in the center of G/K. So we have shown that

$$(z^n k)g = g(z^n k'')$$

for some element $k'' \in K$, thus proving the inclusion whereby

$$Lg \subseteq gL.$$

A symmetric argument may be used to prove the reverse inclusion. A similar argument may be used to prove that $L \unlhd H$. Observe that $H < G$. But since $z \in H$ by assumption, and since

$$K \leq H < G,$$

we have that

$$L \leq H < G,$$

which also shows that G/L is nontrivial. But this contradicts the maximality of K, thus proving that z cannot be in H.

Exercise 1.59. Illustrate Sylow's theorems using the Sylow p-subgroups of S_3.

Solution 1.60. The Sylow 2-subgroups of S_3 are given below:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \leq S_3$$
$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \leq S_3$$
$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \leq S_3.$$

We thus have that $n_2 = 3$. So, $n_2 \geq 1$, n_2 divides the order $|G| = 6$ of G, and $n_2 \equiv 1 (\text{mod } p)$. Also, all Sylow 2-subgroups of S_3 are conjugate, as illustrated below:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

There is a unique Sylow 3-subgroup of S_3, namely:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \leq S_3.$$

We thus have that $n_3 = 1$. So $n_3 \geq 1$, n_3 divides the order $|G| = 6$ of G, and $n_3 \equiv 1 (\text{mod} 3)$. Since there is a unique Sylow 3-subgroup of S_3, it is trivial that Sylow 3-subgroups of S_3 are conjugate.

Exercise 1.61. Write in the details of the proofs of the Sylow theorems given in the handout[5] from the October 4th lecture

Solution 1.62. We begin with an expanded proof of the following result.

Proposition 1.63. *Let G be a p-group acting on a (finite) set E. Then*

$$|E| \equiv |\text{Fix}_G(E)| \, (\text{mod } p) \, .$$

Proof. Since E is a G-set, we may write G as a disjoint union of orbits as follows, letting $n \in \mathbb{N}$:

$$E = \text{Orbit}_G(x_1) \uplus \text{Orbit}_G(x_2) \uplus \cdots \uplus \text{Orbit}_G(x_n).$$

By the orbit-stabilizer theorem, we thus have that

$$|E| = \sum_{i=1}^{n} |\text{Orbit}_G(x_i)| = \sum_{i=1}^{n} \frac{|G|}{|\text{Stab}_G(x_i)|}.$$

[5] See `http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/100616sylows.pdf`.

But since $\mathrm{Stab}_G(x_i)$ is a subgroup of G, by Lagrange's theorem, each expression of the form $\frac{|G|}{|\mathrm{Stab}_G(x_i)|}$ must be of order p^{b_i}. Letting

$$\bullet\colon G \times E \to E$$

denote the group action corresponding to the G-set E, recall that

$$\mathrm{Fix}(g) = \{x \in E : g \bullet x = x\}$$

for $g \in G$. Similarly, we define

$$\mathrm{Fix}_G(E) = \mathrm{Fix}(G) = \{x \in E : \forall g \in G \ g \bullet x = x\}.$$

We claim that: $\mathrm{Fix}(G) = \{x_i : 1 \leq i \leq n, b_i = 0\}$. Equivalently: $\mathrm{Fix}(G) = \{x \in E : |G| = |\mathrm{Stab}_G(x)|\}$. Equivalently:

$$\mathrm{Fix}(G) = \{x \in E : G = \mathrm{Stab}_G(x)\}.$$

Our strategy to prove the above equality is to use *mutual inclusion*. Let $y \in E$ be such that $\forall g \in G \ g \bullet y = y$, so that $y \in \mathrm{Fix}(G)$ is arbitrary. Given that $\forall g \in G \ g \bullet y = y$, consider the expression $\mathrm{Stab}_G(y)$. By definition of the stabilizer of an element, we have that

$$\mathrm{Stab}(y) = \{g \in G : g \bullet y = y\},$$

but since $\forall g \in G \ g \bullet y = y$ in this case, we have that $\mathrm{Stab}(y) = G$. So, given $y \in \mathrm{Fix}(G)$, we thus have that $y \in \{x \in E : G = \mathrm{Stab}_G(x)\}$, thus proving the desired inclusion whereby

$$\mathrm{Fix}(G) \subseteq \{x \in E : G = \mathrm{Stab}_G(x)\}.$$

Conversely, let

$$y \in \{x \in E : G = \mathrm{Stab}_G(x)\}$$

be arbitrary. Since $G = \mathrm{Stab}_G(y)$, we have that $G = \{g \in G : g \bullet y = y\}$, and we thus have that $\forall g \in G \ g \bullet y = y$. Since $y \in E$ is such that $\forall g \in G \ g \bullet y = y$, we thus have that

$$y \in \mathrm{Fix}(G) = \{x \in E : \forall g \in G \ g \bullet x = x\},$$

thus proving that the reverse inclusion whereby

$$\{x \in E : G = \mathrm{Stab}_G(x)\} \subseteq \mathrm{Fix}(G),$$

thus proving that $\mathrm{Fix}(G) = \{x_i : 1 \leq i \leq n, b_i = 0\}$.

