MATH 6121: selected solutions

WRITTEN AND FORMATTED BY JOHN M. CAMPBELL
jmaxwellcampbell@gmail.com

1 MATH 6121 exercises

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.

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

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.

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

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.

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

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

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 $\operatorname{im}(\phi) \leq H$ with respect to $\circ_H$, where $\operatorname{im}(\phi) = \{\phi(g) : g \in G\}$.

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 $\operatorname{im}(\phi)$. Since $\phi\colon G \to H$ is a homomorphism, we have that

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

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

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

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 $\operatorname{im}(\psi)$.

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 $\phi_g \colon H \to gH$ 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 $g_1 H$ and $g_2 H$ 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

$$G = g_1 H \cup g_2 H \cup \cdots \cup g_n H$$

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 $\text{order}(g)$ denote the smallest $n \in \mathbb{N}$ such that $g^n = e$. Show that $\text{order}(g)$ 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 $\text{order}(g)$ divides $|G|$ as desired.

Exercise 1.23. Prove that $\text{Stab}(x)$ 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 $\text{Stab}(x)$. Now consider the following expression: $(g_1 g_2) \bullet x$. By definition of a group action, we have that

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

thus proving that $\text{Stab}(x)$ 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 $\text{Stab}(x) \leq G$.

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 $\bullet \colon G \times X \to X$ denote a group action. Let $x, y \in X$, so that $\text{Orbit}(x)$ and $\text{Orbit}(y)$ are arbitrary orbits. Suppose that $\text{Orbit}(x) \cap \text{Orbit}(y) \neq \varnothing$. Let

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

denote an element in the nonempty intersection $\text{Orbit}(x) \cap \text{Orbit}(y)$. 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

$$g_1 g_3 = g_2 g_4.$$

We thus have that

$$(g_1 g_3) \bullet x = (g_2 g_4) \bullet x,$$

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 $g_1 H \circ_{G/H} g_2 H = g_1 g_2 H$ 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 $g_1 H \circ_{G/H} g_2 H$ does not depend on the coset representatives of the cosets $g_1 H$ and $g_2 H$. So, suppose that $g_1 H = g_3 H$ and $g_2 H = g_4 H$, 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:

$$g_1 g_2 H = g_3 g_4 H.$$

Since $g_1 H = g_3 H$, let $g_3 = g_1 h_1$, where $h_1 \in H$. Similarly, since $g_2 H = g_4 H$, let $g_4 = g_2 h_2$, with $h_2 \in H$. So, it remains to prove that

$$g_1 g_2 H = g_1 h_1 g_2 h_2 H.$$

But since $H \trianglelefteq G$, we have that $gH = Hg$ for all $g \in G$. Since $h_1 g_2 \in Hg_2 = g_2 H$, let $h_1 g_2 = g_2 h_3$, where $h_3 \in H$. We thus have that

$$g_1 h_1 g_2 h_2 H = g_1 g_2 h_3 h_2 H.$$

But it is clear that

$$g_1 g_2 h_3 h_2 H = g_1 g_2 H$$

since the mapping $h \mapsto h_3 h_2 h$ is a bijection on H. We thus have that

$$g_3 g_4 H = g_1 g_2 H$$

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:

$$\begin{aligned} g_1 H \circ (g_2 H \circ g_3 H) &= g_1 H \circ ((g_2 g_3) H) \\ &= g_1 (g_2 g_3) H \\ &= (g_1 g_2) g_3 H \\ &= (g_1 g_2) H \circ g_3 H \\ &= (g_1 H \circ g_2 H) \circ g_3 H. \end{aligned}$$

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

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

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

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

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 $\sigma\colon \mathbb{Z} \to \mathbb{Z}$ 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 $\sigma^{-1}\colon \mathbb{Z} \to \mathbb{Z}$ 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 $\phi: G \to H$, we have that $\ker(\phi) \trianglelefteq G$, and furthermore, we have that $G/\ker(\phi) \cong \operatorname{im}(\phi)$.

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

$$\psi_\phi = \psi: G/\ker(\phi) \to \operatorname{im}(\phi)$$

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 $\phi(g) \in \operatorname{im}(\phi)$ since $\phi: G \to H$. 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 $\phi: G \to H$ 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:

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

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 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 $k_1 HK$. But recall that $hK = Kh$ for all $h \in H$. Given an element

$$k_1 h_1 k_2 \in k_1 HK$$

in the left coset $k_1 HK$, we have that

$$k_1 h_1 k_2 = h_1 k_3 k_2 = h_1 \left(k_3 k_2 k_1^{-1} \right) k_1 \in HK k_1$$

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

$$k_1 HK \subseteq HK k_1.$$

Conversely, given an element

$$h_1 k_2 k_1 \in HK k_1,$$

we have that

$$h_1 k_2 k_1 = h_1 k_3 = k_4 h_1 = k_1 \left(k_1^{-1} k_4 \right) h_1 = k_1 k_5 h_1 = k_1 h_1 k_6 \in k_1 HK,$$

the proving the reverse inclusion whereby

$$k_1 HK \supseteq HK k_1.$$

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 $\tau(h_1 h_2)$:

$$\tau(h_1 h_2) = (h_1 h_2)K.$$

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

$$\tau(h_1 h_2) = h_1 h_2 K = (h_1 K)(h_2 K) = \tau(h_1 \tau(h_2)),$$

thus proving that τ is a group homomorphism.

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

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

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. $\square$

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

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

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 $x_1, x_2 \in \mathrm{dom}(f)$, we have that:

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

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

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

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

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

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:

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

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:

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

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

$$\pi\colon G \to G/N$$

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

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

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

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

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

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

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

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

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

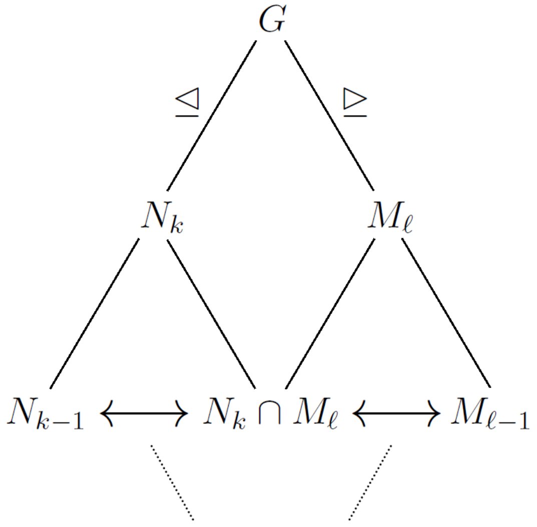
$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

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.



composition factors permute

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.

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

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

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

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

$\circ$	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.

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

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

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

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

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

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

$$\begin{tikzcd}\{1\} \arrow[r] & A \arrow[r, "\alpha"] & A\rtimes_\phi B \arrow[r, "\beta"] & B \arrow[r] & \{1\}.\end{tikzcd}$$

is an exact sequence.

Solution 1.56. Recall that a sequence

$$\begin{tikzcd}G_0 \arrow[r, "f_1"] & G_1 \arrow[r, "f_2"] & G_2 \arrow[r, "f_3"] & \cdots \arrow[r, "f_n"] & G_n\end{tikzcd}$$

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 $L \trianglelefteq H$. 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 $\text{Stab}_G(x_i)$ is a subgroup of G, by Lagrange's theorem, each expression of the form $\frac{|G|}{|\text{Stab}_G(x_i)|}$ 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

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

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

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

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

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

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 $y \in \text{Fix}(G)$ is arbitrary. Given that $\forall g \in G \ g \bullet y = y$, consider the expression $\text{Stab}_G(y)$. By definition of the stabilizer of an element, we have that

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

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

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

Conversely, let

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

be arbitrary. Since $G = \text{Stab}_G(y)$, 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

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

thus proving that the reverse inclusion whereby

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

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

Now, recall that

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

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

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

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

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

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

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*

$$\binom{p^n m}{p^n} \equiv m \pmod{p}.$$

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 $H \leq G$ 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

$$\bullet : H \times X \to X$$

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

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

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

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 $\{1, 2, \ldots, p^n\}$ to $\{1, 2, \ldots, p^n\}$, 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 $\text{Fix}(H)$ 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 $\text{Fig}(G) = Z(G)$ with respect to the conjugation action on G.

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

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

$$= Z(G).$$

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

$$\bullet\colon G \times X \to X$$

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 theorem) 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. *(3^{rd} 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 2^{nd} 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. *(4^{th} 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

$$\phi\colon G \to \operatorname{Aut}(M)$$

be a representation of the finite group G over a field F in which $|G|$ is invertible. Define the mapping

$$[\cdot,\cdot]\colon M \times M \to \mathbb{C}$$

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 $\overline{[\vec{u},\vec{v}]}$.

$$\begin{aligned}
\overline{[\vec{u},\vec{v}]} &= \overline{\frac{1}{|G|}\sum_{g\in G}\langle\phi(g)(\vec{u}),\phi(g)(\vec{v})\rangle} \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\langle\phi(g)(\vec{u}),\phi(g)(\vec{v})\rangle} \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\overline{[\phi(g)(\vec{u})]_{\mathcal{B}}^{T}}[\phi(g)(\vec{v})]_{\mathcal{B}}} \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\overline{[u_1^g,u_2^g,\ldots,u_n^g]}\begin{bmatrix} v_1^g \\ v_2^g \\ \cdots \\ v_n^g \end{bmatrix}} \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{[\overline{u_1^g},\overline{u_2^g},\ldots,\overline{u_n^g}]\begin{bmatrix} v_1^g \\ v_2^g \\ \cdots \\ v_n^g \end{bmatrix}} \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\overline{u_1^g}v_1^g + \overline{u_2^g}v_2^g + \cdots + \overline{u_n^g}v_n^g} \\
&= \frac{1}{|G|}\sum_{g\in G}u_1^g\overline{v_1^g} + u_2^g\overline{v_2^g} + \cdots + u_n^g\overline{v_n^g}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{|G|}\sum_{g\in G}\overline{v_1^g}u_1^g + \overline{v_2^g}u_2^g + \cdots + \overline{v_n^g}u_n^g \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{[v_1^g, v_2^g, \dots, v_n^g]}\begin{bmatrix} u_1^g \\ u_2^g \\ \cdots \\ u_n^g \end{bmatrix} \\
&= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{v}), \phi(g)(\vec{u})\rangle \\
&= [\vec{v}, \vec{u}].
\end{aligned}
$$

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:

$$\frac{1}{|G|}\sum_{g\in G}\langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle = 0 \Longleftrightarrow \sum_{g\in G}\langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle = 0$$

$$\begin{aligned}&\Longleftrightarrow \forall g \in G \ \langle \phi(g)(\vec{u}), \phi(g)(\vec{u})\rangle = 0\\ &\Longleftrightarrow \forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M\\ &\Longleftrightarrow \vec{u} = \vec{0}_M.\end{aligned}$$

To show why the biconditional statement

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M \Longleftrightarrow \vec{u} = \vec{0}_M,$$

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

$$\phi\colon G \to \text{Aut}(M)$$

is a group homomorphism, we have that ϕ must map the identity element $e = e_G$ of G to the identity morphism

$$\text{id}_M = \text{id}\colon M \to M$$

in the codomain of ϕ. So, in the case whereby

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M,$$

we have that:

$$\begin{aligned}\phi_e(\vec{u}) = \vec{0}_M &\Longrightarrow \text{id}(\vec{u}) = \vec{0}_M\\ &\Longrightarrow \vec{u} = \vec{0}_M.\end{aligned}$$

We thus find that the implication whereby

$$\forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M \Longrightarrow \vec{u} = \vec{0}_M$$

holds. Conversely, suppose that the equality $\vec{u} = \vec{0}_M$ holds. Since linear mappings map zero vectors to zero vectors, and since $\phi(g) \in \text{Aut}(M)$ for all $g \in G$, we thus have that

$$\vec{u} = \vec{0}_M \Longrightarrow \forall g \in G \ \phi(g)(\vec{u}) = \vec{0}_M$$

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

$$\phi : G \to \mathrm{Aut}(V)$$

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 $\gamma : B \to \mathrm{Aut}(A)$, 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 $g \in G \smallsetminus H$ as desired.

Now, let $p = 3$, let $q = 2$, and define $\gamma: \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ 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.

Exercise 1.78. Consider the following series:

$$Z_0(G) := \{1\},$$

$$Z_1(G) = Z(G) = \{g \in G \mid \forall g \in G \; gx = xg\} \trianglelefteq G.$$

Then, we recall the map $\pi: G \to G/Z_1(G)$, and note that $Z(G/Z_1(G)) \trianglelefteq G/Z_1(G)$. Thus, we may use the fourth isomorphism theorem to create $Z_2(G)$ as the group corresponding to $Z(G/Z_1(G))$, and we have that $Z_1(G) \trianglelefteq Z_2(G)$, in general we have $Z_i(G)$ as the subgroup corresponding to $Z(G/Z_{i-1}(G))$, and $Z_{i-1}(G) \trianglelefteq Z_i(G) \trianglelefteq G$. Hence we have

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

which is called the Upper Central Series of G. If G is a nontrivial finite group then this series stabilizes at some point.

Def: We say that G is nilpotent of index k if there exists an index k such that $Z_k(G) = G$ and $Z_{k-1}(G) \neq G$.

So, for G a finite group, show that all abelian groups are nilpotent, and that all nilpotent groups are solvable. We note that the converse of each statement is not true.

Solution 1.79. So, let G be a finite group, and suppose that G is abelian. In this case, we have that:

$$\begin{aligned} &Z_0(G) := \{1\} \\ &Z_1(G) = Z(G) = G \trianglelefteq G. \end{aligned}$$

We thus have that there exists an index $i = 1$ such that $Z_i(G) = G$ and $Z_{i-1}(G) \neq G$. We thus find that non-trivial abelian groups are nilpotent of index 1.

Again letting G be a finite group, suppose that G is nilpotent of index k. Now recall that the Upper Central Series

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

is defined so that for each index i, $Z_i(G)$ is the subgroup corresponding to $Z(G/Z_{i-1}(G))$ with respect to the fourth isomorphism theorem. Since

$$Z_{i-1}(G)/Z_{i-1}(G) \trianglelefteq Z(G/Z_{i-1}(G)) \trianglelefteq G/Z_{i-1}(G),$$

by the fourth isomorphism theorem, we have that there is a corresponding subgroup H whereby

$$Z_{i-1}(G) \trianglelefteq H \trianglelefteq G,$$

and this subgroup is given by the inverse image of $Z(G/Z_{i-1}(G))$ with respect to the projection morphism π.

Now, to prove that G is necessarily solvable, our strategy is to prove that

$$Z_{i+1}/Z_i(G) \subseteq Z(G/Z_i(G))$$

for all indices i. So, let i be an arbitrary index. According to the Fourth Isomorphism Theorem, we have that:

$$\begin{aligned} Z_i(G) &= \bigcup Z(G/Z_{i-1}(G)), \\ Z_{i+1}(G) &= \bigcup Z(G/Z_i(G)). \end{aligned}$$

Now, to prove that each element in the quotient group $Z_{i+1}(G)/Z_i(G)$ is in the center of $G/Z_i(G)$, we begin by constructing an arbitrary element in the subgroup $Z_{i+1}(G)$. Let $g_1 \in G$ be such that the left coset $g_1Z_i(G) \in G/Z_i(G)$ is actually in the center $Z(G/Z_i(G))$ of the quotient group $G/Z_i(G)$. Now, let z_1 be an arbitrary element in $Z_{i+1}(G)$, so that the product

$$g_1z_1 \in Z_{i+1}(G)$$

is an arbitrary element in $Z_{i+1}(G)$. Now consider the left coset

$$g_1z_1Z_i(G) \in Z_{i+1}(G)/Z_i(G).$$

We have chosen the elements g_1 and z_1 so that $g_1z_1Z_i(G)$ is an arbitrary element in the quotient group $Z_{i+1}(G)/Z_i(G)$. Now, recall that our strategy for proving that G is solvable is to prove that the quotient group $Z_{i+1}(G)/Z_i(G)$ satisfies the following inclusion:

$$Z_{i+1}(G)/Z_i(G) \subseteq Z(G/Z_i(G)).$$

So, we are interested in proving that the coset $g_1z_1Z_i(G)$ commutes with each coset in $G/Z_i(G)$. Now, let $g_2 \in G$ be arbitrary, so that $g_2Z_i(G)$ is an arbitrary element in $G/Z_i(G)$. Since $z_1 \in Z_i(G)$ and since

$$g_1Z_i(G) \in Z(G/Z_i(G)),$$

we thus have that:

$$\begin{aligned}[g_1z_1Z_i(G)] \bullet [g_2Z_i(G)] &= [g_1Z_i(G)] \bullet [g_2Z_i(G)] \\ &= [g_2Z_i(G)] \bullet [g_1Z_i(G)] \\ &= [g_2Z_i(G)] \bullet [g_1z_1Z_i(G)].\end{aligned}$$

Since

$$Z_{i+1}(G)/Z_i(G) \subseteq Z(G/Z_i(G)),$$

we have that each quotient of the form $Z_{i+1}(G)/Z_i(G)$ is abelian. This effectively proves that G is solvable: even if a subnormal factor of the form $Z_{i+1}(G)/Z_i(G)$ may not be simple, the fourth isomorphism theorem may be applied to construct a subseries consisting of finite abelian simple groups, i.e., groups which are isomorphic to $\mathbb{Z}_p$.

Exercise 1.80. We assume that G is a finite nontrivial group, and define $G^0 = G$ and

$$G^1 = [G, G] := \langle ghg^{-1}h^{-1} \mid g, h \in G\rangle.$$

Show that $[G, G] \trianglelefteq G$ and that $G/[G, G]$ is abelian. Furthermore, show that if $H \triangleleft G$ is such that G/H is abelian then $[G, G] \leq H$. Let

$$G^i = [G, G^{i-1}] = \langle ghg^{-1}h^{-1} \mid g \in G, h \in G^{i-1}\rangle.$$

Show that $G^i \trianglelefteq G$, then we have the Lower Central Series of G given by

$$\ldots \trianglelefteq G^2 \trianglelefteq G^1 \trianglelefteq G,$$

which will stabilize at some point since G is finite. Show that $G^k = \{1\}$ if and only if G is nilpotent of index k. (Hint: $Z_i(G) \leq G^{k-i-1} \leq Z_{i+1}(G)$.)

Solution 1.81. By definition of the commutator subgroup, $[G, G]$ is precisely the subgroup of G generated by all the commutators. We thus have that $[G, G] \leq G$ by definition of the commutator subgroup. Let c be an element in this subgroup, and let $g \in G$ be arbitrary. Consider the product $g \cdot c \cdot g^{-1} \in G$. Rewrite this product in the following manner:

$$\begin{aligned} g \cdot c \cdot g^{-1} &= (g \cdot c \cdot g^{-1}) \cdot (c^{-1} \cdot c) \\ &= (g \cdot c \cdot g^{-1} \cdot c^{-1}) \cdot c \end{aligned}$$

We thus find that a product of the form

$$g \cdot c \cdot g^{-1} = (g \cdot c \cdot g^{-1} \cdot c^{-1}) \cdot c$$

must be equal to a product consisting of an element c in the subgroup $[G, G] \leq G$ and another element

$$g \cdot c \cdot g^{-1} \cdot c^{-1} \in [G, G] \leq G$$

in the commutatory subgroup $[G, G]$. But since $[G, G]$ has to be closed with respect to the underlying binary operation on G, we thus have that $g \cdot c \cdot g^{-1}$ must be in $[G, G]$. We thus have that each element in $g[G, G]$ is in $[G, G]g$ for $g \in G$, and a symmetric argument proves the reverse inclusion. We thus have that $[G, G] \trianglelefteq G$ as desired. Now consider the quotient group $G/[G, G]$. Let g and h be arbitrary elements in G, so that $g[G, G]$ and $h[G, G]$ are arbitrary elements in the quotient group $G/[G, G]$. Consider the following product of cosets:

$$(g[G, G]) \cdot (h[G, G]) = gh[G, G].$$

Since the product

$$h^{-1}g^{-1}hg$$

is in the commutator subgroup, we thus find that the product

$$gh\left(h^{-1}g^{-1}hg\right)$$

is in the coset $gh[G, G]$. We thus have that

$$hg \in gh[G, G].$$

But we also have that

$$hg \in hg[G, G].$$

We thus find that the cosets $gh[G, G]$ and $hg[G, G]$ have a nonempty intersection. But recall that two cosets in a given quotient group are either equal or disjoint. Since $gh[G, G]$ and $hg[G, G]$ are not disjoint, we thus have that $gh[G, G] = hg[G, G]$. We thus find that

$$(g[G, G]) \cdot (h[G, G]) = (h[G, G]) \cdot (g[G, G])$$

for two elements $g[G, G]$ and $h[G, G]$ in $G/[G, G]$, thus proving that $G/[G, G]$ is abelian. Now suppose that $H \lhd G$ is such that G/H is abelian, so that:

$$g_1 g_2 H = H g_1 g_2 = g_2 g_1 H = H g_2 g_1$$

for $g_1, g_2 \in G$. Now, since

$$g_1 g_2 H = H g_2 g_1$$

for all $g_1, g_2 \in G$, and since $e \in H$ we have that:

$$\forall g_1, g_2 \in G \; \exists h \in H \;\; g_1 g_2 = h g_2 g_1.$$

Therefore,

$$g_1 g_2 g_1^{-1} g_2^{-1} \in H$$

for all $g_1, g_2 \in G$. But since the commutator subgroup $[G, G]$ is generated by expressions of the form $g_1 g_2 g_1^{-1} g_2^{-1}$ for $g_1, g_2 \in G$, and since each such generator is in H, we thus find that $[G, G] \subseteq H$. Moreover, since $[G, G] \leq G$ and $H \leq G$, we may thus deduce that $[G, G] \leq H$.

Letting i be an index, we have that $G^i \leq G$ by definition, since G^i is defined as a subgroup generated by certain elements in G. Observe that each generator of the form

$$ghg^{-1}h^{-1}$$

for $g \in G$ and $h \in G^1 \subseteq G$ must be in G^1, since G^1 is generated by expressions of the form $aba^{-1}b^{-1}$ for $a, b \in G$. So, $G^2 \subseteq G^1$. Similarly, each generator of the form

$$ghg^{-1}h^{-1}$$

for $g \in G$ and $h \in G^2 \subseteq G_1$ must be in G_2, since G_2 is generated by expressions of the form $aba^{-1}b^{-1}$ for $a \in G$ and $b \in G^1 \subseteq G$. Continuing in this manner inductively, we thus arrive at the following inclusions:

$$\cdots \subseteq G^2 \subseteq G^1 \subseteq G.$$

Now, let $g \in G$, and let c be an arbitrary element in G^i. Consider the following product:

$$g \cdot c \cdot g^{-1}.$$

Now, rewrite this product as follows:

$$(g \cdot c \cdot g^{-1} \cdot c^{-1}) \cdot c.$$

Since $g \in G$ and $c \in G^i$, we have that $g \cdot c \cdot g^{-1} \cdot c^{-1}$ is a generator for the group G^{i+1}. But we also know that $G^{i+1} \subseteq G^i$. So, $g \cdot c \cdot g^{-1} \cdot c^{-1}$ is in G^i. But we also know that $c \in G^i$. We thus have that

$$g \cdot c \cdot g^{-1} \in G^i,$$

proving the inclusion whereby

$$gG^i g^{-1} \subseteq G^i.$$

A symmetric argument proves the reverse inclusion, which proves that G^i is normal as a subgroup of G.