Now, recall that

$$|E| = \sum_{i=1}^{n} \frac{|G|}{|\mathrm{Stab}_G(x_i)|},$$

by the orbit-stabilizer theorem. Rewrite this equality as follows:

$$\begin{aligned} |E| &= \sum_{i=1}^{n} \frac{|G|}{|\mathrm{Stab}_G(x_i)|} \\ &= \sum_{\substack{1 \leq i \leq n \\ |\mathrm{Stab}_G(x_i)| = |G|}} \frac{|G|}{|\mathrm{Stab}_G(x_i)|} + \sum_{\substack{1 \leq i \leq n \\ |\mathrm{Stab}_G(x_i)| < |G|}} \frac{|G|}{|\mathrm{Stab}_G(x_i)|} \end{aligned}$$

$$= \left(\sum_{\substack{1 \le i \le n \\ |\mathrm{Stab}_G(x_i)| = |G|}} 1 \right) + \sum_{\substack{1 \le i \le n \\ |\mathrm{Stab}_G(x_i)| < |G|}} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}$$

$$= \left(\sum_{\substack{1 \le i \le n \\ \mathrm{Stab}_G(x_i) = G}} 1 \right) + \sum_{\substack{1 \le i \le n \\ |\mathrm{Stab}_G(x_i)| < |G|}} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}$$

$$= |\mathrm{Fix}(G)| + \sum_{\substack{1 \le i \le n \\ |\mathrm{Stab}_G(x_i)| < |G|}} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

By Lagrange's theorem, it is clear that each expression of the form

$$\frac{|G|}{|\mathrm{Stab}_G(x_i)|}$$

such that $|\mathrm{Stab}_G(x_i)| < |G|$ vanishes modulo p, thus proving that

$$|E| \equiv |\mathrm{Fix}(G)| \,(\mathrm{mod}\ p)$$

as desired. □

Corollary 1.64. *If $p \in \mathbb{N}$ is a prime, and $m \in \mathbb{N}$ is such that p does not divide m, then*

$$\binom{p^n m}{p^n} \equiv m\,(mod\ p)\,.$$

Proof. With respect to Proposition 1.63, let G be the cyclic group

$$C_{p^n m} = \mathbb{Z}_{p^n m} = \mathbb{Z}/(p^n m)\mathbb{Z}.$$

Exercise: Prove that there exists a subgroup $H \le G$ of order p^n.

We begin by remarking that the result given in the above exercise follows immediately from the Fundamental Theorem of Cyclic Groups, which is formulated as follows in Joseph Gallian's *Contemporary Abstract Algebra*:

Fundamental Theorem of Cyclic Groups: "Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k – namely, $\langle a^{n/k} \rangle$."

Letting $1 \in \mathbb{Z}/(p^n m)\mathbb{Z}$ denote the coset $1 + (p^n m)\mathbb{Z}$ in the quotient group $\mathbb{Z}/(p^n m)\mathbb{Z}$, we may thus write

$$\langle 1 \rangle = \mathbb{Z}_{p^n m}.$$

Since p^n divides $p^n m$, by the Fundamental Theorem of Cyclic Groups, we thus have that the group $\langle 1 \rangle = \mathbb{Z}_{p^n m}$ has exactly one subgroup of order p^n, namely $\langle m \rangle$. Without resorting to using the Fundamental Theorem of Cyclic Groups, it is easily seen that $\langle m \rangle$ is a cyclic subgroup of $\langle m \rangle$ of order p^n. In particular, it is easily seen that

$$\langle m \rangle = \{m, 2m, 3m, \ldots, (p^n - 1)m, 0\}$$

since the expressions in

$$\{m, 2m, 3m, \ldots, (p^n - 1), m\}$$

do not vanish modulo $p^n m$ because p does not divide m by assumption, and since the elements in

$$\langle m \rangle = \{m, 2m, 3m, \ldots, (p^n - 1), m, 0\}$$

must be pairwise unequal as is easily verified using our assumption that p does not divide m.

So, let $H = \langle m \rangle$. Let X be the set of subsets $S \subseteq G$ such that $|S| = p^n$. Note that $|X| = \binom{p^n m}{p^n}$. Let H act on X by left addition. Let

$$\bullet \colon H \times X \to X$$

denote this action.

Exercise: Prove that $S \in \text{Fix}(H)$ if and only if S is a left coset of H.