As indicated in the hint given for the above exercise, we have that $Z_i(G) \leq G^{k-i-1} \leq Z_{i+1}(G)$. This may be shown inductively. Suppose that $G^k = \{1\}$, with:

$$\{1\} = G^k \trianglelefteq \cdots \trianglelefteq G^2 \trianglelefteq G^1 \trianglelefteq G.$$

But then since $Z_i(G) \leq G^{k-i-1} \leq Z_{i+1}(G)$, we arrive at the following series:

$$\{1\} = G^k \leq Z_0(G) \leq G^{k-1} \leq Z_1(G) \leq G^{k-2} \leq Z_2(G) \leq \cdots \leq G^1 \leq Z_{k-1}(G) \leq G \leq Z_k(G).$$

But then $Z_k(G) = G$. Since the sequence

$$\{1\} = G^k \trianglelefteq \cdots \trianglelefteq G^2 \trianglelefteq G^1 \trianglelefteq G$$

is finite, we have that the inequalities in this sequence must be strict. Therefore, $Z_{k-1}(G) \neq G$.

Exercise 1.82. Let G be a nontrivial finite group. Then define $G^{(0)} = G$ and

$$G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right] \trianglelefteq G^{(i-1)}.$$

We note that it is not true in general that $G^{(i)} \trianglelefteq G$. We call the following normal series a Derived Series, and since G is finite it stabilizes at some point:

$$G^{(k)} \trianglelefteq \cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)}.$$

Show that G is solvable if and only if $G^{(k)} = \{1\}$ for some k.

(Hint: Use the fact that $G^{(i+1)}/G^{(i)}$ is abelian, this implies that $G^{(i+1)} = \left[H_{s-i}, H_{s-ki}\right] \trianglelefteq H_{s-i-1}$ where $\{1\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_k = G$).

Solution 1.83. We have previously shown that $G/[G,G]$ is abelian. For an index i, we have that $\left[G^{(i-1)}, G^{(i-1)}\right]$ is the group generated by all expressions of the form $ghg^{-1}h^{-1}$ for g and h in $G^{(i-1)}$. Since $\left[G^{(i-1)}, G^{(i-1)}\right]$ is a group by definition, and since

$$G^{(i-1)} = \left[G^{(i-2)}, G^{(i-2)}\right]$$

is a group by definition, and since $\left[G^{(i-1)}, G^{(i-1)}\right]$ is generated by elements in the group $G^{(i-1)}$, we have that:

$$G^{(i)} \leq G^{(i-1)}.$$

Now, let g be an arbitrary element in $G^{(i-1)}$, and let c be an arbitrary element in $G^{(i)}$. Consider the following expression:

$$g \cdot c \cdot g^{-1} \in gG^{(i)}g^{-1}.$$

Now, observe that the product

$$g \cdot c \cdot g^{-1}$$

may be rewritten as

$$g \cdot c \cdot g^{-1} \cdot c^{-1} \cdot c.$$

But since $g \in G^{(i-1)}$, and since c is an element in a group $G^{(i)}$ generated by certain products of elements in $G^{(i-1)}$, it is clear that

$$g \cdot c \cdot g^{-1} \cdot c^{-1} \in G^{(i)}$$

so that

$$g \cdot c \cdot g^{-1} \cdot c^{-1} \cdot c \in G^{(i)}c = G^{(i)}$$

thus proving the inclusion whereby

$$gG^{(i)}g^{-1} \subseteq G^{(i)}.$$

A symmetric argument may be used to prove the reverse inclusion, in order to show that:

$$G^{(i)} \trianglelefteq G^{(i-1)}.$$

As indicated above, we thus arrive at a subnormal series of the following form:

$$G^{(k)} \trianglelefteq \cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)}.$$

Now consider the quotient group $G^{(i+1)}/G^{(i)}$, letting i be an index. Let g_1 and g_2 be arbitrary elements in $G^{(i+1)}$. Let c be an element in $G^{(i)}$. Consider the following expression:

$$g_1 \cdot g_2 \cdot c \cdot g_2^{-1} \cdot g_1^{-1}.$$

We know that

$$g_2 \cdot c \cdot g_2^{-1} \in G^{(i)}$$

since $G^{(i)}$ is normal in $G^{(i+1)}$. Since

$$g_2 \cdot c \cdot g_2^{-1} \in G^{(i)}$$

and since $G^{(i)} \trianglelefteq G^{(i+1)}$, we thus have that

$$g_1 \cdot g_2 \cdot c \cdot g_2^{-1} \cdot g_1^{-1} \in G^{(i)},$$

thus proving the inclusion whereby

$$g_1 \cdot g_2 \cdot G^{(i)} \cdot g_2^{-1} \cdot g_1^{-1} \subseteq G^{(i)},$$

which proves the inclusion whereby

$$g_1 \cdot g_2 \cdot G^{(i)} \subseteq G^{(i)} g_1 g_2.$$

A symmetric argument may be used to prove the reverse inclusion. So, each quotient in the subnormal series

$$G^{(k)} \trianglelefteq \cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)}$$

is abelian. So, by definition of a solvable group, if $G^{(k)} = \{1\}$ for some k, then G is solvable. Conversely, suppose that G is abelian, and let

$$\{1\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_k = G$$

be a subnormal series for G such that each quotient group of the form H_{i+1}/H_i is abelian. But the quotient H_{i+1}/H_i is abelian if and only if H_i includes $H_{i+1}^{(1)}$[8]. So, H_k includes $G^{(1)}$. So we obtain a series of the following form:

$$\{1\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq H_k = G.$$

Continuing in this manner, since $H_0/\{1\}$ is abelian and H_1/H_0 is abelian, we find that $G(k) = \{1\}$ for some k.

Exercise 1.84. What can you say about groups of order 2014? Are they simple? Abelian? Nilpotent? Solvable? Note that $2014 = 2 \cdot 19 \cdot 53$.

Solution 1.85. Let G be a group of order $2014 = 2 \cdot 19 \cdot 53$. Let n_2, n_{19}, and n_{53} respectively denote: the number of Sylow 2-subgroups of G, the number of Sylow 19-subgroups of G, and the number of Sylow 53-subgroups of G. From Sylow theory, we have that:

(i) $n_{19} \geq 1$;

(ii) $n_{19} \in \{1, 2, 19, 38, 53, 106, 1007, 2014\}$; and

(iii) $n_{19} \in \{1\}$.

Now recall that Sylow p-subgroups are all conjugate to one another. Since n_{19}, we thus have that there exists a subgroup of G of order 19 which is a normal subgroup of G. Therefore, G is not simple.

It is clear that a group of order 2014 may or may not be abelian. For example, the cyclic group $\mathbb{Z}/2014\mathbb{Z}$ is abelian. However, the dihedral group of order 2014 is not abelian.

[8] See `https://en.wikipedia.org/wiki/Solvable_group`.

It is easily seen that the order of the quotient of a finite group by its center is not a prime number. Using this property along with Lagrange's theorem, we have that:

$$|Z(G)| = \{2, 19, 53, 2014\}.$$

If $Z(G) = 2014$, then G is abelian, and abelian groups are nilpotent. So, suppose that:

$$|Z(G)| = \{2, 19, 53\}.$$

Now suppose that $|Z(G)| = 53$. In this case, we have that

$$|G/Z(G)| = 2 \cdot 19.$$

Using Sylow theory, we know that since $|G/Z(G)| = 2 \cdot 19$, there must be a normal cyclic subgroup of $G/Z(G)$ of order 19. Using this property, it is easily seen that $G/Z(G)$ is either isomorphic to $\mathbb{Z}/38\mathbb{Z}$ or D_{19}. In the former case, $Z(G/Z(G)) = G/Z(G)$, and in the latter case, we have that $Z(G/Z(G))$ is trivial. Recall that the center of a dihedral group of the form D_n for odd n is trivial. In the former case, the Upper Central Series is of the form

$$\{1\} \trianglelefteq Z(G) \trianglelefteq G,$$

and in the latter case, the Upper Central Series is of the form

$$\{1\} \trianglelefteq Z(G).$$

So, in the case whereby $|Z(G)| = 53$, we find that G may or may not be nilpotent, since there may or may not be an index k such that $Z_k(G) = G$ and $Z_{k-1}(G) \neq G$.

But is it even possible that $|Z(G)| = 53$? More specifically, does there exist a group G of order 2014 such that $G/Z(G)$ is isomorphic to D_{19}? Consider the direct product

$$D_{19} \times (\mathbb{Z}/53\mathbb{Z}).$$

We know that the center of D_{19} is trivial. So, an element

$$(d_1, z_1) \in D_{19} \times (\mathbb{Z}/53\mathbb{Z})$$

commutes with each element

$$(d_2, z_2) \in D_{19} \times (\mathbb{Z}/53\mathbb{Z})$$

if and only if $d_1 = e$. So, letting

$$G = D_{19} \times (\mathbb{Z}/53\mathbb{Z})$$

with

$$|G| = 2014,$$

we have that

$$Z(G) \cong \mathbb{Z}/53\mathbb{Z},$$

and we thus have that

$$G/Z(G) \cong D_{19}.$$

But then we have that $Z(G/Z(G))$ is trivial, and as discussed above, in this case we have that the Upper Central Series is given by the sequence whereby:

$$\{1\} \trianglelefteq Z(G) \trianglelefteq Z(G) \trianglelefteq Z(G) \trianglelefteq \cdots,$$

thus proving that there exists a group

$$G = D_{19} \times (\mathbb{Z}/53\mathbb{Z})$$

of order 2014 which is not nilpotent. On the other hand, there exist abelian groups of order 2014 such as $\mathbb{Z}/2014\mathbb{Z}$, and nontrivial abelian groups are nilpotent.

Now, given a group G of order 2014, is G solvable? We have previously shown using Sylow theory that there exists a unique Sylow p-subgroup H_{19} of G, and since $n_{19} = 1$, we have that H_{19} must be a normal subgroup of G:

$$H_{19} \triangleleft G.$$

A similar argument shows that there is a unique subgroup H_{53} of G of order 53 which is also a normal subgroup of G. So, G/H_{53} is either cyclic, or is isomorphic to the dihedral group D_{19}. In the case whereby

$$G/H_{53} \cong \mathbb{Z}/38\mathbb{Z},$$

we have that G is solvable, since the subnormal series

$$\{e\} \triangleleft H_{53} \triangleleft G$$

is a composition series with abelian composition factors. Now suppose that:

$$G/H_{53} \cong D_{19}.$$

The subgroup of D_{19} consisting of rotational isometries in D_{19} is a normal subgroup of D_{19} of index 2. So, let

$$R \triangleleft G/H_{53}$$

denote the subgroup of the quotient group G/H_{53} corresponding to this subgroup consisting of rotational isometries. By the Fourth Isomorphism Theorem for groups, we have that there exists a corresponding subgroup R' whereby:

$$H_{53} \trianglelefteq R' \trianglelefteq G.$$

We thus obtain the subnormal series

$$H_{53}/H_{53} \trianglelefteq R'/H_{53} \trianglelefteq G/H_{53}.$$

Since R'/H_{53} is a group of order 19, we have that R' is a group of order 1007. Writing $R' = H_{1007}$, we thus arrive at the following subnormal series:

$$\{1\} \trianglelefteq H_{53} \trianglelefteq H_{1007} \trianglelefteq G.$$

Now consider the following quotient groups:

$$G/H_{1007} \cong \mathbb{Z}/2\mathbb{Z}$$
$$H_{1007}/H_{53} \cong \mathbb{Z}/19\mathbb{Z}$$

$$H_{53}/\{1\} \cong \mathbb{Z}/53\mathbb{Z}.$$

We thus have that the subnormal series

$$\{1\} \trianglelefteq H_{53} \trianglelefteq H_{1007} \trianglelefteq G$$

is a composition series with abelian composition factors, thus proving that G is solvable.

Exercise 1.86. What can you say about groups of order 2015? Are they simple? Abelian? Nilpotent? Solvable? Note that $2015 = 5 \cdot 13 \cdot 31$.

Solution 1.87. Let G be a group of order $2015 = 5 \cdot 13 \cdot 31$. Letting n_{31} denote the number of Sylow 31-subgroups of G, using Sylow theory, we have that:

(i) $n_{31} \geq 1$;

(ii) $n_{31} \in \{1, 5, 13, 31, 65, 155, 403, 2015\}$; and

(iii) $n_{31} \equiv 1 (\text{mod} 31)$.

Since $n_{31} \in \{1, 5, 13, 31, 65, 155, 403, 2015\}$ and $n_{31} \equiv 1 (\text{mod} 31)$, it is easily seen that $n_{31} = 1$. Since Sylow p-subgroups are all conjugates of each other, we have that the unique Sylow 31-subgroup H_{31} of G must be a normal subgroup of G:

$$H_{31} \triangleleft G.$$

We thus have that G is not a simple group.

It is known that if p and q are primes such that $q \equiv 1 (\text{mod} p)$, then there exists a unique, up to isomorphism, non-abelian group of order pq [9]. So, it is thus easily seen that a group of order 2015 may or may not be abelian.

If G is an abelian group of order 2015, then G must be nilpotent, since non-trivial abelian groups are nilpotent.

Now suppose that G is a non-abelian group of order 2015. As indicated above, there exists a non-abelian group of order 2015. Now, consider the center $Z(G)$ of this group. By Lagrange's theorem, we have that the order of $Z(G)$ divides $|G|$. We claim that $G/Z(G)$ cannot be cyclic. To show this, by way of contradiction, suppose that $G/Z(G)$ is cyclic, and let the coset $gZ(G)$ generate this quotient group. Let g_1 and g_2 be elements in G. If g_1 is in $Z(G)$ or g_2 is in $Z(G)$, then $g_1 \cdot g_2 = g_2 \cdot g_1$. Now suppose that $g_1 \notin Z(G)$ and $g_2 \notin Z(G)$. Since $gZ(G)$ generates the cyclic group $G/Z(G)$, we may write

$$g_1 = g^{n_1} z_1$$

and

$$g_2 = g^{n_2} z_2$$

for some $n_1, n_2 \in \mathbb{N}_0$ and some $z_1, z_2 \in Z(G)$. We thus have that

$$g_1 \cdot g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_1 + n_2} z_1 z_2$$

[9] See https://drexel28.wordpress.com/2011/04/19/groups-of-order-pq-pt-ii/.

and

$$g_2 \cdot g_1 = g^{n_2} z_2 g^{n_1} z_1 = g^{n_2+n_1} z_2 z_1 = g^{n_1+n_2} z_1 z_2.$$

But then $g_1 \cdot g_2 = g_2 \cdot g_1$ for all elements g_1 and g_2 in G, contradicting that G is non-abelian.

So, since $|Z(G)|$ divides $|G|$, and since $G/Z(G)$ cannot be cyclic, we may deduce that:

$$|Z(G)| \in \{1, 5, 13, 31, 2015\}.$$

Similarly, since G is non-abelian, we have that:

$$|Z(G)| \in \{1, 5, 13, 31\}.$$

By way of contradiction, suppose that $Z(G)$ is of order 31. Then the quotient group $G/Z(G)$ must be of order $65 = 5 \cdot 13$. So, each non-identity element in $G/Z(G)$ is either of order 5, of order 13, or of order 65. Letting n_5 denote the number of maximal 5-subgroups, and letting n_{13} denote the number of maximal 13-subgroups, using Sylow theory, it is easily seen that $n_5 = 1$ and $n_{13} = 1$. So, there is exactly 1 subgroup of $G/Z(G)$ of order 5 and exactly 1 subgroup of $G/Z(G)$ of order 13. So the number of elements in $G/Z(G)$ of order 5 is 4, and the number of elements in $G/Z(G)$ of order 13 is 12. But then the remaining non-identity elements must be of order 65, which shows that $G/Z(G)$ must be cyclic, contradicting that G is non-abelian. A similar argument shows that $|Z(G)| \neq 5$. Therefore,

$$|Z(G)| \in \{1, 13\}.$$

Suppose that the order of $Z(G)$ is equal to 13. Now, consider the quotient group $G/Z(G)$. This quotient group is of order $155 = 5 \cdot 31$. It is clear that $G/Z(G)$ cannot be abelian, because otherwise, $G/Z(G)$ would have to be isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_{31} \cong \mathbb{Z}_{155}$, which is impossible since G is non-abelian. We thus have that $G/Z(G)$ is a non-abelian group of order 155. Now consider the expression $Z(G/Z(G))$. By Lagrange's theorem, we have that

$$|Z(G/Z(G))| \in \{1, 5, 31, 155\}.$$

Since $G/Z(G)$ is non-abelian, we have that

$$|Z(G/Z(G))| \in \{1, 5, 31\}.$$

But we know that the quotient

$$(G/Z(G))/Z(G/Z(G))$$

cannot be cyclic since $G/Z(G)$ is non-abelian. So, since the quotient

$$(G/Z(G))/Z(G/Z(G))$$

cannot be cyclic, we have that $Z(G/Z(G))$ cannot be of order 5, and cannot be of order 31. We thus have that:

$$|Z(G/Z(G))| = 1.$$

But since

$$Z(G/Z(G)) = eZ(G) = Z(G),$$

we have that the Upper Central Series

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

would have to be of the form

$$\{1\} \trianglelefteq Z(G) \trianglelefteq Z(G) \trianglelefteq Z(G) \trianglelefteq \cdots,$$

and we thus have that G is not nilpotent in this case. Now suppose that the order of $Z(G)$ is equal to 1. In this case, we have that the Upper Central Series

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

would have to be of the form

$$\{1\} \trianglelefteq \{1\} \trianglelefteq \{1\} \trianglelefteq \{1\} \trianglelefteq \cdots,$$

and we again have that G is not nilpotent. So we have shown that: if G is an abelian group of order 2015, then G is nilpotent, and if G is a non-abelian group of order 2015, then G is not nilpotent.
If G is an abelian group of order 2015, then G must be solvable, since abelian groups are solable. Now suppose that G is a non-abelian group of order $2015 = 5 \cdot 13 \cdot 31$. Let n_5, n_{13}, and n_{31} respectively denote the number of Sylow 5-subgroups, the number of Sylow 13-subgroups, and the number of Sylow 31-subgroups. Using Sylow theory, it is easily seen that there is a unique subgroup H_{13} of order 13 which is a normal subgroup, and there is a unique subgroup H_{31} of order 31 which is a normal subgroup. We thus arrive at the following subnormal series:

$$\{1\} \triangleleft H_{31} \triangleleft G.$$

The quotient group G/H_{31} is of order $65 = 5 \cdot 13$. Since $5 \equiv 5 (\text{mod } 13)$ and $13 \equiv 3 (\text{mod } 5)$, we may deduce that a group of order 65 must be abelian. Furthermore, since 5 and 13 are relatively prime, we may deduce that G/H_{31} is a cyclic group of order $65 = 5 \cdot 13$. Similarly, since $H_{31}/\{1\}$ is a group of order 31, and since 31 is a prime number, we have that the quotient group $H_{31}/\{1\}$ must be cyclic. We thus have that G is solvable, regardless of whether or not G is abelian.

Exercise 1.88. What can you say about groups of order 2016? Are they simple? Abelian? Nilpotent? Solvable? Note that $2016 = 2^5 \cdot 3^2 \cdot 7$.

Solution 1.89. It is known that there are no simple groups of order 2016. Proving this requires a complicated argument involving Sylow theory, as well as some more advanced topics beyond the scope of MATH 6121. Proofs that there are no simple groups of order 2016 are given in the following links:

`http://www.slideshare.net/JnosKurdics/hard-time-to-come`

`http://math.stackexchange.com/questions/1577502/no-simple-group-of-order-2016`

It is clear that a group of order 2016 may or may not be abelian. For example, the cyclic group $\mathbb{Z}/2016\mathbb{Z}$ is abelian, but the dihedral group $D_{\frac{2016}{2}}$ of order 2016 is not abelian.

Of course, there exists a group of order 2016 which is nilpotent. For example, since the cyclic group $\mathbb{Z}/2016\mathbb{Z}$ is nontrivial and abelian, it must be nilpotent. However, it is known that every finite nilpotent group is the direct product of p-groups[10]. But if $G = D_{\frac{2016}{2}}$, then G is not a direct product of p-groups, since dihedral groups are not direct products of p-groups. So, a group of order 2016 may or may not be nilpotent. There is a more concrete way of showing that $G = D_{1008}$ is not nilpotent. It is easily seen that the center of a dihedral group D_n is trivial if n is odd, and consists precisely of the identity element and the isometry given by a hald-turn rotation otherwise. So, the center $Z(G)$ of $G = D_{1008}$ consists precisely of the identity element e and the isometry r given by a half-turn rotation. By considering the

[10] See `https://en.wikipedia.org/wiki/Nilpotent_group`.

homomorphic image of a dihedral group, using the First Isomorphism Theorem for groups, it is easily seen that quotient groups of dihedral groups are dihedral[11] We thus have that

$$D_{1008}/Z(D_{1008}) \cong D_{504}$$

and

$$Z(D_{1008}/Z(D_{1008})) \cong Z(D_{504})$$

so that

$$Z(D_{1008}/Z(D_{1008})) \cong \mathbb{Z}_2.$$

So, the union

$$\bigcup Z(D_{1008}/Z(D_{1008}))$$

consists of the elements in $Z(D_{1008}) = \{e, r\}$, along with elements in some left coset of $Z(D_{1008}) = \{e, r\}$. We may thus write

$$\bigcup Z(D_{1008}/Z(D_{1008})) = \{e, r, a, ar\},$$

for some element a. But since the Upper Central Series for G is of the form

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

we have that $\{e, r, a, ar\}$ forms a group, and therefore must be abelian, since it is of order 4. So we have thus far shown that the Upper Central Series

$$Z_0 \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

for G must be of the form

$$\{e\} \trianglelefteq \{e, r\} \trianglelefteq \{e, r, a, ar\} \trianglelefteq \cdots$$

Continuing in this manner, it is easily seen that a dihedral group D_n nilpotent if and only if n is a power of 2.

An abelian group of order 2016 is, of course, solvable. However, it is actually known that there exists a non-solvable group of order 2016[12]. Constructing such a group is beyond the scope of our paper. However, it is know that a group of order 2016 may or may not be solvable.

Exercise 1.90. Let $C_3 = \{e, a, a^2\}$ act on $V = \mathscr{L}_{\mathbb{C}}\{e_1, e_2, e_3\}$ so that $a(e_1) = e_2$, $a(e_2) = e_3$, $a(e_3) = e_1$, $a^2(e_1) = e_3$, etc. By Maschke's theorem, V is decomposible, with $V \cong \mathscr{L}\{e_1 + e_2 + e_3\} \oplus \mathscr{L}\{b_2, b_3\}$. Find a basis $\{b_2, b_3\}$ for $\mathscr{L}\{b_2, b_3\}$, and check that it is a basis.

Solution 1.91. Following the proof of Maschke's theorem, we start by fixing the basis $\mathcal{B} = \{e_1, e_2, e_3\}$ of $V = \mathscr{L}_{\mathbb{C}}\{e_1, e_2, e_3\}$, and we proceed to construct a scalar product $\langle \cdot, \cdot \rangle$ so that

$$\langle \vec{v}, \vec{u} \rangle = \overline{[\vec{v}]_{\mathcal{B}}^T}[\vec{u}]_{\mathcal{B}}$$

for $\vec{v}, \vec{u} \in V$. It is clear that this scalar product is such that:
Define the scalar product $\langle \cdot, \cdot \rangle$ as follows:

$$\langle \vec{e}_i, \vec{e}_j \rangle = \begin{cases} 1 & \text{if } i = j; \\ 0 & \text{otherwise.} \end{cases}$$

[11] See http://planetmath.org/sites/default/files/texpdf/38175.pdf.
[12] See https://oeis.org/A056866.

Following the proof of Maschke's theorem, we define the scalar product $[\cdot,\cdot]$ by "averaging over" the entire group C_3 as follows:

$$[x,y] = \frac{1}{3}\langle x,y\rangle + \frac{1}{3}\langle a(x),a(y)\rangle + \frac{1}{3}\langle a^2(x),a^2(y)\rangle.$$

Applying the Gram-Schmidt algorithm, define b_2 as follows:

$$b_2 = e_2 - \frac{[e_2, e_1+e_2+e_3]}{[e_1+e_2+e_3, e_1+e_2+e_3]}(e_1+e_2+e_3).$$

Since $e_1+e_2+e_3 = a(e_1+e_2+e_3) = a^2(e_1+e_2+e_3)$, it is clear that:

$$b_2 = e_2 - \frac{1}{3}(e_1+e_2+e_3) = -\frac{1}{3}e_1 + \frac{2}{3}e_2 - \frac{1}{3}e_3.$$

Similarly, we define:

$$b_3 = e_3 - \frac{1}{3}(e_1+e_2+e_3) = -\frac{1}{3}e_1 - \frac{1}{3}e_2 + \frac{2}{3}e_3.$$

Again since $e_1+e_2+e_3 = a(e_1+e_2+e_3) = a^2(e_1+e_2+e_3)$, it is clear that:

$$\langle e_1+e_2+e_3, b_2\rangle = 0,$$
$$\langle e_1+e_2+e_3, b_3\rangle = 0.$$

We claim that $\{b_2, b_3\}$ is linearly independent. Letting c_1 and c_2 be scalars, we have that:

$$\begin{aligned} c_1b_1 = c_2b_2 &\Longrightarrow c_1\left(-\frac{1}{3}e_1 + \frac{2}{3}e_2 - \frac{1}{3}e_3\right) = c_2\left(-\frac{1}{3}e_1 - \frac{1}{3}e_2 + \frac{2}{3}e_3\right) \\ &\Longrightarrow c_1\left(-\frac{1}{3}e_1\right) = c_2\left(-\frac{1}{3}e_1\right) \\ &\Longrightarrow c_1 = c_2. \end{aligned}$$

Since $V = \mathscr{L}_{\mathbb{C}}\{e_1,e_2,e_3\}$ is of dimension 3, and since $\mathscr{L}\{e_1+e_2+e_3\}$ is of dimension 1, we may deduce that $\{b_2, b_3\}$ is a spanning set.

Exercise 1.92. Prove that if $\theta\colon M \to N$ is a G-morphism, then $\ker(\theta) \leq M$ is a G-module and $\operatorname{im}(\theta) \leq N$ is a G-module.

Solution 1.93. Suppose that $\theta\colon M \to N$ is a G-morphism. By definition of a G-homomorphism, θ is a group homomorphism with respect to the abelian group structures of M and N, and θ is also G-equivariant. Since θ is a group homomorphism, the kernel of θ is a subgroup of M and the image of θ is a subgroup of N.

Now, let $m \in M$ be such that $\theta(m) = 0$, so that m is in the kernel of θ. Also, let g be an element in G. We thus have that

$$g\theta(m) = g \cdot 0 = 0,$$

and since θ is a G-homomorphism, we have that

$$\theta(g \cdot m) = 0.$$

So, if m is in the kernel of θ, then $g \cdot m$ is in this kernel, thus proving that $\ker(\theta) \leq M$ as a G-module.

Again let $m \in M$ be arbitrary. We thus have that $\theta(m)$ is an arbitrary element in the image of θ. Since $g \cdot m$ is also in M, we have $\theta(g \cdot m)$ is also in the image of θ. But since θ is a G-homomorphism, we thus find that

$$\theta(g \cdot m) = g \cdot \theta(m)$$

is in the image of θ.

Exercise 1.94. Prove that $Z(\mathrm{Mat}_{n \times n}(\mathbb{C})) = \mathbb{C}\mathrm{Id}_{n \times n}$.

Solution 1.95. Suppose that $A = [a_{ij}]$ is in $Z(\mathrm{Mat}_{n \times n}(\mathbb{C}))$. Let $E_{ij} \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ be such that the (i,j)-entry is 1, and each other entry is 0. Then since

$$E_{ii} A = A E_{ii}$$

for all indices i, A must be diagonal. Since

$$E_{ij} A = A E_{ij}$$

for all indices i and j, it is easily seen that the diagonal entries of A must all be equal. This effectively completes the proof.

Exercise 1.96. Let $G = D_3 = \{e, a, a^2, b, ba, ba^2\}$. Let vectors be indexed by group elements in G, writing $\vec{v}_g$ for $g \in D_3$, and let $h \cdot \vec{v}_g = \vec{v}_{hgh^{-1}}$. Now consider the module

$$\mathscr{L}\{\vec{v}_e, \vec{v}_a, \vec{v}_{a^2}, \vec{v}_b, \vec{v}_{ba}, \vec{v}_{ba^2}\} = W_1 \oplus W_2 \oplus W_3,$$

where $W_1 = \mathscr{L}\{\vec{v}_e\}$, $W_2 = \mathscr{L}\{\vec{v}_a, \vec{v}_{a^2}\}$, and $W_3 = \mathscr{L}\{\vec{v}_b, \vec{v}_{ba}, \vec{v}_{ba^2}\}$. Write

$$W_3 = \mathscr{L}\{\vec{v}_b + \vec{v}_{ba} + \vec{v}_{ba^2}\} \oplus V.$$

Find a basis for V.

Solution 1.97. Since W_3 is of dimension 3, we may deduce that V must be of dimension 2. Consider the following direct sum:

$$\mathscr{L}\{\vec{v}_b + \vec{v}_{ba} + \vec{v}_{ba^2}\} \oplus \mathscr{L}\{\vec{v}_{ba}, \vec{v}_{ba^2}\}.$$

The underlying set of the above direct sum consists of all ordered pairs of the form

$$(c_1\vec{v}_b + c_1\vec{v}_{ba} + c_1\vec{v}_{ba^2}, c_2\vec{v}_{ba} + c_3\vec{v}_{ba^2})$$

where $c_1, c_2, c_3 \in \mathbb{C}$. Now consider the mapping

$$\phi \colon \mathscr{L}\{\vec{v}_b + \vec{v}_{ba} + \vec{v}_{ba^2}\} \oplus \mathscr{L}\{\vec{v}_{ba}, \vec{v}_{ba^2}\} \to \mathscr{L}\{\vec{v}_b, \vec{v}_{ba}, \vec{v}_{ba^2}\}$$

whereby:

$$\phi(c_1\vec{v}_b + c_1\vec{v}_{ba} + c_1\vec{v}_{ba^2}, c_2\vec{v}_{ba} + c_3\vec{v}_{ba^2}) = c_1\vec{v}_b + (c_1 + c_2)\vec{v}_{ba} + (c_1 + c_3)\vec{v}_{ba^2}.$$

This mapping preserves addition, since

$$\phi(c_1\vec{v}_b + c_1\vec{v}_{ba} + c_1\vec{v}_{ba^2}, c_2\vec{v}_{ba} + c_3\vec{v}_{ba^2}) + \phi(d_1\vec{v}_b + d_1\vec{v}_{ba} + d_1\vec{v}_{ba^2}, d_2\vec{v}_{ba} + d_3\vec{v}_{ba^2})$$

is equal to

$$(c_1 + d_1)\vec{v}_b + (c_1 + c_2 + d_1 + d_2)\vec{v}_{ba} + (c_1 + c_3 + d_1 + d_3)\vec{v}_{ba^2},$$

which is also equal to ϕ evaluated at

$$(c_1\vec{v}_b + c_1\vec{v}_{ba} + c_1\vec{v}_{ba^2}, c_2\vec{v}_{ba} + c_3\vec{v}_{ba^2}) + (d_1\vec{v}_b + d_1\vec{v}_{ba} + d_1\vec{v}_{ba^2}, d_2\vec{v}_{ba} + d_3\vec{v}_{ba^2}).$$

It is easily seen that ϕ preserves scalar multiplication. Also, it is clear that ϕ is surjective. If

$$\phi(c_1\vec{v}_b + c_1\vec{v}_{ba} + c_1\vec{v}_{ba^2}, c_2\vec{v}_{ba} + c_3\vec{v}_{ba^2}) = \phi(d_1\vec{v}_b + d_1\vec{v}_{ba} + d_1\vec{v}_{ba^2}, d_2\vec{v}_{ba} + d_3\vec{v}_{ba^2})$$

then

$$c_1\vec{v}_b + (c_1 + c_2)\vec{v}_{ba} + (c_1 + c_3)\vec{v}_{ba^2} = d_1\vec{v}_b + (d_1 + d_2)\vec{v}_{ba} + (d_1 + d_3)\vec{v}_{ba^2},$$

which implied that $c_1 = d_1$, which in turn implies that $c_2 = d_2$ and $c_3 = d_3$. We thus have that ϕ is injective, thus proving that

$$\mathscr{L}\{\vec{v}_b + \vec{v}_{ba} + \vec{v}_{ba^2}\} \oplus \mathscr{L}\{\vec{v}_{ba}, \vec{v}_{ba^2}\} \cong \mathscr{L}\{\vec{v}_b, \vec{v}_{ba}, \vec{v}_{ba^2}\},$$

thus proving that $\{\vec{v}_{ba}, \vec{v}_{ba^2}\}$ is a basis for V.

Exercise 1.98. Prove that $\widehat{P * Q}(\rho) = \hat{P}(\rho) \cdot \hat{Q}(\rho)$.

Solution 1.99. We adopt notation for convolution and the Fourier transform from Diaconis' *Group representations in probability and statistics* [13]. Assume that P and Q are probabilities on a finite group G, so that $P(s) \geq 0$ and $\sum_s P(s) = 1$, and similarly for Q. The convolution is defined as follows:

$$P * Q(s) = \sum_t P(st^{-1})Q(t).$$

The Fourier transform of P at the representation ρ is the matrix

$$\hat{P}(\rho) = \sum_s P(s)\rho(s).$$

By definition, we have

$$\widehat{P * Q}(\rho) = \sum_s \sum_t P(st^{-1})Q(t)\rho(s).$$

Make the change of variables $g = st^{-1}$:

$$\widehat{P * Q}(\rho) = \sum_g \sum_t P(g)Q(t)\rho(gt).$$

Since ρ is a group homomorphism, we have that:

$$\widehat{P * Q}(\rho) = \sum_g \sum_t P(g)Q(t)\rho(g)\rho(t).$$

Therefore,

$$\widehat{P * Q}(\rho) = \sum_g \sum_t P(g)\rho(g)Q(t)\rho(t).$$

Exercise 1.100. Define E so that $E(e) = 1$ and $E(g) = 0$ for $g \neq e$. Also, define the uniform distribution U so that $U(g) = \frac{1}{|G|}$ for all g in G. Prove that $E * P = P$ and $U * P = U$.

[13] See `https://jdc.math.uwo.ca/M9140a-2012-summer/Diaconis.pdf`.

Solution 1.101. By definition of the convolution, we have that:

$$E * P(s) = \sum_t E(st^{-1})P(t).$$

The expression

$$E(st^{-1})P(t)$$

is equal to $P(t)$ if and only if $s = t$, and is equal to 0 otherwise. Therefore,

$$E * P(s) = \sum_t E(st^{-1})P(t) = P(s)$$

for all s. Again by definition of the convolution, we have that

$$U * P(s) = \sum_t U(st^{-1})P(t).$$

That is,

$$U * P(s) = \sum_t \frac{1}{|G|}P(t).$$

Therefore,

$$U * P(s) = \frac{1}{|G|}\sum_t P(t).$$

But since P is a probability on G, we have that

$$U * P(s) = \frac{1}{|G|}$$

for all s.

Exercise 1.102. Let G be a finite group, and let $Z(G)$ be the center of G. Show that the order of $G/Z(G)$ is not a prime.

Solution 1.103. By way of contradiction, suppose that the order $|G/Z(G)|$ of the quotient group $G/Z(G)$ is a prime $p \in \mathbb{N}$. But by Lagrange's theorem, the only group of order p up to isomorphism is the cyclic group $\mathbb{Z}/p\mathbb{Z}$. We thus have that $G/Z(G)$ is a cyclic group of order p. Let $g \in G$ be such that the left coset $gZ(G)$ generates the cyclic group $G/Z(G)$. Now, let g_1 and g_2 be elements in G. If $g_1 \in Z(G)$ or $g_2 \in Z(G)$, then $g_1 \cdot g_2 = g_2 \cdot g_1$, by definition of the center of a group. Now suppose that it is not the case that $g_1 \in Z(G)$, and that it is not the case that $g_2 \in Z(G)$. Consider the cosets $g_1Z(G)$ and $g_2Z(G)$. Since $gZ(G)$ generates the cyclic group $G/Z(G)$, we have that

$$g_1Z(G) = g^{n_1}Z(G)$$

and

$$g_2Z(G) = g^{n_2}Z(G)$$

for some $n_1, n_2 \in \mathbb{N}_0$. So, for some $z_1, z_2 \in Z(G)$, we have that:

$$\begin{aligned} g_1 &= g^{n_1}z_1 \\ g_2 &= g^{n_2}z_2. \end{aligned}$$

Now consider the product $g_1 \cdot g_2$:

$$\begin{aligned} g_1 \cdot g_2 &= g^{n_1} z_1 g^{n_2} z_2 \\ &= g^{n_1} g^{n_2} z_1 z_2 \\ &= g^{n_1+n_2} z_1 z_2. \end{aligned}$$

Now consider the product $g_2 \cdot g_1$:

$$\begin{aligned} g_2 \cdot g_1 &= g^{n_2} z_2 g^{n_1} z_1 \\ &= g^{n_2} g^{n_1} z_2 z_1 \\ &= g^{n_2} g^{n_1} z_1 z_2 \\ &= g^{n_2+n_1} z_1 z_2 \\ &= g^{n_1+n_2} z_1 z_2. \end{aligned}$$

But then we again have that $g_1 \cdot g_2 = g_2 \cdot g_1$, which shows that G is abelian. But then $G = Z(G)$. But then $|G/Z(G)| = 1$, contradicting that $|G/Z(G)|$ is of prime order.

Exercise 1.104. Suppose that $|G| = 175$. Show that G is solvable and give its composition factors.

Solution 1.105. Letting G be of order 175, observe that $|G| = 5^2 \cdot 7$. Let n_7 denote the number of Sylow 7-subgroups of G. The divisors of $|G|$ ordered canonically are given below:

$$(1, 5, 7, 25, 35, 175).$$

The above sequence modulo 7 is given below:

$$(1, 5, 0, 4, 0, 0).$$

Using Sylow theory, we may thus deduce that there exists a unique Sylow 7-subgroup H_7 of G. Again from Sylow theory, since $n_7 = 1$, we have that H_7 must be a normal subgroup of G:

$$\{e\} \lhd H_7 \lhd G.$$

Now consider the quotient group G/H_7. This quotient group is of order 5^2. From the previous exercise, we know that the order of the quotient of a group by its center cannot be prime. So, by Lagrange's theorem, the center of G/H_7 is either trivial or is equal to G/H_7. But it is known that the center of a group of prime power order is necessarily non-trivial: this is easily seen using the class equation with respect to a group acting on itself by conjugation. Therefore, G/H_7 must be abelian, since the center of G/H_7 must be of order 5^2. Since the factor groups of the subnormal series

$$\{e\} \lhd H_7 \lhd G.$$

are all abelian, we thus have that G is solvable.

Exercise 1.106. Let G be a finite group and let $\gamma \colon G \to \operatorname{Aut}(G)$ be defined by $\gamma(g)(h) = ghg^{-1}$. We can now define the semidirect product $G \rtimes_\gamma G$ as the group consisting of the set of pairs $\{(g_1, g_2) : g_1, g_2 \in G\}$ with the product $(g_1, g_2) \cdot_{G \rtimes_\gamma G} (g_3, g_4) = (g_1 \gamma(g_2)(g_3), g_2 g_4)$. Show that $H = \{(g, 1) : g \in G\} \lhd G \rtimes_\gamma G$.

Solution 1.107. We begin by showing that $H \leq G \rtimes_\gamma G$. Let g_1 and g_2 be arbitrary elements in G, so that $(g_1, 1)$ and $(g_2, 1)$ are arbitrary elements in H. We thus have that:

$$\begin{aligned}(g_1, 1) \cdot_{G \rtimes_\gamma G} (g_2, 1) &= (g_1 \gamma(1)(g_2), 1)\\ &= (g_1 g_2, 1) \in H.\end{aligned}$$

We thus have that H is closed under the underlying operation of $G \rtimes_\gamma G$. Similarly, we have that:

$$\begin{aligned}(g_1, 1) \cdot_{G \rtimes_\gamma G} (g_1^{-1}, 1) &= (g_1 \gamma(1)(g_1^{-1}), 1)\\ &= (g_1 g_1^{-1}, 1)\\ &= (1, 1).\end{aligned}$$

A symmetric argument shows that

$$(g_1^{-1}, 1) \cdot_{G \rtimes_\gamma G} (g_1, 1) = (1, 1),$$

thus proving that H is closed under inverses, with $H \leq G \rtimes_\gamma G$.

Again let $g_1, g_2 \in G$. We thus have that (g_1, g_2) is an arbitrary element in the semidirect product $G \rtimes_\gamma G$. Now let $g_3 \in G$, so that the ordered pair $(g_3, 1)$ is an arbitrary element in H. We thus have that the element given by the product

$$(g_1, g_2) \cdot_{G \rtimes_\gamma G} (g_3, 1)$$

is an arbitrary element in the left coset $(g_1, g_2)H$. So, the ordered pair

$$(g_1 g_2 g_3 g_2^{-1}, g_2)$$

is an arbitrary element in the coset $(g_1, g_2)H$. Letting $g_4 \in G$, observe that elements in the right coset $H(g_1, g_2)$ are of the following form:

$$(g_4, 1) \cdot_{G \rtimes_\gamma G} (g_1, g_2) = (g_4 g_1, g_2).$$

So, letting

$$(g_1 g_2 g_3 g_2^{-1}, g_2) = (g_4 g_1, g_2)$$

we have that

$$g_1 g_2 g_3 g_2^{-1} = g_4 g_1$$

and we thus have that:

$$\begin{aligned}g_4 &= g_1 g_2 g_3 g_2^{-1} g_1^{-1}\\ &= (g_1 g_2) g_3 (g_1 g_2)^{-1}.\end{aligned}$$

This proves the inclusion whereby:

$$(g_1, g_2)H \subseteq H(g_1, g_2).$$

Conversely, letting

$$(g_4 g_1, g_2)$$

be an arbitrary element in the right coset $H(g_1, g_2)$, we know that elements in the left coset $(g_1, g_2)H$ are of the form

$$(g_1 g_2 g_3 g_2^{-1}, g_2).$$

Writing

$$(g_4 g_1, g_2) = (g_1 g_2 g_3 g_2^{-1}, g_2),$$

we have that

$$g_4 g_1 = g_1 g_2 g_3 g_2^{-1}.$$

Solving for g_3 shows that the reverse inclusion $(g_1, g_2)H \supseteq H(g_1, g_2)$ holds.

Exercise 1.108. Letting γ be as given above, show that $K = \{(g, g^{-1}) : g \in G\} \lhd G \rtimes_{\gamma} G$.

Solution 1.109. We begin by showing that $K \leq G \rtimes_{\gamma} G$. Let g_1 and g_2 be arbitrary elements in G, so that (g_1, g_1^{-1}) and (g_2, g_2^{-1}) are arbitrary elements in K. Now evaluate the product $(g_1, g_1^{-1}) \cdot_{G \rtimes_{\gamma} G} (g_2, g_2^{-1})$ in the following manner:

$$\begin{aligned}
(g_1, g_1^{-1}) \cdot_{G \rtimes_{\gamma} G} (g_2, g_2^{-1}) &= (g_1 \gamma(g_1^{-1})(g_2), g_1^{-1} g_2^{-1}) \\
&= (g_1 g_1^{-1} g_2 g_1, g_1^{-1} g_2^{-1}) \\
&= (g_2 g_1, g_1^{-1} g_2^{-1}) \\
&= (g_2 g_1, (g_2 g_1)^{-1}) \in K.
\end{aligned}$$

We thus have that K is closed under the underlying binary operation of G. Similarly,

$$\begin{aligned}
(g_1, g_1^{-1}) \cdot_{G \rtimes_{\gamma} G} (g_1^{-1}, g_1) &= (g_1 \gamma(g_1^{-1})(g_1^{-1}), 1) \\
&= (g_1 g_1^{-1} g_1^{-1} g_1, 1) \\
&= (1, 1).
\end{aligned}$$

A symmetric argument shows that

$$(g_1^{-1}, g_1) \cdot_{G \rtimes_{\gamma} G} (g_1, g_1^{-1}) = (1, 1).$$

We thus have that $K \leq G \rtimes_{\gamma} G$.

Again letting g_1 and g_2 be arbitrary elements in G, we thus have that the ordered pair (g_1, g_2) is an arbitrary element in $G \rtimes_{\gamma} G$. Letting $g_3 \in G$, we have that (g_3, g_3^{-1}) is an arbitrary element in K. So the product

$$(g_1, g_2) \cdot_{G \rtimes_{\gamma} G} (g_3, g_3^{-1})$$

is an arbitrary element in the left coset $(g_1, g_2)K$. Evaluate this product as follows:

$$(g_1, g_2) \cdot_{G \rtimes_{\gamma} G} (g_3, g_3^{-1}) = (g_1 g_2 g_3 (g_2^{-1}), g_2 g_3^{-1}).$$

Now let $g_4 \in G$, so that (g_4, g_4^{-1}) is in K. We thus have that elements in the right coset $K(g_1, g_2)$ are of the following form:

$$\begin{aligned}
(g_4, g_4^{-1}) \cdot_{G \rtimes_{\gamma} G} (g_1, g_2) &= (g_4 g_4^{-1} g_1 g_4, g_4^{-1} g_2) \\
&= (g_1 g_4, g_4^{-1} g_2).
\end{aligned}$$

Now, given that

$$(g_1 g_2 g_3 (g_2^{-1}), g_2 g_3^{-1})$$

is an arbitrary element in the left coset $(g_1, g_2)K$, let

$$g_4 = g_2 g_3 g_2^{-1},$$

and rewrite the expression

$$(g_4, g_4^{-1}) \cdot_{G \rtimes_\gamma G} (g_1, g_2)$$

as follows:

$$\begin{aligned}(g_4, g_4^{-1}) \cdot_{G \rtimes_\gamma G} (g_1, g_2) &= (g_1 g_4, g_4^{-1} g_2)\\ &= (g_1 g_2 g_3 g_2^{-1}, g_2 g_3^{-1} g_2^{-1} g_2)\\ &= (g_1 g_2 g_3 g_2^{-1}, g_2 g_3^{-1}).\end{aligned}$$

This shows that each element in $(g_1, g_2)K$ is in the corresponding right coset. A symmetric argument may be used to prove the reverse inclusion.