Suppose that S is a left coset of H. Let $g \in G$, and write $S = \{g + h : h \in H\}$. Since H is a (normal) subgroup of order p^n, we have that $g + H$ is also of order p^n. We thus have that $S \in X$. Now let $i \in H$, and consider the expression $i \bullet S$:

$$\begin{aligned} i \bullet S &= i + S \\ &= i + \{g + h : h \in H\} \\ &= \{i + g + h : h \in H\} \\ &= \{g + i + h : h \in H\} \\ &= \{g + j : j \in H\} \\ &= S. \end{aligned}$$

We thus have that if S is a left coset of H, then S in the following set:

$$\text{Fix}(H) = \{T \in X : \forall i \in H \ i \bullet T = T\}.$$

Conversely, suppose that:

$$S \in \text{Fix}(H) = \{T \in X : \forall i \in H \ i \bullet T = T\}.$$

We thus have that:

$$\forall i \in H \ i \bullet S = S.$$

Therefore,

$$\forall i \in H \ i + S = S.$$

Write:

$$H = \{h_1, h_2, \ldots, h_{p^n}\},$$

for the sake of convenience, and write:

$$S = \{s_1, s_2, \ldots, s_{p^n}\}.$$

Now let $f \colon \{1, 2, \ldots, p^n\} \to \{1, 2, \ldots, p^n\}$ be a mapping defined as follows, using the fact that $\forall i \in H \ i + S = S$:

$$h_1 s_1 = s_{f(1)},$$

$$\begin{aligned}&h_2 s_1 = s_{f(2)},\\&\dots\\&h_{p^n} s_1 = s_{f(p^n)}.\end{aligned}$$

Letting i and j be elements in the domain of f, it is clear that f is injective, since:

$$\begin{aligned}f(i) = f(j) &\implies s_{f(i)} = s_{f(j)}\\&\implies h_i s_1 = h_j s_1\\&\implies h_i = h_j\\&\implies i = j.\end{aligned}$$

So, since f is an injective map from $\{1, 2, \dots, p^n\}$ to $\{1, 2, \dots, p^n\}$, we may thus deduce that f is bijective. Since f is bijective, it is thus clear that

$$s_1 + H = S,$$

thus proving that S is a left coset of H.

So, we have shown that the set $\mathrm{Fix}(H)$ is precisely the set of left cosets of H. Now, by Lagrange's theorem, we have that the number of left cosets of H is m. So the above corollary thus follows from Proposition 1.63. □

Theorem 1.65. *The center of a p-group G is nontrivial.*

Proof. Let G act on itself by conjugation. In particular, let

$$\bullet : G \times G \to G$$

denote the action whereby

$$g \bullet h = ghg^{-1}$$

for all $g, h \in G$. It is clear that $\bullet$ is indeed a group action, since

$$e \bullet g = ege^{-1} = g$$

for $g \in G$, and since the following holds for $g, h, i \in G$:

$$\begin{aligned}(gh) \bullet i &= (gh)i(gh)^{-1}\\&= ghih^{-1}g^{-1}\\&= g(hih^{-1})g^{-1}\\&= g(h \bullet i)g^{-1}\\&= g \bullet (h \bullet i).\end{aligned}$$

Exericse: Show that $\mathrm{Fig}(G) = Z(G)$ with respect to the conjugation action on G.

To show that $\mathrm{Fix}(G) = Z(G)$, rewrite the expression $\mathrm{Fix}(G)$ in the following manner:

$$\begin{aligned}\mathrm{Fix}(G) &= \{i \in G : \forall h \in G \ h \bullet i = i\}\\&= \{i \in G : \forall h \in G \ hih^{-1} = i\}\\&= \{i \in G : \forall h \in G \ hi = ih\}\end{aligned}$$

$$= Z(G).$$

Now, by Proposition 1.63, we have that

$$|G| \equiv |\mathrm{Fix}(G)| \, (\mathrm{mod}\ p),$$

and thus

$$|G| \equiv |Z(G)| \, (\mathrm{mod}\ p),$$

and thus

$$|Z(G)| \equiv |G| \, (\mathrm{mod}\ p).$$

We thus have that

$$|Z(G)| \equiv 0 (\mathrm{mod}\ p),$$

thus proving that p divides the order of $Z(G)$. □

Theorem 1.66. *(1^{st} Sylow theorem): Sylow p-subgroups always exist.*

Proof. Let X be the set of subsets of G of order p^n and let G act on X by left multiplication. Let

$$\bullet : G \times X \to X$$

denote the corresponding action whereby

$$g \bullet x = gx$$

for $g \in G$ and $x \in X$. As above, let expressions of the form x_i denote the representatives of the orbits. Since $|X| = \binom{p^n m}{p^n}$, as shown above, we have that $|X| \equiv m (\mathrm{mod}\ p)$. So p does not divide $|X|$. So there exists at least one expression of the form x_i such that p does not divide $\frac{|G|}{|\mathrm{Stab}_G(x_i)|}$. Now, what is the order of G? It should be clarified that the order $|G|$ of G is such that p is a prime factor with multiplicity n of $|G|$. Since the prime power p^n divides $|G|$ but p^{n+1} does not divide $|G|$, and since $\frac{|G|}{|\mathrm{Stab}_G(x_i)|}$ is a natural number by Lagrange's theorem, and since $\frac{|G|}{|\mathrm{Stab}_G(x_i)|}$ is not divisible by p, we may deduce that p^n divides $|\mathrm{Stab}_G(x_i)|$. We remark that we are implicitly using the Fundamental Theorem of Arithmetic.

Exercise: Explain why $|\mathrm{Stab}_G(x_i)| = |\{zy : z \in \mathrm{Stab}_G(x_i)\}|$.

Letting $y \in x_i$, to show that

$$|\mathrm{Stab}_G(x_i)| = |\{zy : z \in \mathrm{Stab}_G(x_i)\}|,$$

begin by observing that $\mathrm{Stab}_G(x_i)$ is a subgroup of G. Now consider the expression

$$\{zy : z \in \mathrm{Stab}_G(x_i)\}.$$

It is clear that the above set is precisely the following right coset:

$$(\mathrm{Stab}_G(x_i))\, y = \{zy : z \in \mathrm{Stab}_G(x_i)\}.$$

From our previous proof of Lagrange's theorem, which is available through the course webpage for MATH 6121, we know that the order $|\mathrm{Stab}_G(x_i)|$ of the subgroup $\mathrm{Stab}_G(x_i)$ must be equal to the order of the coset $(\mathrm{Stab}_G(x_i))\, y$, thus proving that

$$|\mathrm{Stab}_G(x_i)| = |\{zy : z \in \mathrm{Stab}_G(x_i)\}|,$$

as desired.

Now by definition of the stabilizer of an element, we have that:

$$\mathrm{Stab}_G(x_i) = \{g \in G : g \bullet x_i = x_i\}\,.$$

Denote x_i as follows:

$$x_i = \{w_1, w_2, \dots, w_{p^n}\}.$$

Now, let $z \in \mathrm{Stab}_G(x_i)$. We thus have that $z \in G$, and $z \bullet x_i = x_i$. Now consider the expression zy. Since $y \in x_i$, and since $z \bullet x_i = x_i$, we have that $zy = y'$ for some $y' \in x_i$. So, we have that the set of all expressions of the form zy where z is in $\mathrm{Stab}_G(x_i)$ is contained in x_i. We thus have that

$$|\mathrm{Stab}_G(x_i)| = |\{zy : z \in \mathrm{Stab}_G(x_i)\}| \leq |x_i|\,,$$

and we thus have that

$$|\mathrm{Stab}_G(x_i)| \leq p^n.$$

But recall that we used Lagrange's theorem to prove that p^n divides the order of the subgroup $\mathrm{Stab}_G(x_i)$. We thus have that

$$|\mathrm{Stab}_G(x_i)| \geq p^n,$$

thus proving that

$$|\mathrm{Stab}_G(x_i)| = p^n.$$

But recall that $\mathrm{Stab}_G(x_i)$ forms a subgroup of G with respect to the underlying binary operation on G. We thus have that $\mathrm{Stab}_G(x_i)$ is a subgroup of G of order p^n.

Recall that a finite group is a p-group iff its order is a power of p. Recall that a Sylow p-subgroup of G is a maximal p-subgroup of G, i.e. a subgroup of G that is a p-group that is not a proper subgroup of any other p-subgroup of G. As indicated above, the order $|G|$ of G is such that p is a prime factor with multiplicity n of $|G|$. Therefore, since $\mathrm{Stab}_G(x_i)$ is a subgroup of G of order p^n, we have that $\mathrm{Stab}_G(x_i)$ must be a Sylow p-subgroup, because by Lagrange's theorem, this subgroup cannot be properly contained in any other p-subgroup of G, since the multiplicity of the prime factor p of $|G|$ is n. □

Theorem 1.67. *(2^{nd} Sylow theorems) All Sylow p-subgroups are conjugate to each other.*

Proof. Let T and S be two subgroups of order p^n. Observe that $S \trianglelefteq G$. Let T act on the left cosets of the quotient group G/S by left multiplication. Let

$$\bullet : T \times (G/S) \to G/S$$

denote the corresponding group action whereby

$$t \bullet (gS) = (tg)\,S$$

for $t \in T$ and $g \in G$. Since T is a p-group, by Proposition 1.63, we have that

$$|G/S| \equiv |\mathrm{Fix}_T(G/S)|\,(\mathrm{mod}\ p)\,.$$

Now recall that G is a p-group, such that the multiplicity of the prime p with respect to the prime factorization of $|G|$ is n. Since S is a Sylow p-subgroup, i.e., a maximal p-subgroup, it is clear that p

does not divide the order $|G/S|$ of the quotient group G/S. We may thus deduce that $\mathrm{Fix}_T(G/S)$ is nonempty. So, let $gS \in \mathrm{Fix}_T(G/S)$.

Exericse: Show that if $gS \in \mathrm{Fix}_T(G/S)$, then $T \subseteq gSg^{-1}$.