Exercise 1.110. Again letting γ be as given above, show that $G \rtimes_\gamma G \cong G \times G$.

Solution 1.111. Consider the mapping

$$\phi : G \rtimes_\gamma G \to G \times G$$

so that

$$\phi(a, b) = (ab, b).$$

We claim that ϕ is a group homomorphism.

$$\begin{aligned}\phi(a, b)\phi(c, d) &= (ab, b)(cd, d)\\ &= (abcd, bd).\end{aligned}$$

Now evaluate the product $\phi((a, b) \cdot_{G \rtimes_\gamma G} (c, d))$:

$$\begin{aligned}\phi((a, b) \cdot_{G \rtimes_\gamma G} (c, d)) &= \phi(abcb^{-1}, bd)\\ &= (abcd, bd).\end{aligned}$$

We thus have that ϕ is a group homomorphism. The mapping ϕ is surjective, since given an element (c, d) in the codomain of ϕ, writing

$$(ab, b) = (c, d)$$

we have that $b = d$ and $ab = c$, so that $ad = c$ and $a = c \cdot d^{-1}$. Similarly, if

$$\phi(a, b) = \phi(c, d)$$

then

$$(ab, b) = (cd, d)$$

and thus $b = d$, which in turn implies that $a = c$.

Exercise 1.112. Let $G = \{e, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$, with $\gamma^n = e$ be the cyclic group of order n. Fix an integer d, let $M_d = \mathbb{C}$ be a vector space of dimension 1. Let G act on $z \in M_d$ with the action $\gamma.z = \zeta^d z$ where $\zeta = e^{2\pi i/n}$ is a primitive n^{th} root of unity. [Here you have that $\gamma^2.z = \gamma.(\gamma.z) = \zeta^{2d} z$ and similarly $\gamma^k.z = \zeta^{kd} z$.] For what integers d is M_d a G-module?

Solution 1.113. The module M_d is a G-module for all integers d. Since

$$\gamma^k.z = \zeta^{kd}z$$

we have that

$$\gamma^n.z = \zeta^{nd}z \Longrightarrow e.z = z$$

but by definition of a group action, we have that $e.z = z$. We thus have that

$$\gamma^n.z = \zeta^{nd}z \Longrightarrow z = z.$$

So we have that M_d is a well-defined G-module for all integers d, in the sense that the given group action is well-defined for all d.

Exercise 1.114. Letting M_d be as given above, for which integers d is M_d irreducible?

Solution 1.115. Since $M_d = \mathbb{C}$ is 1-dimensional for all d, it is clear that M_d is irreducible for all integers d.

Exercise 1.116. Letting M_d be as given above, when is $M_d \cong M_{d'}$?

Solution 1.117. We claim that $M_d \cong M_{d'}$ if and only if $d \equiv d' (\text{mod } n)$. Suppose that M_d and $M_{d'}$ are isomorphic as vector spaces and as G-modules. Then there exists a bijective linear map f from M_d to $M_{d'}$ which is G-equivariant:

$$\zeta^{kd'}f(c) = f(\zeta^{kd}c).$$

Letting $k = 1$, we have that

$$\zeta^{d'}f(c) = f(\zeta^{d}c).$$

But this is only possible when d is equivalent to d' modulo n, because

$$\zeta^{d'}f(c) = \zeta^{d}f(c),$$

and for nonzero $f(c)$, we have that

$$\zeta^{d'} = \zeta^{d}$$

which implies that d' is equivalent to d modulo n. Conversely, if d is equivalent to d' modulo n, then $\zeta^{kd} = \zeta^{kd'}$, which implies that M_d and $M_{d'}$ have the same structure.

It was suggested in class that character theory may be used to construct an alternative solution to the above exercise. Since M_d and $M_{d'}$ are both equal to $\mathbb{C}$ as vector spaces, of course we have that $M_d \cong M_{d'}$ as vector spaces. Let

$$\rho_d : G \to \text{Aut}(\mathbb{C})$$

be such that $\rho_1(\gamma^k)(z) = \zeta^{kd}(z)$ and letting

$$\rho_{d'} : G \to \text{Aut}(\mathbb{C})$$

be such that $\rho_2(\gamma^k)(z) = \zeta^{kd'}(z)$. Let χ^{M_d} denote the character corresponding to ρ_1, and let $\chi^{M_{d'}}$ denote the character corresponding to ρ_2. Now consider the scalar product $\langle \chi^{M_d}, \chi^{M_{d'}} \rangle$.

$$\langle \chi^{M_d}, \chi^{M_{d'}} \rangle = \frac{1}{n}\sum_{k=0}^{n-1}\frac{\zeta^{kd}}{\zeta^{kd'}}.$$

We thus have that:

$$\langle \chi^{M_d}, \chi^{M_{d'}} \rangle = \frac{1}{n} \sum_{k=0}^{n-1} \zeta^{k(d-d')}.$$

So the scalar product $\langle \chi^{M_d}, \chi^{M_{d'}} \rangle$ is equal to 1 if and only if $\zeta^{k(d-d')}$ is equal to 1 for all indices k; equivalently, if d is equivalent to d' modulo n.

Exercise 1.118. Let X be a G-set for a finite group G. We denote by

$$X/G = \{\{g.x : g \in G\} : x \in X\}.$$

That is, X/G is the set of equivalence classes of X via the action of G. In other words, X/G is the set of orbits of the action of G on X. For $g \in G$, let

$$\mathrm{Fix}_X(g) = \{x \in X : g.x = x\}.$$

Show that

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|.$$

Hint: count the cardinality of $\{(g,x) : g \in G, x \in X, g.x = x\}$ in two different ways.

Solution 1.119. The result given in the above exercise is known as Burnside's Lemma, which we proved in class using the following strategy. Let n denote the number of orbits of the G-set X. We may write X as a disjoint union of orbits as indicated below:

$$X = X_1 \uplus X_2 \uplus \cdots \uplus X_n.$$

Now, let $x_i \in X_i$:

$$\begin{aligned} |G| &= \frac{|G|}{|\mathrm{Orb}(x_i)|} |\mathrm{Orb}(x_i)| \\ &= \frac{|G|}{|\mathrm{Orb}(x_i)|} \sum_{x \in \mathrm{Orb}(x_i)} 1 \\ &= \sum_{x \in \mathrm{Orb}(x_i)} \frac{|G|}{|\mathrm{Orb}(x_i)|} \\ &= \sum_{x \in \mathrm{Orb}(x_i)} \frac{|G|}{|\mathrm{Orb}(x)|} \\ &= \sum_{x \in \mathrm{Orb}(x_i)} |\mathrm{Stab}(x)|. \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{x \in X} |\mathrm{Stab}(x)| &= \sum_{i=1}^{n} \sum_{x \in \mathrm{Orb}(x_i)} |\mathrm{Stab}(x)| \\ &= \sum_{i=1}^{n} |G| \\ &= n \cdot |G|. \end{aligned}$$

We thus have that:

$$\frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}(x)|.$$

Counting the cardinality of

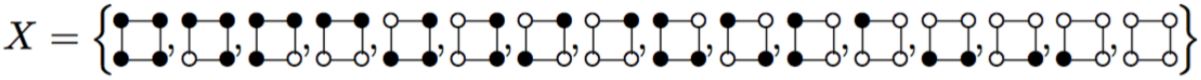
$$\{(g,x) : g \in G, x \in X, g.x = x\}$$

in two different ways, i.e., with respect to the first entry of a tuple in this set and alternatively with respect to the latter entry of a pair in this set, we have that:

$$\sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{x\in X}|\mathrm{Stab}(x)|.$$

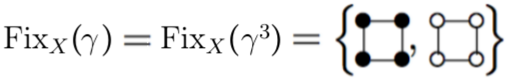
This proves that $n = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$.

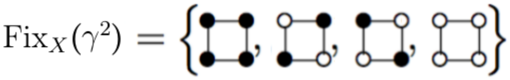
Exercise 1.120. Let $G = \mathbb{Z}_4 = \{e,\gamma,\gamma^2,\gamma^3\}$ with $\gamma^4 = e$ be the cyclic group of order 4. Let G act by rotation on the set of 4-necklaces with black and white beads (where $\gamma.N$ is a rotation of the necklace by 90° clockwise):



Describe the set $\mathrm{Fix}_X(g)$ for each element $g \in \mathbb{Z}_4$.

Solution 1.121. First of all, the identity element $e \in G$ fixes everything, so we have that $\mathrm{Fix}_X(e) = X$. Similarly, we have that:





Exercise 1.122. Use the previous two exercises to count the number of different 4-necklaces up to the action of $G = \mathbb{Z}_4$.

Solution 1.123. By Burnside's Lemma, we have that the number of different 4-necklaces up to the action of G is:

$$\frac{16+2+2+4}{4} = 6.$$

Exercise 1.124. Let $C_n = \{e,a,a^2,\dots,a^{n-1}\}$ with $a^n = e$. Show that for each $0 \le d \le n-1$, if $\psi_d(a^r) = e^{2dr\pi i/n}$ for all $0 \le r \le n-1$, then ψ_d is an irreducible character of C_n.

Solution 1.125. We recall that an irreducible character of a group G is a character of an irreducible representation of G.

Now, letting $d \in \mathbb{N}_0$ be an index whereby $0 \le d \le n-1$ define the mapping

$$\phi_d\colon C_n \to \mathrm{GL}_1(\mathbb{C})$$

so that

$$\phi_d(a^r) = [e^{2dr\pi i/n}]_{1\times 1}$$

for all $r \in \mathbb{N}_0$ such that $0 \leq r \leq n-1$. We claim that ϕ_d is a group homomorphism. To show this, letting $r_1, r_2 \in \mathbb{N}_0$ be such that $0 \leq r_1, r_2 \leq n-1$, we have that:

$$\begin{aligned}\phi_d(a^{r_1})\phi_d(a^{r_2}) &= [e^{2dr_1\pi i/n}]_{1\times 1}[e^{2dr_2\pi i/n}]_{1\times 1}\\ &= [e^{2dr_1\pi i/n}e^{2dr_2\pi i/n}]_{1\times 1}\\ &= [e^{2dr_1\pi i/n+2dr_2\pi i/n}]_{1\times 1}\\ &= [e^{\frac{2\pi i}{n}\cdot d(r_1+r_2)}]_{1\times 1}\\ &= [e^{\frac{2\pi i}{n}\cdot d\cdot[(r_1+r_2)(\text{mod } n)]}]_{1\times 1}.\end{aligned}$$

Similarly, we have that:

$$\begin{aligned}\phi_d(a^{r_1}a^{r_2}) &= \phi_d(a^{r_1+r_2})\\ &= \phi_d(a^{(r_1+r_2)(\text{mod } n)})\\ &= [e^{\frac{2\pi i}{n}\cdot d\cdot[(r_1+r_2)(\text{mod } n)]}]_{1\times 1}.\end{aligned}$$

We thus find that the mapping

$$\phi_d \colon C_n \to \mathrm{GL}_1(\mathbb{C})$$

is a representation for each index d.

Recall that a representation

$$\rho \colon G \to \mathrm{GL}(V)$$

of a group G is irreducible if V is non-trivial and has no non-trivial proper G-invariant subspaces. Considering the morphism

$$\phi_d \colon C_n \to \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C},$$

we observe that $\mathbb{C}$ is nontrivial, and since $\mathbb{C}$ is a 1-dimensional vector space, we find that $\mathbb{C}$ has no non-trivial proper subspaces. Therefore, the morphism

$$\phi_d \colon C_n \to \mathrm{GL}_1(\mathbb{C}),$$

must be an irreducible representation. It is obvious that ψ_d is given by the trace of ϕ_d. That is, ψ_d is the character of the irreducible representation ϕ_d.

Exercise 1.126. Show that for a character χ of C_n, $\chi(e) = 1$ if and only if $\chi(g^r) = \chi(g)^r$ for all $g \in C_n$ and $0 \leq r \leq n-1$.

Solution 1.127. $(\Longrightarrow)$ First, suppose that $\chi(e) = 1$, letting

$$\rho \colon C_n \to \mathrm{GL}_m(\mathbb{C})$$

be a representation of the multiplicative cyclic group C_n, letting $m \in \mathbb{N}$. Now, since ρ is a group homomorphism, we know that ρ must map the identity element $e \in C_n$ to the $m \times m$ identity matrix $I_m \in \mathrm{GL}_m(\mathbb{C})$. We thus have that

$$\chi(e) = \chi_\rho(e) = \mathrm{tr}(\rho(e)) = \mathrm{tr}(I_m) = m = 1.$$

We thus find that the codomain $\mathrm{GL}_m(\mathbb{C})$ of the group homomorphism ρ is necessarily equal to $\mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^*$. Now, let $g \in C_n$, and let $r \in \mathbb{N}_0$ be such that $0 \leq r \leq n-1$. Let

$$\rho(g) = [c_g]_{1\times 1},$$

where $c_g \in \mathbb{C}^*$. We thus have that

$$\rho(g)^r = [c_g]_{1\times 1}^r = \left[c_g^r\right]_{1\times 1}.$$

Since ρ is a group homomorphism, we thus have that

$$\rho(g^r) = \left[c_g^r\right]_{1\times 1}.$$

Therefore,

$$\chi(g^r) = \chi_\rho(g^r) = \mathrm{tr}(\rho(g^r)) = \mathrm{tr}(\left[c_g^r\right]_{1\times 1}) = c_g^r.$$

Now consider the expression $\chi(g)$. Since

$$\rho(g) = [c_g]_{1\times 1},$$

we thus have that

$$\chi(g) = \mathrm{tr}([c_g]_{1\times 1}) = c_g,$$

and we thus find that

$$\chi(g)^r = c_g^r,$$

thus proving the desired equality whereby $\chi(g^r) = \chi(g)^r$.

($\Longleftarrow$) Conversely, suppose that $\chi(g^r) = \chi(g)^r$ for all $g \in C_n$ and $0 \leq r \leq n-1$. Again let

$$\rho\colon C_n \to \mathrm{GL}_m(\mathbb{C})$$

be a representation of the multiplicative cyclic group C_n, again letting $m \in \mathbb{N}$. Again since ρ is a group homomorphism, we have that ρ must map the identity element e in C_n to the $m \times m$ identity matrix I_m in the general linear group $\mathrm{GL}_m(\mathbb{C})$ given by the codomain of ρ. Now, from our assumption that the equality

$$\chi(g^r) = \chi(g)^r,$$

we have that

$$\chi(e^r) = \chi(e)^r,$$

for all $r \in \mathbb{N}_0$ whereby $0 \leq r \leq n-1$. We thus find that

$$\chi(e) = \chi(e)^r,$$

for all $r \in \mathbb{N}_0$ satisfying the inequality whereby $0 \leq r \leq n-1$. Now, we know that $\chi(e)$ must be equal to the trace of $I_m \in \mathrm{GL}_m(\mathbb{C})$. Therefore, $\chi(e) = m$. Therefore,

$$m = m^r,$$

for all $r \in \mathbb{N}_0$ satisfying the inequality whereby $0 \leq r \leq n-1$. But recall that $m \in \mathbb{N}$. Since m is a positive integer and

$$m = m^r,$$

for all $0 \leq r \leq n-1$, we may thus deduce that $m = 1$, with $\chi(e) = m = 1$, as desired.

Exercise 1.128. Show that for a character χ of C_n, if $\chi(a^r) = e^{2r\pi i/n}$ for all $1 \leq r \leq n-1$, then $\chi(e) \equiv 1 (\operatorname{mod} n)$. Hint: compute the multiplicity of the trivial character in χ.

Solution 1.129. Let

$$\rho\colon C_n \to \mathrm{GL}_m(\mathbb{C})$$

be a group homomorphism, and let $\chi = \chi_\rho$ denote the corresponding character. Suppose that $\chi(a^r) = e^{2r\pi i/n}$ for all $1 \leq r \leq n-1$. We proceed to consider the multiplicity of the trivial character χ^T of χ. Recall that a trivial representation of a group maps each element in such a group to a fixed identity automorphism. The multiplicity of the trivial character in χ is equal to $\langle \chi, \chi^T \rangle$. Now, from the definition of the scalar product $\langle \cdot, \cdot \rangle$, we find that:

$$\begin{aligned}
\langle \chi, \chi^T \rangle &= \frac{1}{|C_n|} \sum_{c \in C_n} \chi(c) \chi^T(c^{-1}) \\
&= \frac{1}{n} \sum_{c \in C_n} \chi(c) \\
&= \frac{1}{n} \left(\chi(e) + e^{\frac{2\pi i}{n}} + e^{\frac{4\pi i}{n}} + \cdots + e^{\frac{2(n-1)\pi i}{n}} \right) \\
&= \frac{1}{n} \left(\chi(e) - 1 \right).
\end{aligned}$$

We proceed to remark that $\frac{1}{n}(\chi(e) - 1)$ must be an integer, since $\langle \chi, \chi^T \rangle$ is the multiplicity of the trivial character in χ. Write $\langle \chi, \chi^T \rangle = k$, letting $k \in \mathbb{N}_0$. We thus find that $\chi(e) - 1 = kn$, which implies that $\chi(e) \equiv 1 (\operatorname{mod} n)$.

Exercise 1.130. Let $D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$ be the dihedral group of order $2n$ where n is odd with $a^n = b^2 = e$ and $ba = a^{-1}b$. Let $V = \mathscr{L}\{v_h : h \in D_n\}$ be the module where g acts on V by $g.v_h = v_{ghg^{-1}}$ and for each X conjugacy class of D_n, let $V_X = \mathscr{L}\{v_h : h \in X\} \subseteq V$ be a submodule. Show that the sets $X_0 = \{e\}$, $X_i = \{a^i, a^{-i}\}$ for $1 \leq i \leq (n-1)/2$ and $X' = \{b, ba, ba^2, \ldots, ba^{n-1}\}$ are all conjugacy classes of D_n.

Solution 1.131. Letting g be an arbitrary element in D_n, we have that $geg^{-1} = g \cdot g^{-1} = e$, which proves that $\{e\}$ is a conjugacy class.

Now, consider the dihedral relation whereby $ba = a^{-1}b$. From this dihedrla relation, we have that

$$ba^2 = a^{-1}ba = a^{-2}b,$$

and by induction, it is easily seen that

$$ba^i = a^{-i}b,$$

for all $i \in \mathbb{N}_0$. So, given an element of the form a^j in D_n, we have that

$$a^j a^i a^{-j} = a^{j+i-j} = a^i \in X_i = \{a^i, a^{-i}\}$$

and

$$a^{-j} a^i a^j = a^{-j+i+j} = a^i \in X_i = \{a^i, a^{-i}\}.$$

Similarly, given an element of the form ba^j in D_n, we have that:

$$\left(ba^j\right) a^i \left(ba^j\right)^{-1} = ba^j a^i a^{-j} b^{-1}$$

$$\begin{aligned} &= ba^{j+i-j}b^{-1} \\ &= ba^{i}b^{-1} \\ &= a^{-i}bb^{-1} \\ &= a^{-i} \in X_i = \{a^i, a^{-i}\}. \end{aligned}$$

Similarly, we have that:

$$\begin{aligned} \left(ba^j\right) a^{-i} \left(ba^j\right)^{-1} &= ba^j a^{-i} a^{-j} b^{-1} \\ &= ba^{j-i-j}b^{-1} \\ &= ba^{-i}b^{-1} \\ &= a^{i}bb^{-1} \\ &= a^{i} \in X_i = \{a^i, a^{-i}\}. \end{aligned}$$

This proves that X_i is a conjugacy class of D_n.

Finally, consider the set $X' = \{b, ba, ba^2, \dots, ba^{n-1}\}$. Given an element of the form a^j in D_n, and given an element of the form ba^i in the set X', we have that:

$$\begin{aligned} a^j ba^i a^{-j} &= a^j ba^{i-j} \\ &= a^j a^{-(i-j)} b \\ &= a^j a^{-i+j} b \\ &= a^{2j-i} b \\ &= ba^{i-2j} \in X'. \end{aligned}$$

This shows that $ba^i \sim ba^k$ for all i and k, writing k in place of $i - 2j$. Similarly, given an element of the form ba^j in D_n, and given an element of the form ba^i in the set X', we have that:

$$\begin{aligned} \left(ba^j\right) \cdot ba^i \cdot \left(ba^j\right)^{-1} &= ba^j \cdot ba^i \cdot a^{-j} b^{-1} \\ &= ba^j ba^{i-j} b^{-1} \\ &= ba^j a^{-i+j} bb^{-1} \\ &= ba^j a^{-i+j} \\ &= ba^{-i+2j} \in X'. \end{aligned}$$

We thus find that X' is a conjugacy class of D_n, as desired.

Exercise 1.132. With respect to the previous exercise, show that if $n = 5$, $V_{X'}$ decomposes into 3 irreducible submodules, exactly one of which has a trivial action.

Solution 1.133. Letting $n = 5$, consider the submodule $V_{X'}$:

$$V_{X'} = \mathscr{L}_{\mathbb{C}}\{v_b, v_{ba}, v_{ba^2}, v_{ba^3}, v_{ba^4}\}.$$

Define W_0 as follows:

$$W_0 = \mathscr{L}_{\mathbb{C}}\{v_b + v_{ba} + v_{ba^2} + v_{ba^3} + v_{ba^4}\}.$$

We claim that W_0 is a submodule of $V_{X'} \leq V$ with a trivial action. Since X' is a conjugacy class, we know that W_0 must be stable under the action of D_5. But furthermore, we claim that the action of D_5 on W_0 must be trivial. We know that given $g \in D_5$ and an element ba^i in the conjugacy class $X' = \{b, ba, ba^2, ba^3, ba^3, ba^4\}$, we have that

$$g\left(ba^i\right)g^{-1} \in X'$$

since X' is a conjugacy class of D_5. So, in other words, the mapping

$$\star : D_5 \times X' \to X'$$

whereby

$$g \star x = gxg^{-1}$$

for $g \in D_5$ and $x \in X'$ is well-defined. But furthermore, for fixed $g \in D_5$, we claim that the mapping

$$\phi_g : X' \to X'$$

on X' whereby

$$\phi_g(x) = g \star x = gxg^{-1}$$

for $x \in X'$ is actually a bijection on X'. The mapping ϕ_g is certainly injective, since for $x, y \in X'$, we have that:

$$\begin{aligned} \phi_g(x) = \phi_g(y) &\Longrightarrow gxg^{-1} = gyg^{-1} \\ &\Longrightarrow x = y. \end{aligned}$$

Similarly, it is clear that ϕ_g is sujective, since for y in the codomain of ϕ_g, the product $g^{-1}yg$ must be in the conjugacy class X', and $\phi_g(g^{-1}yg) = y$. So, for each element g in D_5, we have that

$$g.(v_b + v_{ba} + v_{ba^2} + v_{ba^3} + v_{ba^4}) = v_{\sigma_g(b)} + v_{\sigma_g(ba)} + v_{\sigma_g(ba^2)} + v_{\sigma_g(ba^3)} + v_{\sigma_g(ba^4)}$$

for some permutation σ_g of the conjugacy class $\{b, ba, ba^2, ba^3, ba^4\}$. Since W_0 is 1-dimensional, we have that W_0 is irreducible. We now make use of Maschke's theorem.