To show that

$$gS \in \mathrm{Fix}_T(G/S) \Longrightarrow T \subseteq gSg^{-1},$$

begin by rewriting the expression $\mathrm{Fix}_T(G/S)$ as follows:

$$\mathrm{Fix}_T(G/S) = \{hS \in G/S : \forall t \in T \; t \bullet (hS) = hS\}.$$

We thus have that:

$$\forall t \in T \; t \bullet (gS) = gS.$$

So, for each element $t \in T$, since $tge = tg$ must be in gS, we have that the following holds: for each element $t \in T$, there exists a corresponding element $s = s_t$ in S such that $tge = tg = gs$. So, for each element $t \in T$, there exists a corresponding element $s = s_t$ in S such that $t = gsg^{-1}$. We thus have that $T \subseteq gSg^{-1}$ as desired. But since T is a p-group of order p^n, and since gSg^{-1} is of order p^n, we thus have that $T = gSg^{-1}$ as desired. □

Theorem 1.68. *(3rd Sylow Theorem) Let n_p be the number of Sylow subgroups, then n_p divides the order of G*

Proof. Let G act on the set of all Sylow p-subgroups of G by conjugation. By the 2nd Sylow Theorem, we know that there is a unique orbit with respect to this group action. So, letting S denote a fixed Sylow p-subgroup, we have that $\mathrm{Orbit}_G(S)$ consists precisely of all the Sylow p-subgroups of G. Now, by the orbit-stabilizer theorem, we have that

$$n_p = |\mathrm{Orbit}_G(S)| = \frac{|G|}{|\mathrm{Stab}_G(S)|}.$$

So, since

$$n_p \cdot |\mathrm{Stab}_G(S)| = |G|,$$

we thus have that n_p divides the order of G, as desired. □

Theorem 1.69. *(4th Sylow Theorem) $n_p \equiv 1(\mathrm{mod} p)$.*

Proof. Let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups of G, and let $S \in \mathrm{Syl}_p(G)$. Let S act on $\mathrm{Syl}_p(G)$ by conjugation. By Proposition 1.63, we thus have that

$$n_p = \left|\mathrm{Syl}_p(G)\right| \equiv \left|\mathrm{Fix}_S(\mathrm{Syl}_p(G))\right| (mod\ p).$$

Exericse: Show that if $P \in \mathrm{Fix}_S(\mathrm{Syl}_p(G))$, then $S \subseteq N_G(P)$.

By definition of the normalizer of a subset, we have that:

$$N_G(P) = \{g \in G : gP = Pg\}.$$

Assuming that P is in $\mathrm{Fix}_S(\mathrm{Syl}_p(G))$, we have that

$$\forall s \in S \; s \bullet P = P.$$

Therefore, $\forall s \in S \; sPs^{-1} = P$. That is,

$$\forall s \in S \; sP = Ps.$$

So, for each element s in $S \leq G$, we have that $sP = Ps$. So it is clear that each element s in S must necessarily be in $N_G(P)$. This proves that $S \subseteq N_G(P)$. Since S is a subgroup of G, and since $N_G(P) \leq G$, we thus have that:

$$S \leq N_G(P) \leq G.$$

Now, since S and P are both Sylow p-subgroups of $N_G(P)$, by the first Sylow theorem, we have that $S = gPg^{-1}$ with $g \in N_G(P)$, and we thus have that $S = gPg^{-1} = P$. □

Exercise 1.70. Does S_4 have a composition series with composition factors of the form $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3)$? Does S_4 have a composition series with composition factors of the form $(\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2)$?

Solution 1.71. As discussed on the course webpage, the SageMath input

```
[H.order() for H in SymmetricGroup(4).subgroups()]
```

produces the following integer sequence:

$$(1,2,2,2,2,2,2,2,2,2,3,3,3,3,4,4,4,4,4,4,4,6,6,6,6,8,8,8,12,24).$$

We thus find that $n_2 = 3$, meaning that a subgroup of S_4 of order 8 cannot be a normal subgroup. This is easily seen using Sylow theory in the following way: we know that Sylow p-subgroups are all conjugate, so if there are multiple Sylow p-subgroups, i.e., if there are at least two distinct Sylow p-subgroups A and B, we have that

$$gAg^{-1} = B$$

for some $g \in G$, which shows that

$$gA = Bg \neq Ag,$$

which shows that A is not normal. So, as indicated on the course webpage, since $n_2 = 3$, it is impossible to have a composition series of S_4 with composition factors of the form $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3)$.

On the other hand, is it possible that S_4 has a composition series with composition factors of the form $(\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2)$? Begin by observing that $A_4 \trianglelefteq S_4$, with $S_4/A_4 \cong \mathbb{Z}_2$. It is easily seen that the only subgroup of S_4 of order 12 is A_4[6]. But it is also easily seen that A_4 does not have any subgroup of order 6[7]. We thus find that it is impossible for S_4 to have a composition series with composition factors of the form $(\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2)$.

Exercise 1.72. Show that the function $[\cdot,\cdot]$ constructed in the proof of Maschke's theorem is a scalar product.

Solution 1.73. Recall that a module is basically a "vector space over a ring". A module is decomposable if it can be written in the form $M \cong W \oplus V$, where W and V are proper nontrivial submodules of M. Also recall that a module is reducible if there exists a proper non-trivial submodule. According to Maschke's Theorem, over $\mathbb{C}$, a module M is an irreducible module if and only if M is decomposable.