Now, let

$$\rho : D_5 \to \mathrm{Aut}(V_{X'})$$

denote the mapping whereby ρ_g is the linear mapping on $V_{X'}$ satisfying

$$\rho(g)(v_{ba^i}) = \rho_g(v_{ba^i}) = v_{gba^ig^{-1}}$$

for all $g \in D_5$. The mapping ρ is a group homomorphism, and is therefore a representation of D_4. We have shown that W_0 is an invariant subspace of of $V_{X'}$. So, by Maschke's theorem, there exists an invariant subspace W_1 of $V_{X'}$ such that $V_{X'} = W_0 \oplus W_1$. We remark that W_1 must be of dimension 4.

Since characters are constant on conjugacy classes, we begin by considering the following matrix given by ρ_b acting on elements in the given basis for $V_{X'}$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

This shows that $\chi^{V_{X'}}(b) = 1$. Similarly, we have that $\chi^{V_{X'}}(e) = 5$, and $\chi^{V_{X'}}(a^i) = 0$. Now compute $\langle \chi^{V_{X'}}, \chi^T \rangle$ and $\langle \chi^{V_{X'}}, \chi^{V_{X'}} \rangle$:

$$\begin{aligned}
\langle \chi^{V_{X'}}, \chi^T \rangle &= \frac{1}{10}(5 + 0 + 0 + 0 + 0 + 1 + 1 + 1 + 1 + 1) = 1 \\
\langle \chi^{V_{X'}}, \chi^{V_{X'}} \rangle &= \frac{1}{10}(25 + 0 + 0 + 0 + 0 + 1 + 1 + 1 + 1 + 1) = 3.
\end{aligned}$$

From the above equalities, we may deduce that $V_{X'}$ decomposes into 3 irreducible submodules, exactly one of which has a trivial action.

Exercise 1.134. Let G be a finite group. Let G act on itself by conjugation and let $\mathrm{Fix}_G(G)$ be the set of fixed points by this action. Show that $\mathrm{Fix}_G(G) = Z(G)$.

Solution 1.135. Recall that the center of a group G, denoted $Z(G)$, may be defined as follows:

$$Z(G) = \{g \in G : \forall h \in G \ gh = hg\}.$$

Now, let

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

denote the group action on G given by conjugation. Explicitly,

$$h \bullet g = hgh^{-1},$$

for $g, h \in G$.

Now, $\mathrm{Fix}_G(G)$ denotes the set of points which are fixed by this action:

$$\begin{aligned}
\mathrm{Fix}_G(G) &= \{g \in G : \forall h \in G \ h \bullet g = g\} \\
&= \{g \in G : \forall h \in G \ hgh^{-1} = g\} \\
&= \{g \in G : \forall h \in G \ hg = gh\} \\
&= Z(G).
\end{aligned}$$

Exercise 1.136. Let T and S be subgroups of a finite group G such that $|T| = |S|$. Let T act on the left cosets, G/S, by left multiplication and let $\mathrm{Fix}_T(G/S)$ be the dixed points under the action. Show that if $gS \in \mathrm{Fix}_T(G/S)$, then $T = gSg^{-1}$.

Solution 1.137. Let $\bullet$ denote the action on $T \times (G/S)$ whereby:

$$t \bullet (gS) = t(gS).$$

Let set $\mathrm{Fix}_T(G/S)$ is the set of fixed points under this action:

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

So, let the left coset gS be in the above set, letting $g \in G$. So, for $t \in T$,

$$\{t \cdot g \cdot s : s \in S\} = \{g \cdot s : s \in S\}.$$

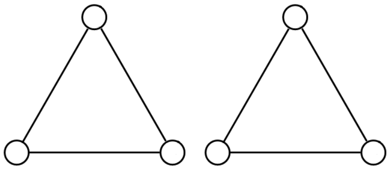


Figure 1: A D_3 action is defined on colorings of diagrams of the form indicated above.

So, for each $t \in T$ and each $s \in S$, there exists an element $u \in S$ such that:

$$t \cdot g \cdot s = g \cdot u.$$

So, for each $t \in T$ and each $s \in S$, there exists an element $u \in S$ such that:

$$t = g \cdot u \cdot s^{-1} \cdot g^{-1}.$$

But s is an element in S, and u is also an element in S. So, since S is a subgroup of G, we thus have that S must be closed under the underlying binary operation of G, which means that the product $u \cdot s^{-1}$ must be in S. So,

$$t = g \cdot u \cdot s^{-1} \cdot g^{-1} \in gSg^{-1},$$

thus proving the inclusion whereby

$$T \subseteq gSg^{-1}.$$

Now, we make use of the equality whereby $|T| = |S|$ in the following manner.

We have thus har shown that the inclusion whereby $T \subseteq gSg^{-1}$ holds. Now, consider the cardinality of gSg^{-1}. We claim that the sets S and gSg^{-1} are bijectively equivalent. Consider the mapping $\phi_g : S \to gSg^{-1}$ whereby $\phi_g(s) = gsg^{-1}$. It is clear that this mapping is injective, since: $\phi_g(s) = \phi_g(t)$ implies that $gag^{-1} = gtg^{-1}$, which in turn implies that $s = t$. Similarly, it is clear that this mapping is surjective, since for gsg^{-1} in the codomain, we have that $\phi_g(s) = gsg^{-1}$. So, we have shown that

$$|S| = |gSg^{-1}|.$$

But since $|S| = |T|$, we have that $|T| = |gSg^{-1}|$. But since T is contained in gSg^{-1}, and T and gSg^{-1} are bijectively equivalent, we may deduce that $T = gSg^{-1}$.

Exercise 1.138. Let $D_3 = \{e, a, a^2, b, ba, ba^2\}$ be the dihedral group of order 6 with $a^3 = b^2 = e$ and $ba = a^2b$. Define an action on colorings of the diagrams of the form indicated in Fig. 1, where the vertices are either black or white. There are $2^6 = 64$ total colorings, but we would like to know how many orbits there are under the action of D_3 where a rotates both colored diagrams (simultaneously) 120° clockwise and b reflects the two diagrams across the vertical between them. For example, if we act ba on the diagram on the left in Fig. 2, we obtain the diagram on the right in Fig. 2 by $ba.(D) = b.(a.(D))$.

Prove that this defines a D_3-action on the colorings of the diagram.

Solution 1.139. To prove that the given action is actually a group action, since the given group is defined in terms of the generators a and b and the relations $a^3 = b^2 = e$ and $ba = a^2b$, we need to show that the given action agrees with the above relations.

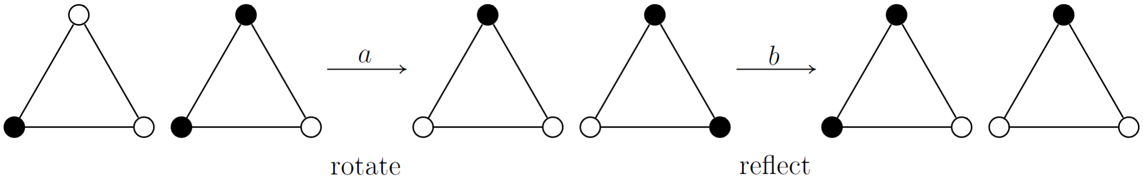


Figure 2: An illustration of the group action . defined on colorings of diagrams as in Fig. 1.

Relation 1: $a^3 = b^2 = e$. Let $1, 2, 3, 4, 5$, and 6, as below, denote colors. Fig. 3 illustrates that the given action . is such that

$$a.a.a.x = x$$

for an element x in the D_3-set X consisting of 64 colorings. This shows that the given action . agrees with the dihedral relation whereby $a^3 = e$.

Fig. 4 illustrates that the given action . is such that

$$b.b.x = x$$

for element $x \in X$. So the action . agrees with the dihedral relation whereby $b^2 = e$.

Fig. 5 illustrates that the given action . is such that

$$e.x = x$$

for elements $x \in X$.

So, the above three figures together illustrate that the given action agrees with the dihedral relations whereby $a^3 = b^2 = e$.

Relation 2: $ba = a^2 b$.

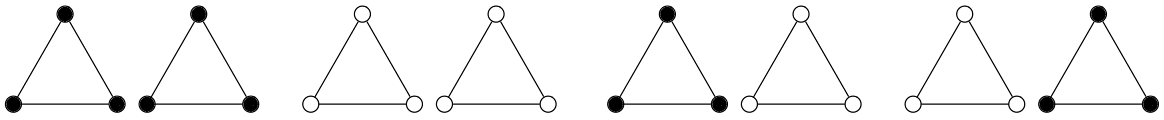
The following two figures show that the given action defines a D_3-action on the colorings of the given diagram, with respect to the given definition of D_3, defined in terms of generators and relations.

Exercise 1.140. With respect to the previous exercise, use Burnside's Lemma,

$$\# \text{ orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}_g(E)|$$

to determine the number of orbits of colorings under the action of D_3.

Solution 1.141. We evaluate $\text{Fix}_g(E)$ for $g \in G$, in order to use Burnside's Lemma. First of all, the identity element e fixes everything, so $\text{Fix}_e(E) = E$. Now observe that $\text{Fix}_a(E)$ and $\text{Fix}_{a^2}(E)$ each consist of the following diagrams.



We have that $\text{Fix}_b(E)$ consists of the following diagrams.

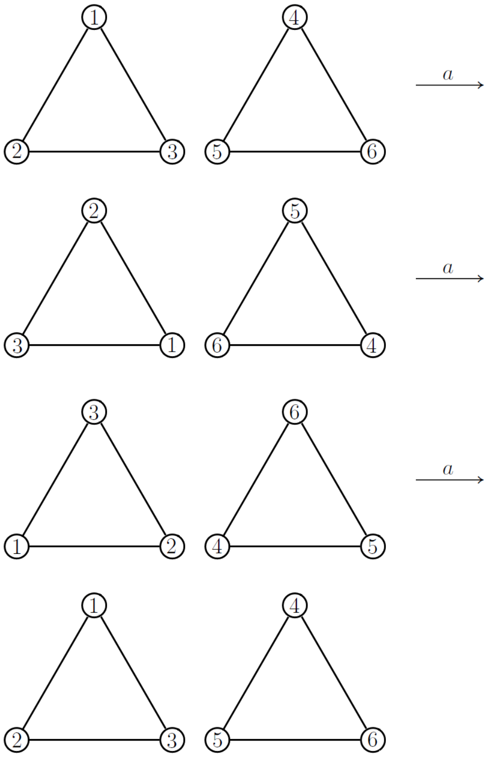


Figure 3: An illustration of the identity $a^3 = e$, with respect to the group action on the set of all colorings of diagrams of the form indicated in Fig 1.

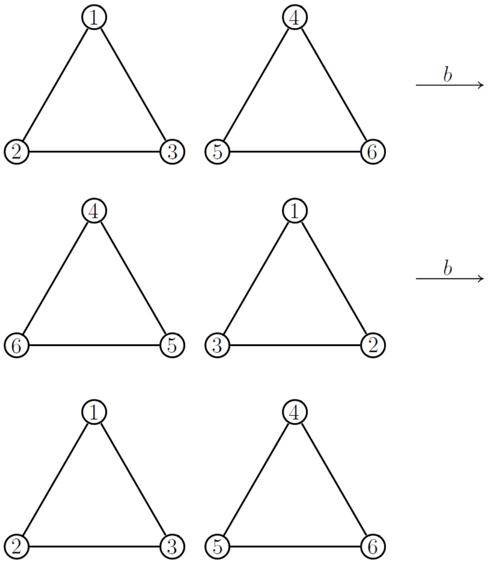


Figure 4: An illustration of the identity $b^2 = e$, with respect to the group action on the set of all colorings of diagrams of the form indicated in Fig 1.

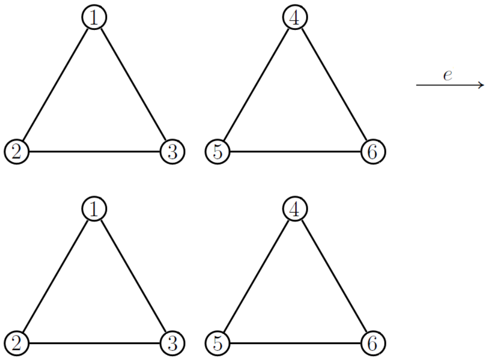


Figure 5: An illustration of the group action axiom whereby $e.x = x$.

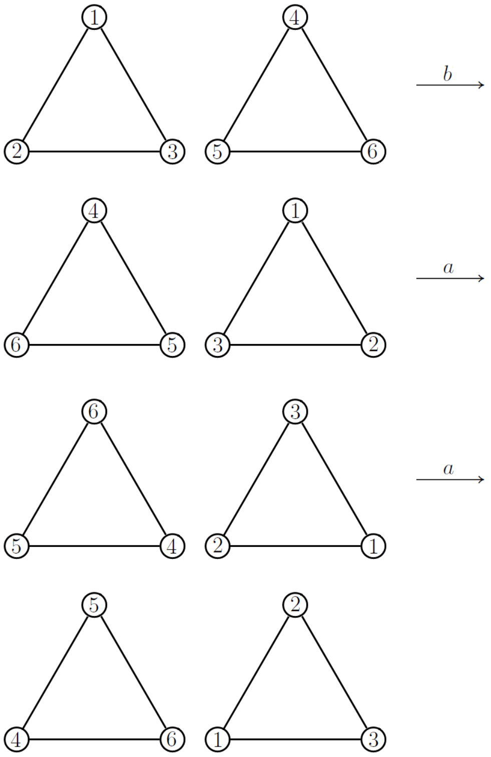


Figure 6: An illustration of the given action.

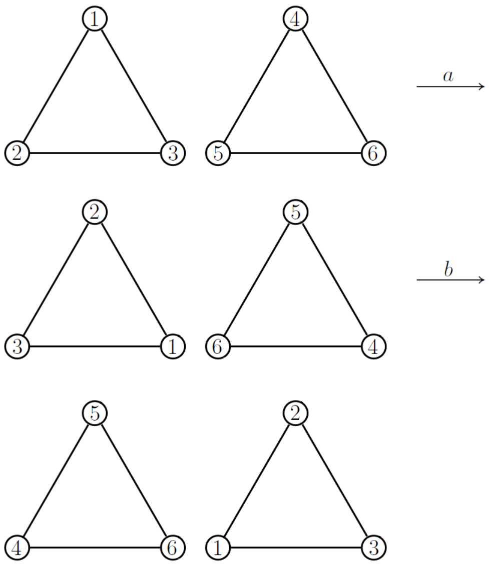
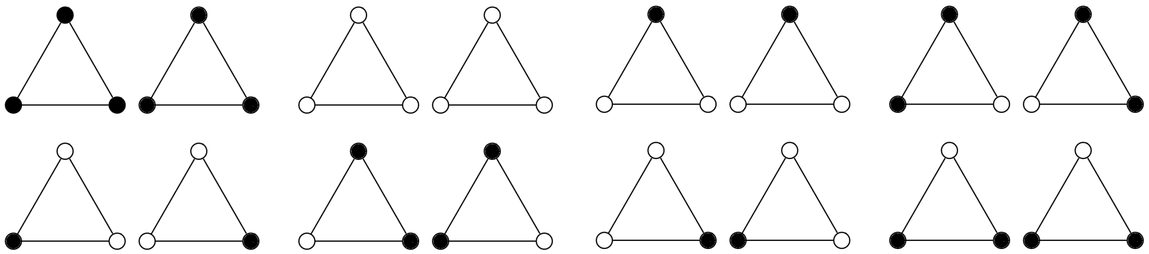
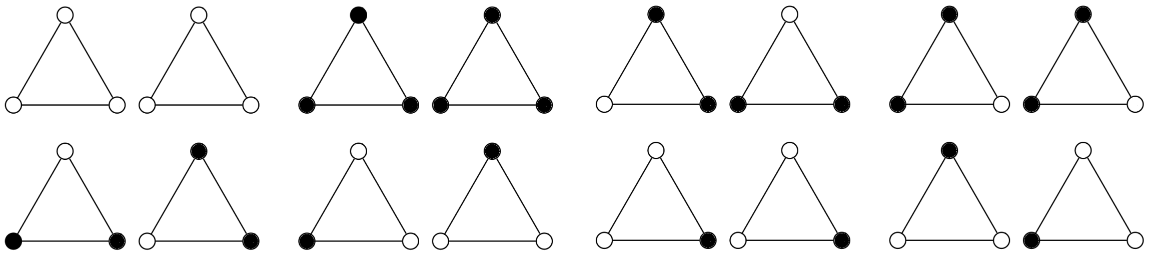


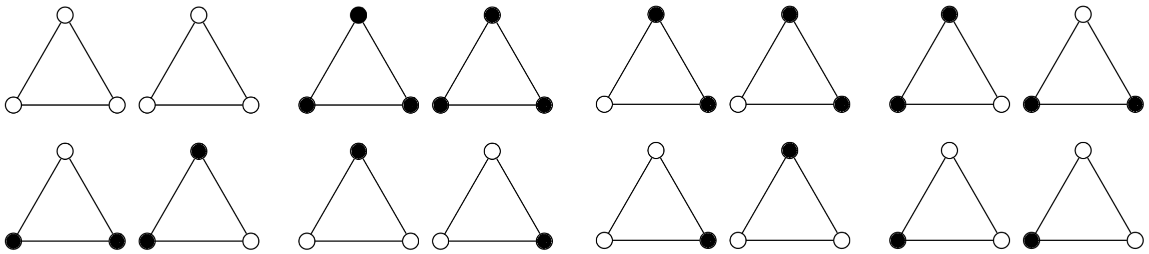
Figure 7: An illustration of the given action.



We have that $\mathrm{Fix}_{ba}(E)$ consists of the following diagrams.



We have that $\mathrm{Fix}_{ba^2}(E)$ consists of the following diagrams.



So, by Burnside's Lemma, we have that:

$$\begin{aligned}\#\text{ of orbits} &= \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_g(E)| \\ &= \frac{2^6+4+4+8+8+8}{6} \\ &= 16.\end{aligned}$$

Exercise 1.142. Let R be a ring with 1. Letting I be an ideal of R, prove that $I = R$ iff I contains a unit.

Solution 1.143. Recall that an ideal I of a ring R is a nonempty subset of R such that

$$a \in I, b \in I \Longrightarrow a + b \in I$$

and

$$a \in I, r \in R \Longrightarrow ra \in I.$$

So, let R be a ring with 1, as above, and let I be an ideal of R.

($\Longrightarrow$) Assume that $I = R$. Since R is a ring with 1, and since $I = R$, we have that I contains 1, and we thus have that I contains a unit.

($\Longleftarrow$) Conversely, suppose that I contains a unit u. Since u is a unit, we have that there exists an element v in R such that $uv = vu = 1$. But since I is an ideal, we have that vu must be in I, so 1 must be in I. Again since I is an ideal, we thus have that each expression of the form $r \cdot 1 = r$ must be in I, thus proving the desired equality whereby $I = R$.

Exercise 1.144. Let R be a commutative ring with unity. Prove that R is a field iff the only ideals of R are the trivial ideal and R itself.

Solution 1.145. ($\Longrightarrow$) Suppose that R is a field. Let I be an arbitrary ideal of R. We begin by considering the case whereby $1 \in I$, and we later consider the case in which $1 \notin I$. So, suppose that $1 \in I$. From our results given in our previous solution, since I contains a unit, we thus have that $I = R$. Now suppose that $1 \notin I$. By definition of an ideal, we have that I must be nonempty. So, let a be an element in I. By definition of an ideal, we have that I must be closed under addition. We may thus deduce that $0 \in I$. Now, by way of contradiction, suppose that there exists a nonzero element $b \neq 0$ in I. Now, under our assumption that R is a field, since b is nonzero, we find that b is invertible. But since I is an ideal, with $b \in I$, we thus find that $b^{-1} \cdot b \in I$. Therefore, $1 \in I$. But this contradicts that $1 \notin I$. We thus have that if $1 \notin I$, then $I = \{0\}$.

($\Longleftarrow$) Conversely, suppose that the only ideals of R are the trivial ideal and R itself. Now, let r be a nonzero element in R. Consider the principal ideal $\langle r\rangle$ generated by $r \in R$. From our initial assumption that the only ideals of R are $\{0\}$ and R itself, we may thus deduce that $\langle r\rangle = R$. Since $1 \in R$, we thus find that $1 \in \langle r\rangle = rR$. So, there exists some element $s \in R$ such that $1 = rs$, thus proving that r is invertible.

Exercise 1.146. Compute $\gcd(2, x)$ in the Euclidean domain $\mathbb{Q}[x]$.

Solution 1.147. Since $x = \left(\frac{x}{2}\right) \cdot 2 + 0$, we have that 2 divides x as well as 2. So, $\gcd(2, x) = 2$, by the Euclidean algorithm.

Exercise 1.148. Show that if F is a field, then $F[x]$ is a Euclidean domain.

Solution 1.149. We begin by reviewing some preliminary terminology. The following definitions are from "Introductory Algebraic Number Theory" by Alaca and Williams.

Let D be an integral domain. A mapping $\phi: D \to \mathbb{Z}$ is called a Euclidean function on D if it has the following two properties:

(i) $\phi(ab) \geq \phi(a)$, for all $a, b \in D$ with $b \neq 0$; and

(ii) If $a, b \in D$ with $b \neq 0$ then there exist $q, r \in D$ such that $a = qb + r$ and $\phi(r) < \phi(b)$.

Again, let D be an integral domain. If D possesses a Euclidean function ϕ, then D is called a Euclidean domain with respect to ϕ.

So, letting F be a field, to show that $F[x]$ is a Euclidean domain, we begin by constructing an appropriate Euclidean function. For $p(x) \in F[x]$, define $\phi(p(x))$ so that $\deg(p(x))$ if $p(x)$ is nonzero, and let $\deg(p(x)) = -1$ otherwise. It is clear that $\phi(ab) \geq \phi(a)$ for all $a, b \in D$ with $b \neq 0$. The second axiom may be proven inductively using "long division" for polynomials in the following sense. If $a(x)$ is the zero polynomial then take $q(x) = r(x) = 0$. So, let $a(x) \neq 0$. We may prove the existence of $q(x)$ and $r(x)$ by induction with respect to the degree of $a(x)$.

Exercise 1.150. Show that if F is a field, then $F[x]$ is a principal ideal domain and a unique factorization domain.

Solution 1.151. We have previously shown that if F is a field, then $F[x]$ is a Euclidean domain. But since every Euclidean domain is a principal ideal domain, we thus have that $F[x]$ is a principal ideal domain. Also, it is known that every PID is a UFD. In the following exercise, we prove that for a ring R, R is a UFD iff $R[x]$ is a UFD. Since a field is necessarily a UFD, we thus have that $F[x]$ is a UFD.

Exercise 1.152. Prove that R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Solution 1.153. Suppose that R is a UFD. Let $p(x)$ be a nonzero element in the polynomial ring $R[x]$ that is not a unit. If $p(x)$ is irreducible, then it is a product of irreducibles. Now suppose that $p(x)$ is not irreducible. Write $p(x) = s_1(x)s_2(x)$, letting $s_1(x)$ and $s_2(x)$ be non-units. Repeating this argument inductively shows that every nonzero element of $R[x]$ that is not a unit can be written as a product of irreducibles. Since R is a UFD, the elements in $R[x]$ which are in R satisfy the unique factorization property. A degree-1 polynomial $ax + b$ in $R[x]$ must satisfy the unique factorization property, since if $ax + b = c(dx + e)$, then $a = cd$ and $b = ce$, but R is a UFD. Continuing in the manner inductively shows that $R[x]$ is a UFD. Conversely, if $R[x]$ is a UFD, then R must be a PFD since $R \subseteq R[x]$.