So, let M be a $\mathbb{C}$-module, and let W be a proper non-trivial submodule. We want to find a submodule V such that $M \cong W \oplus V$.

[6] See `http://groupprops.subwiki.org/wiki/Subgroup_structure_of_symmetric_group:S4`.

[7] See `http://groupprops.subwiki.org/wiki/Subgroup_structure_of_alternating_group:A4`.

Fix a basis $\mathcal{B}$ of M. Define the scalar product $\langle \cdot, \cdot \rangle$ as follows:

$$\langle \vec{v}, \vec{u} \rangle = \overline{[\vec{v}]_{\mathcal{B}}^{T}}[\vec{u}]_{\mathcal{B}}.$$

Now, let

$$\phi : G \to \mathrm{Aut}(M)$$

be a representation of the finite group G over a field F in which $|G|$ is invertible. Define the mapping

$$[\cdot, \cdot] : M \times M \to \mathbb{C}$$

as follows:

$$[\vec{v}, \vec{u}] = \frac{1}{|G|} \sum_{g \in G} \langle \phi(g)(\vec{v}), \phi(g)(\vec{u}) \rangle.$$

We claim that this mapping is a scalar product. For the sake of clarity, let $\phi(g)(\vec{u})$ and $\phi(g)(\vec{v})$ be denoted as follows:

$$[\phi(g)(\vec{u})]_{\mathcal{B}} = \begin{bmatrix} u_1^g \\ u_2^g \\ \cdots \\ u_n^g \end{bmatrix}$$

$$[\phi(g)(\vec{v})]_{\mathcal{B}} = \begin{bmatrix} v_1^g \\ v_2^g \\ \cdots \\ v_n^g \end{bmatrix}$$

Now consider the expression $\overline{[\vec{u}, \vec{v}]}$.

$$\begin{aligned}
\overline{[\vec{u}, \vec{v}]} &= \overline{\frac{1}{|G|} \sum_{g \in G} \langle \phi(g)(\vec{u}), \phi(g)(\vec{v}) \rangle} \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\langle \phi(g)(\vec{u}), \phi(g)(\vec{v}) \rangle} \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\overline{[\phi(g)(\vec{u})]_{\mathcal{B}}^{T}}[\phi(g)(\vec{v})]_{\mathcal{B}}} \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\overline{[u_1^g, u_2^g, \ldots, u_n^g]} \begin{bmatrix} v_1^g \\ v_2^g \\ \cdots \\ v_n^g \end{bmatrix}} \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{[\overline{u_1^g}, \overline{u_2^g}, \ldots, \overline{u_n^g}] \begin{bmatrix} v_1^g \\ v_2^g \\ \cdots \\ v_n^g \end{bmatrix}} \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\overline{u_1^g} v_1^g + \overline{u_2^g} v_2^g + \cdots + \overline{u_n^g} v_n^g} \\
&= \frac{1}{|G|} \sum_{g \in G} u_1^g \overline{v_1^g} + u_2^g \overline{v_2^g} + \cdots + u_n^g \overline{v_n^g}
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{|G|}\sum_{g\in G}\overline{v_1^g}u_1^g + \overline{v_2^g}u_2^g + \cdots + \overline{v_n^g}u_n^g \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{[v_1^g, v_2^g, \ldots, v_n^g]}\begin{bmatrix} u_1^g \\ u_2^g \\ \cdots \\ u_n^g \end{bmatrix} \\
&= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}), \phi(g)(\vec{u})\rangle \\
&= [\vec{v}, \vec{u}].
\end{aligned}$$

We thus find that the mapping

$$[\cdot,\cdot]\colon M \times M \to \mathbb{C}$$

satisfies the conjugate symmetry axiom. We claim that the linearity in the first argument of $[\cdot,\cdot]$ is inherited from the linearity in the first argument of $\langle\cdot,\cdot\rangle$ and the linearity of mappings of the form ϕ_g for $g \in G$. This is illustrated below, letting a be a scalar, and letting $\vec{v}_1$ and $\vec{v}_2$ be elements in the module M.

$$\begin{aligned}
[a\vec{v}, \vec{u}] &= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(a\vec{v}), \phi(g)(\vec{u})\rangle \\
&= \frac{1}{|G|}\sum_{g\in G}\langle a\phi(g)(\vec{v}), \phi(g)(\vec{u})\rangle \\
&= \frac{1}{|G|}\sum_{g\in G}a\langle \phi(g)(\vec{v}), \phi(g)(\vec{u})\rangle \\
&= a\frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}), \phi(g)(\vec{u})\rangle \\
&= a[\vec{v}, \vec{u}].
\end{aligned}$$

$$\begin{aligned}
[\vec{v}_1 + \vec{v}_2, \vec{u}] &= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}_1 + \vec{v}_2), \phi(g)(\vec{u})\rangle \\
&= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}_1) + \phi(g)(\vec{v}_2), \phi(g)(\vec{u})\rangle \\
&= \frac{1}{|G|}\sum_{g\in G}\Big(\langle \phi(g)(\vec{v}_1), \phi(g)(\vec{u})\rangle + \langle \phi(g)(\vec{v}_2), \phi(g)(\vec{u})\rangle\Big) \\
&= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}_1), \phi(g)(\vec{u})\rangle + \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}_2), \phi(g)(\vec{u})\rangle \\
&[\vec{v}_1, \vec{u}] + [\vec{v}_2, \vec{u}].
\end{aligned}$$

Since $\langle \vec{u}, \vec{u}\rangle \geq 0$, we find that

$$\langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle \geq 0$$

for $g \in G$, so it is clear that $[\vec{u}, \vec{u}] \geq 0$. Similarly, we have that:

$$\frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle = 0 \Longleftrightarrow \sum_{g\in G}\langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle = 0$$

$$
\begin{aligned}
&\iff \forall g \in G \ \langle \phi(g)(\vec{u}), \phi(g)(\vec{u}) \rangle = 0 \\
&\iff \forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M \\
&\iff \vec{u} = \vec{0}_M.
\end{aligned}
$$

To show why the biconditional statement

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M \iff \vec{u} = \vec{0}_M,$$

begin by assuming that $\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M$. In particular, letting $e = e_G$ denote the identity element in G, we have that

$$\phi_e(\vec{u}) = \vec{0}_M.$$

Since

$$\phi \colon G \to \mathrm{Aut}(M)$$

is a group homomorphism, we have that ϕ must map the identity element $e = e_G$ of G to the identity morphism

$$\mathrm{id}_M = \mathrm{id} \colon M \to M$$

in the codomain of ϕ. So, in the case whereby

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M,$$

we have that:

$$
\begin{aligned}
\phi_e(\vec{u}) = \vec{0}_M &\implies \mathrm{id}(\vec{u}) = \vec{0}_M \\
&\implies \vec{u} = \vec{0}_M.
\end{aligned}
$$

We thus find that the implication whereby

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M \implies \vec{u} = \vec{0}_M$$

holds. Conversely, suppose that the equality $\vec{u} = \vec{0}_M$ holds. Since linear mappings map zero vectors to zero vectors, and since $\phi(g) \in \mathrm{Aut}(M)$ for all $g \in G$, we thus have that

$$\vec{u} = \vec{0}_M \implies \forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M$$

as desired.

Exercise 1.74. Prove that $[\phi(h)(\vec{v}), \phi(h)(\vec{u})] = [\vec{v}, \vec{u}]$.

Solution 1.75. By definition of the mapping

$$[\cdot, \cdot] \cdot M \times M \to \mathbb{C},$$

we have that:

$$[\phi(h)(\vec{v}), \phi(h)(\vec{u})] = \frac{1}{|G|} \sum_{g \in G} \langle \phi(g)(\phi(h)(\vec{v})), \phi(g)(\phi(h)(\vec{u})) \rangle.$$

It is convenient to write $\phi(g) = \phi_g$ and $\phi(h) = \phi_h$. We thus arrive at the following equality:

$$[\phi_h(\vec{v}), \phi_h(\vec{u})] = \frac{1}{|G|} \sum_{g \in G} \langle \phi_g(\phi_h(\vec{v})), \phi_g(\phi_h(\vec{u})) \rangle. \tag{1.1}$$

But recall that the mapping

$$\phi : G \to \operatorname{Aut}(V)$$

is a group homomorphism. We thus have that the equality given in (1.1) may be rewritten as follows:

$$[\phi_h(\vec{v}), \phi_h(\vec{u})] = \frac{1}{|G|} \sum_{g \in G} \langle \phi_{g \cdot h}(\vec{v}), \phi_{g \cdot h}(\vec{u}) \rangle.$$

But recall that the mapping on the underlying set of G whereby $g \mapsto g \cdot h$ for fixed $h \in G$ is a permutation of the underlying set of G. Therefore,

$$\begin{aligned} [\phi_h(\vec{v}), \phi_h(\vec{u})] &= \frac{1}{|G|} \sum_{g \in G} \langle \phi_{g \cdot h}(\vec{v}), \phi_{g \cdot h}(\vec{u}) \rangle \\ &= \frac{1}{|G|} \sum_{i \in G} \langle \phi_i(\vec{v}), \phi_i(\vec{u}) \rangle \\ &= [\vec{v}, \vec{u}] . \end{aligned}$$

Exercise 1.76. Recall that for groups A and B and $\gamma : B \to \operatorname{Aut}(A)$, then the group $A \rtimes_\gamma B$ is the set of pairs $\{(a, b) : a \in A, b \in B\}$ with product $(a, b) \cdot_{A \rtimes_\gamma B} (a', b') = (a\gamma_b(a'), bb')$. Find an example of p, q, and γ such that $\mathbb{Z}_p \rtimes_\gamma \mathbb{Z}_q$ is solvable but not abelian.