Exercise 1.154. Let $f(x) \in \mathbb{Z}[x]$. Prove that if $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Solution 1.155. Our solution is based upon a proof given in Joseph Gallian's *Contemporary Abstract Algebra.* Recall that the content of a nonzero polynomial with integer coefficients is the greatest common divisor of the coefficients. A primitive polynomial is a polynomial with integer coefficients which has content 1. Let $f(x) \in \mathbb{Z}[x]$, and suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are in $\mathbb{Q}[x]$. We may assume without loss of generality that $f(x)$ is primitive, because we may divide $f(x)$ and $g(x)$ by the content of $f(x)$. Let a be the least common multiple of the denominators of the coefficients of $g(x)$, and let b be the least common multiple of the denominators of the coefficients of $h(x)$. Let c_1 be the content of $ag(x)$ and let c_2 be the content of $bh(x)$. The content of $abf(x)$ is ab since $f(x)$ is primitive. Since the product of two primitive polynomials is primitive, we have that the content of $abf(x)$ is also equal to c_1c_2. So, $f(x) = g_1(x)h_1(x)$, writing $ag(x) = c_1g_1(x)$ and $bh(x) = c_2h_1(x)$, where the degree of g_1 is equal to the degree of g, and similarly for h_1.

Exercise 1.156. Letting R be a commutative ring with unity, and letting I be an ideal of R, prove that I is a prime ideal if and only if R/I is an integral domain.

Solution 1.157. ($\Longrightarrow$) Suppose that I is a prime ideal, and consider the quotient ring R/I. Let r_1 and r_2 be elements in R, so that $r_1 + I$ and $r_2 + I$ are in R/I. Now consider the product

$$(r_1 + I)(r_2 + I) = r_1r_2 + I.$$

Since R is a commutative ring with unity, it is clear that R/I is also a commutative ring with unity. So, to prove that R/I is an integral domain, it remains to prove that R/I has no zero divisors. By way of contradiction, suppose that it is not the case that R/I has no zero divisors. So, suppose that

$$(r_1 + I)(r_2 + I) = r_1r_2 + I = 0 + I = I,$$

for some nonzero elements $r_1 + I$ and $r_2 + I$ in the quotient ring R/I. But since

$$r_1r_2 + I = 0 + I = I,$$

we may deduce that the product r_1r_2 is in I, and since I is a prime ideal, we may thus deduce that $r_1 \in I$ or $r_2 \in I$. So, we may assume without loss of generality that $r_1 \in I$. Therefore, $r_1 + I = 0 + I$. But this contradicts that $r_1 + I$ is nonzero.

($\Longleftarrow$) Conversely, suppose that R/I is an integral domain. Let r_1 and r_2 be elements in R, and suppose that $r_1r_2 \in I$. Equivalently, $r_1r_2 + I = (r_1 + I)(r_2 + I) = 0 + I$. But since R/I is an integral domain, we have that R/I has no zero divisors. So, $r_1 + I = 0 + I$ or $r_2 + I = 0 + I$. We may assume without loss of generality that $r_1 + I = 0 + I$. Since $r_1 + I = I$, we thus find that $r_1 \in I$, thus proving that I is a prime ideal.

1.1 Practice problems for the final exam

Exercise 1.158. Show that a group of order $2001 = 3 \cdot 23 \cdot 29$ must contain a normal cyclic subgroup of index 3.

Solution 1.159. Let G be an arbitrary group of order $2001 = 3 \cdot 23 \cdot 29$. The following integer tuple consists of the positive divisors of $|G|$, ordered canonically:

$$(1, 3, 23, 29, 69, 87, 667, 2001).$$

Now, reduce the entries in the above tuple modulo 23:

$$(1, 3, 0, 6, 0, 18, 0, 0).$$

Let n_{23} denote the number of Sylow 23-subgroups of G. By Sylow's First Theorem, $n_{23} \geq 1$. By Sylow's Third Theorem, we have that n_{23} must be congruent to 1 modulo 23, and that n_{23} must divide the order of G. From the above integer tuple, it is clear that $n_{23} = 1$. So, there is a unique Sylow 23-subgroup of G. Let this unique Sylow 23-subgroup be denoted by H_{23}. By Sylow's Second Theorem, we have that all Sylow 23-subgroups must be conjugates of each other. But since $n_{23} = 1$, we may deduce that H_{23} must be a normal subgroup of G.

So, we obtain the subnormal series of the form

$$H_{23} \triangleleft G.$$

We thus proceed to consider the quotient group G/H_{23}. We begin by observing that the quotient group G/H_{23} is of order $87 = 3 \cdot 29$. The positive divisors of the order of G/H_{23} are: 1, 3, 29, and 87. Reducing these divisors modulo 29, we find that there must be a unique Sylow 29-subgroup $\overline{K}$ of G/H_{23}. By Sylow's Second Theorem, we have that $\overline{K}$ must be a normal subgroup G/H_{23}, since there is only one Sylow 29-subgroup of G/H_{23}:

$$H_{23}/H_{23} \trianglelefteq \overline{K} \triangleleft G/H_{23}.$$

So, by the Fourth Isomorphism Theorem for groups, we may thus deduce that there is a corresponding group K such that

$$H_{23} \trianglelefteq K \triangleleft G,$$

and such that K is of order $23 \cdot 29 = 667$.

So, we have shown that there exists a normal subgroup K of G such that $|K| = 667$. That is, we have shown that a group G of order 2001 must contain a normal subgroup of index

$$\frac{2001}{667} = 3.$$

So, it remains to prove that K is cyclic.

The positive divisors of 667 are 1, 23, 29, and 667. Let η_{23} denote the number of Sylow 23-subgroups of K, and let η_{29} denote the number of Sylow 29-subgroups of K. Reducing the tuple $(1, 23, 29, 667)$ modulo 23, we find that $n_{23} = 1$. Reducing this tuple modulo 29, we obtain the equality whereby $n_{29} = 1$. Now, consider the orders of the elements in K. Of course, there is exactly one element of order 1, namely, the identity element. By Lagrange's theorem, we have that the order of an element in K must be in $\{1, 23, 29, 667\}$. Since there is a unique subgroup of K of order 23, we have that there are exactly 22 elements of order 23 in K. Since there is a unique subgroup of K of order 29, we may deduce that there are exactly 28 elements of order 29 in K. So, there are a total of

$$1 + 22 + 28 = 51$$

elements in K with an order in $\{1, 23, 29\}$. So, by Lagrange's theorem, the $667 - 51$ remaining elements in K must be of order 667. Since there exists an element in K of order 667, we thus have that K is cyclic.

Exercise 1.160. For $n \geq 3$, the dihedral group D_n of order $2n$ is given by $D_n = \langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b \rangle$. What are the conjugacy classes of D_n?

Solution 1.161. Since $g \cdot e \cdot g^{-1} = e$ for each element g in $D_{n \geq 3}$, we have that the singleton set $\{e\}$ is a conjugacy class of D_n. Let $i, j \in \mathbb{N}$. Now consider the conjugacy class of D_n containing a^j.

$$\begin{aligned} a^j a^i a^{-j} &= a^{j+i-j} = a^i \\ ba^j a^i \left(ba^j\right)^{-1} &= ba^j a^i a^{-j} b^{-1} \\ &= ba^i b^{-1} \end{aligned}$$

$$
\begin{aligned}
&= b\,\underbrace{aa\cdots a}_{i}\,b^{-1}\\
&= b\,\underbrace{aa\cdots a}_{i}\,b\\
&= ba\,\underbrace{aa\cdots a}_{i-1}\,b\\
&= a^{-1}b\,\underbrace{aa\cdots a}_{i-1}\,b\\
&= a^{-1}ba\,\underbrace{aa\cdots a}_{i-2}\,b\\
&= a^{-2}b\,\underbrace{aa\cdots a}_{i-2}\,b\\
&\cdots\\
&= a^{-i}bb\\
&= a^{-i}.
\end{aligned}
$$

We thus find that $\{a^i, a^{-i}\}$ is a conjugacy class of D_n for all $i \in \mathbb{N}$. Now consider the conjugacy class of D_n which contains the element ba^i, letting $i \in \mathbb{N}_0$.

$$
\begin{aligned}
b(ba)b &= ab\\
&= ba^{n-1}\\
ba(ba)ba &= babaa^{-1}b\\
&= babb\\
&= ba\\
ba^2(ba)ba^2 &= baababaa\\
&= baabaa^{-1}ba\\
&= baabba\\
&= baaa\\
&= ba^3\\
ba^3(ba)ba^3 &= baaababaaa\\
&= baaabaa^{-1}baa\\
&= baaabbaa\\
&= baaaaa\\
&= ba^5\\
&\text{etc.}
\end{aligned}
$$

So, in general, we have that $ba^j(ba)ba^j = ba^{2j-1}$. So, all expressions of the form ba^i for odd positive integers $i \leq n-1$ are in the conjugacy class of ba. But we also have that:

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

$$ba^{n-2}(ba)ba^{n-1} = ba^{n-5}$$
$$\text{etc.}$$

So, if n is odd, all expressions of the form ba^i for $i \in \mathbb{N}$ are in the same conjugacy class. If n is even, then the set of all expressions of the form ba^{2i} for $i \in \mathbb{N}$ is a conjugacy class, and the set of all expressions of the form ba^{2i+1} is also a conjugacy class.

Exercise 1.162. When n is odd, how many Sylow 2-subgroups does D_n have?

Solution 1.163. Let n be odd, and consider the number of Sylow 2-subgroups of D_n. The number of Sylow 2-subgroups of D_n is equal to the number of elements in D_n of order 2. The elements in D_n are precisely the elements in the following set:

$$\{1, a, a^2, \dots, a^{n-1}, b, ba, ba^2, \dots, ba^{n-1}\}.$$

The collection $\{1, a, a^2, \dots, a^{n-1}\}$ consisting of the rotational isometries in D_n forms a cyclic subgroup. By the Fundamental Theorem of Cyclic Groups, we have that: a subgroup of $\{1, a, a^2, \dots, a^{n-1}\}$ must be cyclic and must be of order d for a positive divisor d of n. But since n is odd, we find that no element in $\{1, a, a^2, \dots, a^{n-1}\}$ is of order 2.

We have that b is of order 2, since $b \neq 1$, and since $b^2 = 1$. Now consider the order of $ba \in D_n$:

$$\begin{aligned}(ba)(ba) &= baa^{-1}b \\ &= bb \\ &= 1.\end{aligned}$$

Now consider the order of $ba^2 \in D_n$:

$$\begin{aligned}ba^2ba^2 &= baabaa \\ &= baa(ba)a \\ &= baa(a^{-1}b)a \\ &= baba \\ &= 1.\end{aligned}$$

Continuing in this manner, we find that each expression of the form ba^i for $i \in \mathbb{N}_0$ is of order 2. That is, each element in the set $\{b, ba, ba^2, \dots, ba^{n-1}\}$ is of order 2. So it is clear that there are precisely n Sylow 2-subgroups of D_n in the case whereby n is odd.

Exercise 1.164. What are the composition factors of D_n?

Solution 1.165. Recall that a subnormal series is a composition series if the subnormal factors are simple. The cyclic rotational subgroup

$$\{1, a, a^2, \dots, a^{n-1}\} \leq D_n$$

must be a normal subgroup of D_n, because, in general, a subgroup of index 2 is necessarily normal. From a geometric perspective, it is easily seen that the cyclic subgroup of D_n consisting of the rotational isometries in D_n must be normal, since this subgroup is precisely the kernel of the homomorphism from D_n to $\mathbb{Z}/2\mathbb{Z}$ which maps each orientation-preserving isometry to 0, and each orientation-reversing isometry to 1.

So, it remains to consider the composition factors of the cyclic group $\{1, a, a^2, \dots, a^{n-1}\}$. By the Fundamental Theorem of Cyclic Groups, we have that: for each positive divisor d of the order of $\{1, a, a^2, \dots, a^{n-1}\}$, there exists a unique cyclic subgroup of $\{1, a, a^2, \dots, a^{n-1}\}$ of order d. Now, consider the prime factorization of n, writing

$$n = p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m}.$$

So, there exists a cyclic subgroup

$$C_{p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m - 1}} \lhd \{1, a, a^2, \dots, a^{n-1}\}$$

of order $p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m - 1}$, as well as a second subgroup

$$C_{p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m - 2}} \lhd C_{p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m - 1}} \lhd \{1, a, a^2, \dots, a^{n-1}\}$$

of order $p_{a_1}^{b_1} p_{a_2}^{b_2} \cdots p_{a_m}^{b_m - 2}$, and so forth. Continuing in this manner, we find that the composition factors of D_n are as given below, ordered based on the procedure outlined above:

$$\begin{aligned}
&\underbrace{\mathbb{Z}/p_{a_1}\mathbb{Z}, \mathbb{Z}/p_{a_1}\mathbb{Z}, \dots, \mathbb{Z}/p_{a_1}\mathbb{Z},}_{b_1 - 1} \\
&\underbrace{\mathbb{Z}/p_{a_2}\mathbb{Z}, \mathbb{Z}/p_{a_2}\mathbb{Z}, \dots, \mathbb{Z}/p_{a_2}\mathbb{Z},}_{b_2} \\
&\underbrace{\mathbb{Z}/p_{a_3}\mathbb{Z}, \mathbb{Z}/p_{a_3}\mathbb{Z}, \dots, \mathbb{Z}/p_{a_3}\mathbb{Z},}_{b_3} \\
&\cdots \\
&\underbrace{\mathbb{Z}/p_{a_m}\mathbb{Z}, \mathbb{Z}/p_{a_m}\mathbb{Z}, \dots, \mathbb{Z}/p_{a_m}\mathbb{Z},}_{b_m} \\
&\mathbb{Z}/2\mathbb{Z}.
\end{aligned}$$

Exercise 1.166. How many irreducibles does D_n have? What are the dimensions?

Solution 1.167. The number of irreducible representations of D_n is equal to the number of conjugacy classes of D_n. The conjugacy classes of D_n are given in a previous solution. We thus find that the number of irreducible representations of D_n for even n is

$$\frac{n}{2} + 3,$$

and the number of irreducible representations of D_n for odd n is $\frac{n+3}{2}$.

It is known that the possible dimensions of the irreducible representations of D_n are: 1 and 2. The commutators of D_n generate the subgroup of the squares of rotation. So, the number of 1-dimensional irreducible representations of D_n is 2 if n is odd, and 4 otherwise.

The following mappings yield irreducible representations of D_n for $1 \leq k < \frac{n}{2}$:

$$\begin{aligned}
a &\mapsto \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \\
b &\mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\end{aligned}$$

So, this shows that the total number of irreducible representations of D_n which are 1-dimensional or 2-dimensional is $\frac{n}{2}+3$ for n even and $\frac{n+3}{2}$ for n odd. This shows that the total number of irreducible representations of D_n which are 1-dimensional or 2-dimensional is equal to the total number of irreducible representations of D_n.

Exercise 1.168. For R a U.F.D., show that a non-zero element is prime if and only if it is irreducible.

Solution 1.169. ($\Longrightarrow$) Suppose that p is a non-zero prime element in a unique factorization domain R. Now, suppose that

$$p = ab,$$

where $a, b \in R$. Recall that a unique factorization domain must be an integral domain, by definition. We thus find that R is a commutative ring with unity and no zero divisors. Since

$$p = ab,$$

and since R is a unital ring, we find that:

$$p \cdot 1 = ab.$$

Therefore, $p|ab$. Since p prime, we have that p divides a or b. We may assume without loss of generality that p divides a. Write $pc = a$, letting $c \in R$. So, from the equality

$$p = ab,$$

we obtain the equality

$$p = pcb.$$

Equivalently,

$$p - pcb = 0.$$

Again since R must be a unital ring, we have that the above equality is equivalent to the following:

$$p(1 - cb) = 0.$$

Now, recall that R must be an integral domain. Since R cannot have any zero divisors, we have that p or $1 - cb$ must be equal to 0. But recall that p is non-zero. We thus have that

$$1 - cb = 0,$$

and we find that

$$1 = cb.$$

So, we have shown that b and c are both units. A symmetric argument shows that if we instead assume without loss of generality that p divides b, then a must be a unit. So we have shown that if $p = ab$, then either a or b must be a unit. Therefore, p is irreducible.

($\Longleftarrow$) Conversely, suppose that i is a non-zero irreducible element in a unique factorization domain R. If i is a unit, then i must be prime, since for a unit u, if u divides ab with $a, b \in R$, then u divides a, since $ua' = a$, where $a' = u'a$, letting u' denote the inverse of u.

Now, assume that it is not the case that i is a unit. Suppose that i divides ab, letting a and b be nonzero elements in R. Since $i|ab$, we have that

$$ic = ab$$

for some element c in R.

First consider the case whereby c is a unit. Then

$$i = abd$$

for some $d \in R$, but since R is a unique factorization domain and since $i \neq 0$ is irreducible and i is not a unit, we have that i has a unique factorization as a product of irreducible elements. But the unique factorization of i as a product of irreducible elements is precisely i, itself. Each element among a, b, and d must be non-zero, since i is nonzero. Moreover, it cannot be the case that a, b, and d are all units, since i is not a unit. So, at least one element among a, b, and d is a non-zero, non-unit element in R. We may assume without loss of generality that a is a non-zero, non-unit element in R. Again since R is a unique factorization domain, we have that a has a unique factorization as a product of irreducible elements in D. But since R is a U.F.D., we have that $a = ui$ for some unit u. But then i must divide a, thus showing that i is prime in this case.

Now, suppose that it is not the case that c is a unit. Since a and b are nonzero, we have that c is a nonzero, nonunit element in R. So, since R is a U.F.D., we have that c has a unique factorization as a product of irreducible elements:

$$i \cdot j_1 \cdot j_2 \cdot \cdots \cdot j_{m_1} = a \cdot b.$$

Recall that a and b are nonzero. If a is a unit, then we have that

$$a^{-1} \cdot i \cdot j_1 \cdot j_2 \cdot \cdots \cdot j_{m_1} = b,$$

so that i divides b. Similarly, if b is a unit, then i must divide a. So, it remains to consider the case whereby neither a nor b is a unit. In this remaining case, we have that a and b are both non-zero, non-unit elements in the unique factorization domain R. So, in this case we have that both a and b have unique factorizations as products of irreducible elements. So, we arrive at decompositions into products of irreducible elements of the following form:

$$i \cdot j_1 \cdot j_2 \cdot \cdots \cdot j_{m_1} = u \cdot k_1 \cdot k_2 \cdot \cdots \cdot k_{m_2} \cdot \ell_1 \cdot \ell_2 \cdot \cdots \cdot \ell_{m_3},$$

where u is a unit, and the remaining product on the right-hand side of the above equation is a rearrangement of the product of irreducibles on the left-hand side. So, we may assume without loss of generality that $i = k_1$. But then the irreducible terms ℓ_1, ℓ_2, …, ℓ_{m_3} for c cancel with the same terms on the other side of the above equation, which shows that

$$i \cdot j_1 \cdot j_2 \cdot \cdots \cdot j_{m_4} = u \cdot a,$$

so that

$$u^{-1} \cdot i \cdot j_1 \cdot j_2 \cdot \cdots \cdot j_{m_4} = a,$$

thus proving that i divides a, proving that i is prime in this remaining case.

Exercise 1.170. For a ring R we say that $a \in R$ is right quasi-regular (r.q.r.) if $a + x = ax$ has a solution $x = b \in R$. The unity is never r.q.r. and 0 is always r.q.r. Show that if a^2 is r.q.r., then a is r.q.r.

Solution 1.171. Letting a be an element in a unital ring R, suppose that a^2 is r.q.r. Now, observe that an element c in R is right quasi-regular if and only if $c + x - cx = 0$ has a solution $x \in R$. Equivalently, $c \in R$ is r.q.r. iff $(1-c)(1-x) = 1$ has a solution $x \in R$. So, by assumption that a^2 is r.q.r. in the unital ring R, we have that $(1-a^2)(1-x) = 1$ has a solution $x \in R$. Therefore, $(1-a)(1+a)(1-x) = 1$ has a solution $x \in R$. So, $(1-a)(1-y) = 1$ has a solution $y \in R$, which shows that a is r.q.r.

Exercise 1.172. Show that if R is a division ring, then the unity is the only non-r.q.r. element of R.

Solution 1.173. Suppose that R is a division ring. So, each non-zero element in R is invertible. That is, each non-zero element in R is a unit.

We have previously shown that, in general, for a ring S, an element $c \in S$ is r.q.r. iff $(1-c)(1-x) = 1$ has a solution $x \in S$. So, in general, for a ring S, an element $c \in S$ is right quasi-regular if and only if $1-c$ is invertible. So, assuming that R is a division ring, we have that each non-zero element in R is invertible. So, an expression of the form $1-c$ is invertible in R iff $c =\neq 1$. That is, for an element c in the division ring R, c is right quasi-regular if and only if $c =\neq 1$. That is, the only element in the division ring R which is not right quasi-regular is the unity in R.

Exercise 1.174. Prove that R is a division ring if and only if all elements of R but one are r.q.r.

Solution 1.175. ($\Longrightarrow$) Suppose that R is a division ring. From our previous solution, we have that the unity of R is the only element of R which is not right quasi-regular. So, all elements of R but one are r.q.r.

($\Longleftarrow$) Conversely, suppose that all elements of a unital ring R are r.q.r. As indicated previously, the unity is never r.q.r. So, we may deduve that all non-unity elements of the unital ring R are r.q.r. Equivalently, all non-zero elements in R are invertible. So, R must be a division ring.

Exercise 1.176. Let $\phi: G \to \text{Aut}(M)$ be a representation of a finite group G and let χ be its associated character. Show that $\frac{1}{|G|}\sum_{g \in G} \chi(g)$ is equal to the number of times the trivial representation appears in the decomposition of ϕ into irreducibles.

Solution 1.177. Let the module M be decomposed so that

$$M = \bigoplus_{i=0}^{n} M_i^{\oplus m_i},$$

where m_i denotes the multiplicity of the irreducible component M_i in the above decomposition for each index i. Let M_0 denote the module such that the character χ^{M_0} is trivial. We thus have that:

$$\langle \chi, \chi^{M_0} \rangle = m_0.$$

That is, the value of the scalar product $\langle \cdot, \cdot \rangle$ evaluated at χ and χ^{M_0} is precisely equal to the number of times the trivial representation appears in the decomposition of ϕ into irreducibles. Now expand the expression $\langle \chi, \chi^{M_0} \rangle$ as follows:

$$\langle \chi, \chi^{M_0} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi^{M_0}(g^{-1}).$$

But since the character function χ^{M_0} is trivial, we have that:

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \chi^{M_0}(g^{-1}) = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

thus proving that $\frac{1}{|G|}\sum_{g \in G} \chi(g) = m_0$.

Exercise 1.178. Letting $\phi: G \to \text{Aut}(M)$ and χ be as given above, show that if $\frac{1}{|G|}\sum_{g \in G} \|\chi(g)\|^2 = 3$, then ϕ is the idrect sum of three distinct irreducible representations.