Solution 1.77. We begin by proving a useful preliminary result. We claim that given a finite group G, if G has a subgroup H of index 2, then H must be normal in G. For fixed h_1 and h_2, the mappings $h \mapsto h_1 \cdot h$ and $h \mapsto h \cdot h_2$ on H are both permutations of H. So it is clear that $hH = Hh$ for $h \in H$. But we also know that the mappings $g \mapsto h_1 \cdot g$ and $g \mapsto g \cdot h_2$ on G are both permutations of G. We may thus deduce that the mappings $g \mapsto h_1 \cdot g$ and $g \mapsto g \cdot h_2$ on $G \setminus H$ are both permutations of $G \setminus H$. We thus arrive at the following incomplete Cayley table, where mappings denoted using the symbol ρ or the symbol μ are permutations of $G \setminus H$, writing $H = \{h_1, h_2, \ldots, h_n\}$ and $G \setminus H = \{g_1, g_2, \ldots, g_n\}$, noting that $|H| = |G \setminus H|$.

$\circ$	h_1	h_2	$\cdots$	h_n	g_1	g_2	$\cdots$	g_n
h_1					$g_{\rho_1^1}$	$g_{\rho_1^2}$	$\cdots$	$g_{\rho_1^n}$
h_2					$g_{\rho_2^1}$	$g_{\rho_2^2}$	$\cdots$	$g_{\rho_2^n}$
$\vdots$					$\vdots$	$\vdots$	$\ddots$	$\vdots$
h_n					$g_{\rho_n^1}$	$g_{\rho_n^2}$	$\cdots$	$g_{\rho_n^n}$
g_1	$g_{\mu_1^1}$	$g_{\mu_2^1}$	$\cdots$	$g_{\mu_n^1}$				
g_2	$g_{\mu_1^2}$	$g_{\mu_2^2}$	$\cdots$	$g_{\mu_n^2}$				
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$				
g_n	$g_{\mu_1^n}$	$g_{\mu_2^n}$	$\cdots$	$g_{\mu_n^n}$				

But since

$$\{g_{\mu_1^i}, g_{\mu_2^i}, \ldots, g_{\mu_n^i}\} = \{g_{\rho_1^i}, g_{\rho_2^i}, \ldots, g_{\rho_n^i}\}$$

for all indices i, we thus find that

$$gH = Hg$$

for all $g \in G \setminus H$ as desired.

Now, let $p = 3$, let $q = 2$, and define $\gamma\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ so that γ_0 is the identity automorphism on $\mathbb{Z}_3$, and γ_1 is the automorphism on $\mathbb{Z}_3$ mapping each element in $\mathbb{Z}_3$ to its inverse. As discussed in class, we have that

$$\mathbb{Z}_p \rtimes_\gamma \mathbb{Z}_q = \mathbb{Z}_3 \rtimes_\gamma \mathbb{Z}_2 \cong D_3 \cong S_3.$$

We adopt the notation indicated below for dihedral groups introduced in class:

$$D_3 = \{1, a, a^2, b, ba, ba^2\}.$$

It is clear that the set $\{1, a, a^2\}$ forms a cyclic subgroup of D_3 which is isomorphic to $\mathbb{Z}_3$. From the preliminary result given towards the beginning of our present solution, since $\{1, a, a^2\}$ is a subgroup of D_3 of index 2, we have that this subgroup must in fact be a normal subgroup of D_3. This is also easily seen from a geometric perspective in the sense outlined as follows. Observe that the elements in the cyclic subgroup $\{1, a, a^2\}$ are precisely the orientation-preserving isometries in D_3. Recall that the composition of two orientation-preserving isometries must be an orientation-preserving isometry. Similarly, the composition of an orientation-preserving isometry and an orientation-reversing isometry, or vice-versa, yields an orientation-reversing isometry. Finally, the composition of two orientation-reversing isometries must yield an orientation-preserving isometry. It is thus seen that the rotation subgroup $\{1, a, a^2\}$ must be the kernal of a homomorphism from D_3 to $\mathbb{Z}_2$, thus showing that $\{1, a, a^2\}$ forms a normal subgroup of D_3, as desired.

We thus arrive at the subnormal series given below:

$$\{1\} \lhd \{1, a, a^2\} \lhd D_3 \cong \mathbb{Z}_p \rtimes_\gamma \mathbb{Z}_q.$$

Of course, the group

$$\mathbb{Z}_3 \rtimes_\gamma \mathbb{Z}_2 \cong D_3 \cong S_3$$

is not abelian. But given the subnormal series

$$\{1\} \lhd \{1, a, a^2\} \lhd D_3 \cong \mathbb{Z}_p \rtimes_\gamma \mathbb{Z}_q,$$

and given that

$$D_3/\{1, a, a^2\} \cong \mathbb{Z}_2$$

and

$$\{1, a, a^2\}/\{1\} \cong \mathbb{Z}_3,$$

we have that the above subnormal series is a composition series whose composition factors are abelian. We thus have that $\mathbb{Z}_p \rtimes_\gamma \mathbb{Z}_q$ is solvable but not abelian.