Solution 1.179. Suppose that $\frac{1}{|G|}\sum_{g\in G}\|\chi(g)\|^2 = 3$. Let the module M be decomposed as above, with:

$$M = \bigoplus_{i=0}^{n} M_i^{\oplus m_i},$$

again letting m_i denote the multiplicity of the irreducible component M_i in the above decomposition for each index i. We thus have that:

$$\langle \chi, \chi \rangle = \sum_{i=0}^{n} m_i^2.$$

By definition of the scalar product $\langle \cdot, \cdot \rangle$, we have that

$$\langle \chi, \chi \rangle = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi(g)},$$

since we may assume without loss of generality that the matrices under consideration are unitary matrices, letting $\overline{\chi(g)}$ denote the complex conjugate of $\chi(g)$. Since $\chi(g)\overline{\chi(g)} = \|\chi(g)\|^2$, we thus have that

$$\sum_{i=0}^{n} m_i^2 = 3.$$

So each integer of the form m_i must be less than or equal to 1. So, we may deduce that there are three distinct terms in the irreducible decomposition

$$M = \bigoplus_{i=0}^{n} M_i^{\oplus m_i} = M_0 \oplus M_1 \oplus M_2,$$

each of which has multiplicity 1.

Exercise 1.180. Let R be a commutative ring with identity 1 and M a finitely generated left R-module. Show that for any $m \in M$, the set $\operatorname{Ann}(m) = \{a \in R : am = 0\} \subseteq R$ is an ideal.

Solution 1.181. Let $m \in M$. Let a_1 and a_2 be elements in R such that $a_1 m = 0$ and $a_2 m = 0$. We thus have that

$$a_1 m + a_2 m = 0.$$

But since M is a left R-module, we have that the equality $a_1 m + a_2 m = 0$ is equivalent to the equality whereby

$$(a_1 + a_2)m = 0.$$

Therefore, $a_1 + a_2$ is in $\operatorname{Ann}(m)$, thus proving that $\operatorname{Ann}(m)$ is closed with respect to the underlying additive binary operation on R. Letting a_1 be as given above, let r be an arbitrary element in the commutative unital ring R. Since

$$a_1 m = 0,$$

we find that

$$r(a_1 m) = r \cdot 0.$$

Since M is a left R-module, we may deduce that

$$(ra_1)m = 0.$$

We thus have that $\operatorname{Ann}(m)$ is closed under multiplication my elements in R, thus proving that $\operatorname{Ann}(m)$ is an ideal of R.

Exercise 1.182. Letting R and M be as given above, let $P = \{\mathrm{Ann}(m) : 0 \neq m \in M\}$. Show that a maximal element of P must be a prime ideal.

Solution 1.183. Let $\mu \in M$ be such such that $\mu \neq 0$, and $\mathrm{Ann}(\mu)$ is a maximal element in $\{\mathrm{Ann}(m) : 0 \neq m \in M\}$ Now, letting a and b be elements in the ring R, suppose that:

$$ab \in \mathrm{Ann}(\mu).$$

By way of contradiction, suppose that it is not the case that a is in $\mathrm{Ann}(\mu)$. Now, consider the ideal generated by the elements in $\mathrm{Ann}(\mu)$ and a. This ideal properly contains $\mathrm{Ann}(\mu)$, by assumption that $a \notin \mathrm{Ann}(\mu)$. An element in this ideal would be of the form $n + ra$ for some $n \in \mathrm{Ann}(\mu)$, and some $r \in R$. Therefore,

$$\begin{aligned}(n + ra) \cdot b\mu &= n(b\mu) + ra(b\mu) \\ &= (nb)\mu + r(ab)\mu \\ &= (nb)\mu.\end{aligned}$$

Since $n \in \mathrm{Ann}(\mu)$, and since $\mathrm{Ann}(\mu)$ is an ideal as proven above, we have that nb is in $\mathrm{Ann}(\mu)$, so that $(nb)\mu$ vanishes. So, we have shown that there exists an ideal J which properly contains $\mathrm{Ann}(\mu)$, such that $j \cdot (b\mu)$ for each element $j \in J$:

$$\mathrm{Ann}(\mu) \subsetneq J \subseteq \mathrm{Ann}(b\mu),$$

thus contradicting the maximality of $\mathrm{Ann}(\mu)$

Exercise 1.184. Assume that the following diagram of group homomorphisms commutes and that the two rows are exact sequences.

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\alpha"] & B \arrow[r, "\phi"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "\psi'"] & B' \arrow[r, "\phi'"] & C'
\end{tikzcd}$$

Prove that if β is surjective and if γ and ψ' are injective then α is surjective.

Solution 1.185. Since the bottom row forms an exact sequence, we have that an element $b' \in B'$ is mapped to $e_{C'}$ iff it is in $\mathrm{im}\psi'$. Since the top row forms an exact sequence, we have that an element $b \in B$ is mapped to e_C iff it is in $\mathrm{im}\psi$.

Now, since γ is injective, an element $b \in B$ is mapped to $e_{C'}$ through $\gamma \circ \phi$ iff it is in $\mathrm{im}\psi$.

So, since the given diagram commutes, with $\gamma \circ \phi = \phi' \circ \beta$, we have that an element $b \in B$ is mapped to $e_{C'}$ iff:

(i) $b \in \mathrm{im}\psi$; and

(ii) $\beta(b) \in \mathrm{im}(\psi')$.

We claim that the image of $\beta \circ \psi$ is equal to the image of ψ'. Given in element $a \in A$, we have that:

$$\psi(a) \in \mathrm{im}\psi = \ker(\phi).$$

Again by injectivity of γ, we find that $\psi(a)$ must be mapped to $e_{C'}$. Given an element $a \in A$, we know that $\psi(a)$ is mapped to $e_{C'}$ iff $(\beta \circ \psi)(a) \in \mathrm{im}(\psi')$. So, this shows that $\mathrm{im}(\beta \circ \psi) \subseteq \mathrm{im}(\psi')$.

Now, by way of contradiction, suppose that there exists an element $x \in \mathrm{im}(\psi')$ outside of $\mathrm{im}(\beta \circ \psi)$. But by surjectivity of β, there exists an element $y \in B$ such that $\beta(y) = x$. But y would be mapped to $e_{C'}$ y would have to be in the image of ψ, so that $\beta(y) \in \mathrm{im}(\beta \circ \psi)$, contradicting our initial assumption that $\beta(y) \notin \mathrm{im}(\beta \circ \psi)$.

So, we have shown that $\mathrm{im}(\beta \circ \psi) = \mathrm{im}(\psi')$. So, for each element $a' \in A'$, we have that

$$\psi'(a') \in \mathrm{im}(\psi') = \mathrm{im}(\beta \circ \psi),$$

so that there exists a corresponding element $a \in A$ such that:

$$\psi(\beta(a)) = \psi'(a').$$

But since the given diagram commutes, we have that

$$\psi(\beta(a)) = \psi'(a') = \psi'(\alpha(a)).$$

By injectivity of ψ', we have that:

$$\psi'(a') = \psi'(\alpha(a)) \Longrightarrow a' = \alpha(a),$$

thus proving the surjectivity of α.

Exercise 1.186. Let I and J be ideals of R, a ring with identity $1 \neq 0$. Recall that IJ is the set of all finite sums of products xy where $x \in I$ and $y \in J$. Prove that $I + J$ is the smallest ideal containing both I and J.

Solution 1.187. The set $I + J$ consists of all expressions of the form $i + j$, where $i \in I$ and $j \in J$. Letting $i_1, i_2 \in I$ and $j_1, j_2 \in J$, we have that $i_1 + j_1$ and $i_2 + j_2$ are arbitrary elements in $I + J$. So, the sum

$$(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2)$$

must be in $I + J$, since I and J are both closed under addition. Similarly, given an element $r \in R$, together with an element i in I and an element $j \in J$, since

$$r \cdot (i + j) = r \cdot i + r \cdot j$$

and since I and J are closed under multiplication by elements in R, we have that $r \cdot i + r \cdot j$ must be in $I + J$. Since $I + J$ is closed with respect to the underlying additive binary operation of R, and since $I + J$ is closed under multiplication by elements in R, we thus have that $I + J$ is an ideal of R, as desired.

Since I and J are ideals, $0 \in I$ and $0 \in J$. So, each element of the form $0 + j$ is in $I + J$ for $j \in J$, and each element of the form $i + 0$ for $i \in I$ is in $I + J$, for $i \in I$. So, the ideal $I + J$ contains both I and J.

Now, let K be an arbitrary ideal of R which contains both I and J. Since K must be closed under addition, and since $I, J \subseteq K$, we thus find that each expression of the form $i + j$ must be in K, for $i \in I$ and $j \in J$. This shows that an arbitrary ideal $K \subseteq R$ which contains I and J must be such that $I + J \subseteq K$. This proves that $I + J$ is the smallest ideal of R containing both I and J.

Exercise 1.188. Prove that IJ is an ideal contained in $I \cap J$.

Solution 1.189. As indicated above, IJ is the set of all finite sums of expressions of the form xy where $x \in I$ and $y \in J$. Let

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

and

$$x_{n+1}y_{n+1} + x_{n+2}y_{n+2} + \cdots + x_my_m$$

be arbitrary elements in IJ. Then the sum

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n + x_{n+1}y_{n+1} + x_{n+2}y_{n+2} + \cdots + x_my_m$$

of these two elements is also a finite sum of expressions of the form xy for $x \in I$ and $y \in J$, thus proving that IJ is closed under addition. Letting $r \in R$, and letting

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n \in IJ$$

be as given above, we thus have that

$$r \cdot (x_1y_1 + x_2y_2 + \cdots + x_ny_n) = (r \cdot x_1)y_1 + (r \cdot x_2)y_2 + \cdots + (r \cdot x_n)y_n$$

and since I is closed under multiplication by elements in R, we have that the sum

$$(r \cdot x_1)y_1 + (r \cdot x_2)y_2 + \cdots + (r \cdot x_n)y_n$$

is also a finite sum of products of the form xy for $x \in I$ and $y \in J$. This shows that IJ is an ideal of R. Again letting

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n \in IJ$$

be as given above, so that

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n \in IJ$$

is an arbitrary element in IJ, each expression of the form x_1y_1 is in I since $x_i \in I$ for each index i, and since I is closed under multiplication by elements in R, and each expression of the form x_1y_1 is in J since $y_i \in J$ for each index i, and since J is an ideal. This shows that each element in IJ is contained in $I \cap J$.

Exercise 1.190. Give an example where $IJ \neq I \cap J$.

Solution 1.191. Let $R = \mathbb{Z}/8\mathbb{Z}$. Observe that R is a ring with unity $1 \neq 0$. Let $I \subseteq R$ denote the principal ideal $\{0, 2, 4, 6\}$ generated by $2 \in R$, and let J denote the ideal $\{0, 4\}$. We thus find that $I \cap J = \{0, 4\}$. However, as indicated in the following multiplication table, each product of the form ij for $i \in I$ and $j \in J$ vanishes:

$\cdot_8$	0	2	4	6
0	0	0	0	0
4	0	0	0	0

Since each expression of the form ij vanishes for $i \in I$ and $j \in J$, we thus have that IJ must be equal to the singelton set $\{0\}$. We thus have that $IJ \subsetneq I \cap J$, as desired.

Exercise 1.192. Prove that if R is commutative and if $I + J = R$, then $IJ = I \cap J$.

Solution 1.193. Suppose that R is commutative, and suppose that $I + J = R$. We have previously shown that IJ is an ideal satisfying the inclusion whereby $IJ \subseteq I \cap J$. So, it remains to prove the reverse inclusion. So, suppose that x is an element in $I \cap J \subseteq R = I + J$. Since R is untial, we may rewrite the element x in the manner indicated below:

$$x = x \cdot 1.$$

Since $1 \in R = I + J$, we thus have that the unit 1 in R may be written as $1 = i + j$ where $i \in I$ and $j \in J$. We thus have that:

$$\begin{aligned} x &= x \cdot 1 \\ &= x \cdot (i + j) \\ &= x \cdot i + x \cdot j. \end{aligned}$$

Since I is an ideal, we have that the expression $x \cdot i$ must be in I, since $x \in R$ and $i \in I$. Since J is closed under multiplication by elements of R, we have that $x \cdot j \in J$. Therefore,

$$x \cdot i + x \cdot j \in I + J.$$

So, we have shoiwn that each element $x \in I \cap J$ must be in IJ in the case whereby $I + J$.

Exercise 1.194. Let A and B be ideals in R, a commutative ring with $1 \neq 0$. For $r \in R$, prove that $\phi(r) = (r + A, r + B)$ is a ring homomorphism from R to $R/A \times R/B$ and compute $\ker \phi$.

Solution 1.195. Let A, B, R, etc., be as given above. Let r_1 and r_2 be arbitrary elements in the domain R of ϕ. We thus have that:

$$\begin{aligned} \phi(r_1) + \phi(r_2) &= (r_1 + A, r_1 + B) + (r_2 + A, r_2 + B) \\ &= ((r_1 + A) + (r_2 + A), (r_1 + B) + (r_2 + B)) \\ &= (r_1 + r_2 + A, r_1 + r_2 + B) \\ &= \phi(r_1 + r_2). \end{aligned}$$

Similarly, we have that:

$$\begin{aligned} \phi(r_1) \cdot \phi(r_2) &= (r_1 + A, r_1 + B) \cdot (r_2 + A, r_2 + B) \\ &= ((r_1 + A) \cdot (r_2 + A), (r_1 + B) \cdot (r_2 + B)) \\ &= (r_1 \cdot r_2 + A, r_1 \cdot r_2 + B) \\ &= \phi(r_1 \cdot r_2). \end{aligned}$$

Since ϕ preserves the multiplicative operation of R, as well as the additive operation of R, we have that ϕ is a ring homomorphism, as desired. Now evaluate the kernel of $\phi \colon R \to R/A \times R/B$ in the manner suggested below:

$$\begin{aligned} \ker(\phi) &= \{r \in R \ : \ \phi(r) = (0 + A, 0 + B)\} \\ &= \{r \in R \ : \ (r + A, r + B) = (0 + A, 0 + B)\} \\ &= \{r \in R \ : \ r + A = 0 + A, r + B = 0 + B\} \\ &= \{r \in R \ : \ r \in A, r \in B\} \\ &= A \cap B. \end{aligned}$$

Exercise 1.196. Let $\mathbb{F}$ be a field. Show that the subring $\mathbb{F}[x, x^2y, x^3y^2, \ldots, x^ny^{n-1}, \ldots]$ of the ring $\mathbb{F}[x, y]$ contains an ideal which is not finitely generated.

Solution 1.197. Consider the ideal

$$I = \langle x, x^2y, x^3y^2, \ldots, x^ny^{n-1}, \ldots\rangle \subseteq \mathbb{F}[x, x^2y, x^3y^2, \ldots, x^ny^{n-1}, \ldots].$$

This ideal consists precisely of polynomials in

$$R = \mathbb{F}[x, x^2y, x^3y^2, \ldots, x^ny^{n-1}, \ldots]$$

with a constant term equal to 0. By way of contradiction, suppose that I is finitely generated, writing

$$I = \langle p_1, p_2, \ldots, p_m\rangle,$$

where $m \in \mathbb{N}$, and p_i is in R for each index i. The non-constant terms of each polynomial in R must be of the form x^jy^{j-1}. Now, let $k \in \mathbb{N}$ be the least natural number such that the monomial x^ky^{k-1} is greater than all of the terms among the polynomials in $\{p_1, p_2, \ldots, p_m\}$. There must exist a monomial of this form, since there are only a finite number of terms for each polynomial in $\{p_1, p_2, \ldots, p_m\}$, and since there are only a finite number of elements in $\{p_1, p_2, \ldots, p_m\}$. But since x^ky^{k-1} is a polynomial in R with a constant term equal to 0, we have that:

$$x^ky^{k-1} = p_1q_1 + p_2q_2 + \cdots + p_mq_m$$

where $q_1, q_2, \ldots, q_m \in R$. But given monomials $x^{\ell_1}y^{\ell_1-1}$ and $x^{\ell_2}y^{\ell_2-1}$ such that $\ell_1 < k$, we have that:

$$x^{\ell_1}y^{\ell_1-1}x^{\ell_2}y^{\ell_2-1} = x^{\ell_1+\ell_2}y^{\ell_1+\ell_2-2}.$$

So, each term in the expansion of

$$p_1q_1 + p_2q_2 + \cdots + p_mq_m$$

is either of the form $x^\ell y^{\ell-1}$ where $\ell < k$, or is of the form

$$x^\ell y^{\ell-2},$$

which shows that it cannot be the case that

$$x^ky^{k-1} = p_1q_1 + p_2q_2 + \cdots + p_mq_m.$$

thus showing that I cannot be finitely generated.

Exercise 1.198. Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]/\langle x_1x_2, x_3x_4, x_5x_6, \ldots\rangle$ contains infinitely many minimal prime ideals.

Solution 1.199. Let $R = \mathbb{Z}[x_1, x_2, x_3, \ldots]$, and let $K = \langle x_1x_2, x_3x_4, x_5x_6, \ldots\rangle$. Our solution is based on a solution given in the below link[14]. Let Y denote the set of all choice functions on $\{\{2k+1, 2k+2\} | k \in \mathbb{N}\}$. For $\lambda \in Y$, let $I_\lambda = \langle \lambda_0, \lambda_1, \ldots\rangle$. Observe that $K \subseteq I_\lambda$ for each index λ.

By the third isomorphism theorem for rings, we have that

$$(R/K)/(I_\lambda/K) \cong R/I_\lambda.$$

[14] See `https://crazyproject.wordpress.com/2010/11/26/exhibit-a-ring-with-infinitely-many-minimal-prime-ideals/`.

Similarly, we have that $R/I_\lambda \cong R$. Since R is an integral domain, I_λ/K must be a prime ideal of R/K.

Suppose that $J/K \subseteq I_\lambda/K$ is a prime ideal. Let $(i, i+1)$ be a pair such that i is an odd natural number. We may assume without loss of generality that $x_i \in I_\lambda$. Since $x_i x_{i+1} \in K \subseteq J$. Since J is prime and $x_{i+1} \notin J$ as $x_{i+1} \notin I_\lambda$, we have that $x_i \in J$. This shows that $J = I_\lambda$.

Observe that R/K is not an integral domain since $(x_1 + K)(x_2 + K) = 0$, so that the trivial ideal is not prime. So, each ideal of the form I_λ is a prime ideal which is minimal with respect to inclusion.

Exercise 1.200. Suppose that I is a monomial ideal generated by monomials $m_1, m_2, \ldots, m_k$. Prove that the polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is in I if and only if every monomial term f_i of f is a multiple of one of the m_j.

Solution 1.201. ($\Longrightarrow$) Letting

$$I = \langle m_1, m_2, \ldots, m_k \rangle,$$

where each expression of the form m_i is a monomial, suppose that the polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ is in I. We thus have that

$$f = m_1 p_1 + m_2 p_2 + \cdots + m_k p_k,$$

where p_i is a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ for each index i. Expanding each polynomial of the form p_i in terms of its monomial terms, we thus have that each monomial term in f must be a multiple of m_j for some index j.

($\Longleftarrow$) Conversely, suppose that every monomial term f_i of f is a multiple of some expression of the form m_j. Writing

$$f = f_1 + f_2 + \cdots + f_r,$$

we thus have that

$$f = m_1 q_1 + m_2 q_2 + \cdots + m_r q_r,$$

where q_i is a polynomial for each index i. This shows that f must be in I.

Exercise 1.202. Fix a monomial ordering on $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$ and suppose that $\{g_1, g_2, \ldots, g_m\}$ is a Gröbner basis for the ideal

$$I = \langle m_1, m_2, \ldots, m_k \rangle$$

in R. Prove that $h \in \mathrm{LT}(I)$ if and only if h is a sum of monomial terms each of which is divisible by some $\mathrm{LT}(g_i)$.

Solution 1.203. ($\Longrightarrow$) Suppose that $h \in \mathrm{LT}(I)$. Since $\{g_1, g_2, \ldots, g_m\}$ is a Gröbner basis of I, we have that

$$I = \langle g_1, g_2, \ldots, g_m \rangle$$

and

$$\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_m) \rangle.$$

Since $h \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_m) \rangle$, we have that

$$h = \mathrm{LT}(g_1) p_1 + \mathrm{LT}(g_2) p_2 + \cdots + \mathrm{LT}(g_m) p_m$$

where each expression of the form p_i is a polynomial in R. Expanding each such polynomial in terms of monomials, we thus have that h is a sum of monomial terms each of which is divisible by some expression of the form $\mathrm{LT}(g_i)$.

($\Longleftarrow$) Conversely, suppose that h is a sum of monomial terms each of which is divisible by some expression of the form $\mathrm{LT}(g_i)$, writing

$$h = \mathrm{LT}(g_1)\ell_1 + \mathrm{LT}(g_2)\ell_2 + \cdots + \mathrm{LT}(g_k)\ell_k,$$

where ℓ_i is a monomial in R for each index i. But then

$$h \in \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_m)\rangle$$

and we thus have that $h \in \mathrm{LT}(I)$, as desired.

Exercise 1.204. Show that $\{x - y^3, y^5 - y^6\}$ is a Gröbner basis for the ideal $I = \langle x - y^3, -x^2 + xy^2\rangle$ with respect to lexicographic ordering where $x > y$ in the ring $\mathbb{F}[x, y]$.

Solution 1.205. Let J denote the ideal generated by $\{x - y^3, y^5 - y^6\}$ in $\mathbb{F}[x, y]$. We claim that $I = J$. In the ideal

$$I = \langle x - y^3, -x^2 + xy^2\rangle,$$

we have that x is equivalent to y^3 modulo I. That is, $-x^2 + xy^2$ is equivalent to $-y^6 + y^5$ modulo I, which shows that:

$$\langle x - y^3, -x^2 + xy^2\rangle = \langle x - y^3, -y^6 + y^5\rangle,$$

as desired. Now observe that:

$$\{\mathrm{LT}(x - y^3), \mathrm{LT}(y^5 - y^6)\} = \{x, y^5\}.$$

Now consider the ideal $\mathrm{LT}(I)$. Recall that x is equivalent to y^3 in $I = \langle x - y^3, -x^2 + xy^2\rangle$. Suppose that a leading term in I contains x as a factor. Then this leading term must be in $\langle x, y^5\rangle$. Now suppose that it is not the case that a leading term in I contains x as a factor. Then since x is equivalent to y^3 in I, this leading term must be of the form $y^{\geq 5}$, which shows that this leading term must be in $\langle x, y^5\rangle$. This shows that $\mathrm{LT}(I) \subseteq \langle x, y^5\rangle$. Similarly, since $x = \mathrm{LT}(x - y^3)$ and $y^6 \equiv \mathrm{LT}(-x^2 + xy^2)$, we have that the reverse inclusion holds.

Exercise 1.206. Prove that the rings $\mathbb{F}[x, y]/\langle y^2 - x\rangle$ and $\mathbb{F}[x, y]/\langle y^2 - x^2\rangle$ are not isomorphic for any field $\mathbb{F}$.

Solution 1.207. Let R denote the polynomial ring $\mathbb{F}[x, y]$. The expression polynomial $y^2 - x$ is irreducible, but $y^2 - x^2 = (y - x)(y + x)$. The ideal $\langle y^2 - x\rangle$ consists of expressions of the form $(y^2 - x)p$ But since $y^2 - x$ is irreducible, if $ab = (y^2 - x)p$ for some polynomials a and b, then either a or b must be a multiple of $y^2 - x$. This proves that $\langle y^2 - x\rangle$ is a prime ideal in $\mathbb{F}[x, y]$, so that $\mathbb{F}[x, y]/\langle y^2 - x\rangle$ is an integral domain. However, if

$$ab = (y^2 - x^2)p = (y - x)(y + x)p,$$

then it is possible that $a = y - x \notin \langle y^2 - x^2\rangle$ and that $b = (y + x)p \notin \langle y^2 - x^2\rangle$. This shows that $\langle y^2 - x^2\rangle$ is not a prime ideal in $\mathbb{F}[x, y]$. Therefore, $\mathbb{F}[x, y]/\langle y^2 - x^2\rangle$ is not an integral domain, and therefore cannot be isomorphic to $\mathbb{F}[x, y]/\langle y^2 - x\rangle$, since $\mathbb{F}[x, y]/\langle y^2 - x\rangle$ is an integral domain.

2 Former comprehensive exam questions

2.1 University of Toronto comprehensive exam questions

Exercise 2.1. (Toronto, 2008) Show that every group of order 200 has a nontrivial normal subgroup.

Solution 2.2. Begin by writing 200 as a product of primes:

$$200 = 2^3 \cdot 5^2.$$

Now, let G be a group of order 200. Let n_5 denote the number of Sylow 5-subgroups of G. The divisors of 200 which are positive are precisely the elements in the following set:

$$\{1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200\}.$$

Now, consider the tuple

$$(1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200)$$

consisting of the positive divisors of 200 ordered canonically, and reduce each entry in the above tuple modulo 5:

$$(1, 2, 4, 0, 3, 0, 0, 0, 0, 0, 0, 0)\,.$$

Since $n_5 \equiv 1 (\text{mod } 5)$ and $n_5 | 200$, we have that $n_5 = 1$. But since Sylow 5-subgroups of G are all conjugate to each other, we thus have that the unique Sylow 5-subgroup H_5 of G is necessarily normal in G. By definition of a Sylow p-subgroup, H_5 is a maximal 5-subgroup, so H_5 must be nontrivial.

Exercise 2.3. (Toronto, 2008) Make a list (up to isomorphism) of all abelian groups of order 200.

Solution 2.4. By the Fundamental Theorem of Finitely-Generated Abelian Groups, we have that a finitely-generated abelian group of order 200 must be of the form

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \cdots \times C_{p_m^{n_m}}$$

where p_i is a prime for all indices i, with $m \in \mathbb{N}$, and $n_i \in \mathbb{N}$ for all indices i, with:

$$p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m} = 200.$$

So, the following list consists prev--isely of the abelian groups of order 200, up to isomorphism, since $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$ if a and b are relatively prime.

$\mathbb{Z}_{200}$,
$\mathbb{Z}_2 \times \mathbb{Z}_{100}$,
$\mathbb{Z}_4 \times \mathbb{Z}_{50}$,
$\mathbb{Z}_5 \times \mathbb{Z}_{40}$,
$\mathbb{Z}_{10} \times \mathbb{Z}_{20}$,
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{50}$,
$\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$.

Exercise 2.5. (Toronto, 2008) Find all ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 26)$.

Solution 2.6. Consider the ideal of $\mathbb{Z}[x]$ generated by $\{2, x^3 + 26\} \subseteq \mathbb{Z}[x]$:

$$I = (2, x^3 + 26) = 2\mathbb{Z}[x] + (x^3 + 26)\mathbb{Z}[x].$$

Define:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ q(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0. \end{aligned}$$

So, an element in I is of the form:

$$\begin{aligned} &(2a_0 + 26b_0) + (2a_1 + 26b_1)x + (2a_2 + 26b_2)x^2 + \\ &(2a_3 + 26b_3 + b_0)x^3 + (2a_4 + 26B_4 + b_1)X^4 + \text{(higher powers)}. \end{aligned}$$

Observe that the constant term of an element in I must be even. So $0 + I \neq 1 + I$. Similarly, the first 3 coefficients of an element in I must be even. This shows that the following cosets are pairwise unequal:

$$\{0 + I, 1 + I, x + I, x + 1 + I, x^2 + I, x^2 + 1 + I, x^2 + x + I, x^2 + x + 1 + I\}.$$

Since higher coefficients may be of the form $2a_3 + 26b_3 + b_0$, $2a_4 + 26b_4 + b_1$, etc., it is easily seen that $\mathbb{Z}[x]/(2, x^3 + 26)$ is equal to the above set of 8 cosets. So $\mathbb{Z}[x]/I$ is a ring of order 8. It is evident that the underlying additive abelian group of this ring is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

To compute the ideals of the quotient ring $\mathbb{Z}[x]/I$, begin by considering the principal ideals $(x + I)$, $(x + 1 + I)$, etc.

$$(x + I) = \{0 + I, x + I, x^2 + x + I, x^2 + I\} = (x^2 + I) = (x^2 + x + I).$$

Since $(x + I)$ is of order 4 and $\mathbb{Z}[x]/I$ is of order 8, $(x + I)$ is maximal. It is easily seen that $(x + 1 + I) = (x^2 + 1 + I) = (x^2 + x + 1 + I) = \mathbb{Z}[x]/I$. Also,

$$(x^2 + x + I) = \{0 + I, x^2 + x + I, x^2 + I, x + I\}.$$

Since the above ideal is of order 4 and $\mathbb{Z}[x]/I$ is of order 8, $(x^2 + x + I)$ is maximal. So, the above evaluations show that the ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 26)$ are:

$\{0 + I\}$
$\mathbb{Z}[x]/(2, x^3 + 26)$,
$\{0 + I, x + I, x^2 + x + I, x^2 + I\}$,
$\{0 + I, x^2 + x + I, x^2 + I, x + I\}$.

Exercise 2.7. (Toronto, 2007) Let G be a group. State the three Sylow theorems. What is a composition series of G? To what extent is it unique?

Solution 2.8. First Sylow Theorem: Sylow p-subgroups always exist for a prime p dividing the order of G.

Second Sylow Theorem: Sylow p-subgroups are all conjugates of each other.

Third Sylow Theorem: Letting n_p denote the number of Sylow p-subgroups of G, for a prime p dividing the order of G, $n_p \big| |G|$ and $n_p \equiv 1 (\text{mod } p)$[15].

[15] See http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/100416notes.pdf.

A composition series of G is a subnormal series

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

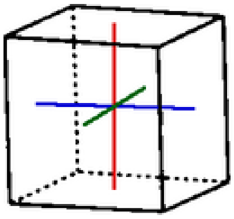
of G such that $H_i \lhd H_{i+1}$ for all indices i, and H_{i+1}/H_i is simple for all indices i[16]. By the Jordan-Hölder theorem, two composition series of the same group G must be isomorphic, i.e., they must be the same up to a rearrangement of the composition quotients, up to isomorphism.

Exercise 2.9. (Toronto, 2007) Let R be an integral domain. Define the terms prime element and irreducible element. What is the connection between prime elements and irreducible elements in R?

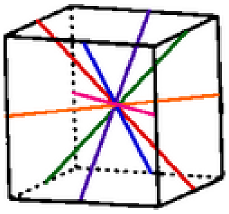
Solution 2.10. (See Alaca and Williams' "Introductory Algebraic Number Theory", for example.) A nonzero, nonunit element a of an integral domina R is called an irreducible, or said to be irreducible, if $a = bc$, where $b, c \in R$, implies that either b or c is a unit. A nonzero, nonunit element p of an integral domain R is called a prime if $p \Big| ab$, where $a, b \in R$, implies that $p|a$ or $p|b$. We claim that in an integral domain R, a prime element must necessarily be irreducible. Letting $p \in R$ be a prime, suppose that $p = ab$, with $a, b \in R$. By definition of an integral domain, R must have a unity. We may thus write $ab = p \cdot 1$. Since p is a prime, we have that $p|a$ or $p|b$, that is, $a/p \in R$ or $b/p \in R$. Since $a = a/p \cdot b$ or $1 = a \cdot b/p$, either b is a unit or a is a unit of R.

Exercise 2.11. (Toronto, 2006) What is the order of the group of rotations of the cube?

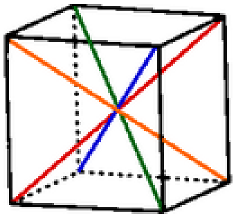
Solution 2.12. The following solution is based on the linked MATH 4160 course website given below[17]. There are 24 rotations of the cube. The identity isometry is trivially a rotational isometry. There are also 9 rotations of the cube about the 3 axes illustrated below.



There are 6 rotational isometries of the cube by 180° around the axes shown in the following image.



There are rotations by 120° and 240° around the 4 axes shown in the image below.



[16] See `http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/092716notes.pdf`.

[17] See `http://garsia.math.yorku.ca/~zabrocki/math4160w03/cubesyms/`.

We thus have that the group of rotations of the cube is of order 24.

Exercise 2.13. (Toronto, 2006) The dihedral group D_{30} is the group of rotations and reflections of the regular 15-gon: $D_{30} = \langle \sigma, \rho \mid \sigma^2 = 1 = \rho^{15}, \sigma\rho = \rho^{-1}\sigma \rangle$. How many Sylow subgroups of each possible order are there in D_{30}? Are any of them normal?

Solution 2.14. For a prime p, a Sylow p-subgroup of a given group is a maximal p-subgroup. The dihedral group D_{30} is of order 30:

$$|D_{30}| = 30 = 2 \cdot 3 \cdot 5.$$

For $p \in \{2, 3, 5\}$, let n_p denote the number of Sylow p-subgroups of D_{30}. The following tuple consists of the positive divisors of $|D_{30}| = 30$:

$$(1, 2, 3, 5, 6, 10, 15, 30).$$

Reduce the above tuple modulo p, for $p \in \{2, 3, 5\}$:

$$\begin{gathered}(1, 0, 1, 1, 0, 0, 1, 0),\\ (1, 2, 0, 2, 0, 1, 0, 0),\\ (1, 2, 3, 0, 1, 0, 0, 0).\end{gathered}$$

By Sylow's First Theorem, we have that $n_2 \geq 1$, $n_3 \geq 1$, and $n_5 \geq 1$. We begin by considering the value of n_5. To find the value of n_5, we proceed to consider the subgroup of D_{30} consisting of the rotational isometries in D_{30}:

$$R = \{1, \rho, \rho^2, \ldots, \rho^{14}\}.$$

We remark that R is a cyclic subgroup, and that $R \triangleleft D_{30}$, since subgroups of index 2 must be normal. Consider the following subgroup of R:

$$\{1, \rho^3, \rho^6, \rho^9, \rho^{12}\} \triangleleft R.$$

A group of order 5 must be cyclic. So, a Sylow 5-subgroup of D_{30} must be a cyclic subgroup of order 5. What elements in D_{30} are of order 5? The elements in the dihedral group D_{30} are indicated below:

$$D_{30} = \{1, \rho, \rho^2, \ldots, \rho^{14}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{14}\}.$$

By the Fundamental Theorem of Cyclic Groups, the only elements in $\{1, \rho, \rho^2, \ldots, \rho^{14}\}$ of order 3 are ρ^3, ρ^6, ρ^9, and ρ^{12}. Now consider the orders of elements in $\{\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{14}\}$:

$$\begin{aligned}\sigma^2 &= 1\\ (\sigma\rho) \cdot (\sigma\rho) &= (\sigma\rho) \cdot (\rho^{-1}\sigma) = 1\\ (\sigma\rho^2) \cdot (\sigma\rho^2) &= \sigma\rho\rho\sigma\rho\rho\\ &= \sigma\rho\sigma\rho = 1.\end{aligned}$$

Continuing in the manner suggested above, we find that the only elements in D_{30} of order 5 are: ρ^3, ρ^6, ρ^9, and ρ^{12}. So, the only subgroup of D_{30} of order 5 is $\{1, \rho^3, \rho^6, \rho^9, \rho^{12}\}$. Now, consider the subgroups of D_{30} of order 3. Of course, a group of order 3 must be cyclic. So, to determine the subgroups of D_{30} of order 3, it remains to consider the elements in D_{30} of order 3. We have shown above that the elements in $\{\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{14}\}$ are all of order 2. So it remains to consider the elements of order 3 in the rotational cyclic subgroup $R = \{1, \rho, \rho^2, \ldots, \rho^{14}\} \triangleleft D_{30}$. By the Fundamental Theorem of Cyclic

Groups, we have that the only elements of order 3 are the non-identity elements in the following cyclic subgroup:

$$\{1, \rho^5, \rho^{10}\}.$$

We thus find that there is a unique subgroups of D_{30} of order 3, namely, the cyclic subgroup $\{1, \rho^5, \rho^{10}\}$, with $n_3 = 1$. So, it remains to evaluate n_2. By Sylow's Third Theorem, since $n_2 \equiv 1 \pmod 2$ and $n_2 \big| |G|$, we may deduce that:

$$n_2 \in \{1, 3, 5, 15\}.$$

Now, we have previously shown that each element in

$$\{\sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{14}\}$$

is of order 2. Therefore, there are at least 15 subgroups of order 2. Using Sylow theory, we thus find that $n_2 = 15$. So, we have thus far shown that:

$$\begin{aligned} n_2 &= 15, \\ n_3 &= 1, \\ n_5 &= 1. \end{aligned}$$

By Sylow's second theorem, for fixed p, Sylow p-subgroups are all conjugates of one another. So, since $n_3 = 1$, the unique Sylow 3-subgroup of D_{30} is normal, and since $n_5 = 1$, the unique Sylow 5-subgroup of D_{30} is normal. Since $n_2 = 15$, Sylow 2-subgroups of D_{30} are not normal.

Exercise 2.15. (Toronto, 2005) Show that there are no simple groups of order 70.

Solution 2.16. Let G be a group of order $70 = 2 \cdot 5 \cdot 7$. The following tuple consists of the positive divisors of 70, ordered canonically:

$$(1, 2, 5, 7, 10, 14, 35, 70).$$

Now, reduce the entries in the above tuple modulo 5:

$$(1, 2, 0, 2, 0, 4, 0, 0).$$

By Sylow's Third Theorem, we have that the number n_5 of Sylow 5-subgroups of G must divide $|G|$, and must be such that $n_5 \equiv 1 \pmod 5$. As indicated above, we have that n_5 must be equal to 1. But by Sylow's Second Theorem, all Sylow 5-subgroups must be conjugates od each other. But since $n_5 = 1$, we thus havce that the unique Sylow 5-subgroup of G must be a normal subgroup of G. But since this normal subgroup must be of prime power order, and since $|G| = 2 \cdot 5 \cdot 7$, we have that this subgroup is normal, proper, and nontrivial.

Exercise 2.17. (Toronto, 2005) Prove or disprove: every finite p-group is nilpotent.

Solution 2.18. Recall that every finite p-group must be of prime power order. Also recall that groups of prime power order must have nontrivial centers, as may be verified using the class equation with respect to conjugation. So, let G be a finite p-group. We thus have that G must be nontrivial, since it must be of prime power order. Also, $Z(G)$ must be nontrivial. We thus arrive at the following series:

$$Z_0(G) \triangleleft Z_1(G).$$

Now, the quotient group $G/Z(G)$ also must be of prime power order. Therefore, $Z(G/Z(G))$ also must be nontrivial in the quotient group $G/Z(G)$:

$$Z(G)/Z(G) \lhd Z(G/Z(G)) \unlhd G/Z(G).$$

We thus arrive at a series of the form

$$Z_0(G) \lhd Z_1(G) \lhd Z_2(G).$$

Continuing in this manner, we have that the series

$$Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd Z_3(G) \lhd \cdots$$

is always strictly increasing provided that we are dealing with proper subgroups of prime power order. So the above series must be of the form

$$Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd Z_3(G) \lhd \cdots \lhd Z_{n-1}(G) \lhd G$$

for some $n \in \mathbb{N}$.

Exercise 2.19. (Toronto, 2005) How many Sylow subgroups of each possible order are there in the symmetric group S_4? Are any of them normal?

Solution 2.20. We begin by writing the order of S_4 as a product of prime powers:

$$|S_4| = 24 = 8 \cdot 3 = 2^3 \cdot 3.$$

The following tuple consists of the positive divisors of $|S_4|$, ordered canonically:

$$(1, 2, 3, 4, 6, 8, 12, 24).$$

Reduce the entries in the above tuple modulo 2:

$$(1, 0, 1, 0, 0, 0, 0, 0).$$

Now, reduce the entries in the tuple $(1, 2, 3, 4, 6, 8, 12, 24)$ modulo 3:

$$(1, 2, 0, 1, 0, 2, 0, 0).$$

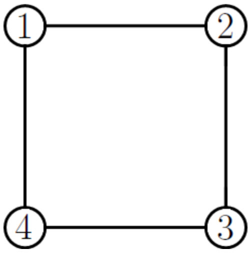
Let n_p denote the number of Sylow p-subgroups of S_4 for $p \in \{2, 3\}$. By definition of a Sylow p-subgroup, a Sylow p-subgroup is a maximal p-subgroup. So, a maximal 3-subgroup of S_4 must be a subgroup of S_4 of order 3. By Sylow's First Theorem, we have that $n_3 \geq 1$. By Sylow's Third Theorem, we have that $n_3 \equiv 1 (\text{mod } 3)$ and $n_3 \big| |S_4|$. From our above reduction of the entries in $(1, 2, 3, 4, 6, 8, 12, 24)$ modulo 3, we find that n_3 is either equal to 1 or 4. So, to evaluate n_3, it remains to consider the elements in S_4 of order 3. Observe that:

$$\langle (234) \rangle = \{\text{id}, (234), (243)\}$$
$$\langle (123) \rangle = \{\text{id}, (123), (132)\}.$$

So, we have shown that there are at least two order-3 subgroups of S_4. But since $n_3 \in \{1, 4\}$, we may thus deduce that $n_3 = 4$.

Now, by Sylow's Second Theorem, we have that all Sylow 3-subgroups of S_4 must be conjugates of each other. But since $n_3 = 4 \neq 1$, we have that Sylow 3-subgroups of S_4 are not normal subgroups.

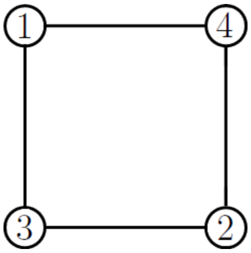
Now consider the number of Sylow 2-subgroups of S_4. From our above computations, by Sylow's Third Theorem, we find that $n_2 \in \{1, 3\}$. We proceed to construct an order-8 subgroup of S_4. By labeling the corners of a square as suggested below, we find that there is a subgroup of S_4 which is isomorphic to the dihedral group of order 8.



We thus obtain the following permutation subgroup which is isomorphic to D_4.

$$\{\text{id}, (1234), (13)(24), (1432), (12)(34), (14)(23), (24), (13)\}.$$

Now consider the following labeling.



We thus obtain a subgroup of S_4 which is isomorphic to D_4 and which contains to the permutation (1423). This shows that there are at least two different subgroups of S_4 which are isomorphic to the dihedral group of order 8. Using Sylow theory, we have shown that $n_2 \in \{1, 3\}$. But since $n_2 \geq 2$, we have that $n_2 = 3$, so by Sylow's Second Theorem, we have that an arbitrary Sylow 2-subgroup of S_4 is not normal.

In summary, we have shown that there are 4 Sylow 3-subgroups of S_4, and 3 Sylow 2-subgroups of S_4, and that Sylow subgroups of S_4 cannot be normal subgroups.

Exercise 2.21. (Toronto, 2004) What is the smallest positive integer n so that the symmetric group S_n contains an element of order 18?

Solution 2.22. By Ruffini's theorem[18], the order of a permutation written in disjoint cycle form is equal to the least common multiple of the lengths of its cyclies. So, it remains to find $a_1, a_2, \ldots, a_m \in \mathbb{N}$ such that $\text{lcm}(a_1, a_2, \ldots, a_m) = 18$, and $a_1 + a_2 + \cdots + a_m$ is minimal. Writing $18 = 2 \cdot 3^2$ as a product of prime powers, we proceed to consider possible expressions of the form $\text{lcm}(a_1, a_2, \ldots, a_m) = 18$:

$$\text{lcm}(2, 9) = 18,$$

[18] See Gallian's "Contemporary Abstract Algebra". Ruffini's theorem was formulated in the following manner in this textbook: "The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles."

$$\operatorname{lcm}(6,9) = 18,$$
$$\operatorname{lcm}(18,1) = 18.$$

So, the least $a_1, a_2, \dots, a_m \in \mathbb{N}$ such that $\operatorname{lcm}(a_1, a_2, \dots, a_n) = 18$ is such that $a_1 = 2$ and $a_2 = 9$. Observe that the element $(1,2)(3,4,5,6,7,8,9,10,11)$ is of order 18 in S_{11}. So, the smallest positive integer n such that S_n contains an element of order 18 is $n = 11$.

Exercise 2.23. (Toronto, 2004) Let $\sigma \in S_{10}$ be the permutation $\sigma = (123)(456)$. What is the order of $Z_{S_{10}}(\sigma)$, its centralizer in S_{10}?

Solution 2.24. Recall that given a group G and a subset A of G, the centralizer $C_G(A)$ of A in G is the following set[19]:

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

So, the centralizer $Z_{S_{10}}(\sigma)$ of σ in S_{10} is the following set:

$$Z_{S_{10}}(\sigma) = \{\rho \in S_{10} \mid \rho\sigma = \sigma\rho\}.$$

For $\rho \in S_{10}$, we have that $\rho\sigma = \sigma\rho$ iff the following holds:

$$\begin{aligned}
\rho_2 &= \sigma(\rho_1)\\
\rho_3 &= \sigma(\rho_2)\\
\rho_1 &= \sigma(\rho_3)\\
\rho_5 &= \sigma(\rho_4)\\
\rho_6 &= \sigma(\rho_5)\\
\rho_4 &= \sigma(\rho_6)\\
\rho_7 &= \sigma(\rho_7)\\
\rho_8 &= \sigma(\rho_8)\\
\rho_9 &= \sigma(\rho_9)\\
\rho_{10} &= \sigma(\rho_{10}).
\end{aligned}$$

Since $\sigma_i = i$ iff $i \in \{7,8,9,10\}$, and since $\sigma_i = i$ iff $i \in \{\rho_7, \rho_8, \rho_9, \rho_{10}\}$, there are 4! choices for ρ_7, ρ_8, ρ_9, and ρ_{10}. Each remaining element ρ_i in $\{\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6\}$ is such that ρ_i, $\sigma(\rho_i)$, and $\sigma^2(\rho_i)$ are all distinct, with $\sigma^3(\rho_i) = \rho_i$. So, there are 6 choices for ρ_1. Given each choice for ρ_1, ρ_2 and ρ_3 are "automatically" determined. Then, there are 3 remaining choices for ρ_4. Given each such choice for ρ_4, ρ_5 and ρ_6 are automatically given. So, the order of $Z_{S_{10}}$ is $4! \cdot 6 \cdot 3$.

There is a general formula for the order of the centralizer of a permutation[20] Let n_1, n_2, …, n_k be the distinct lengths of the cycles of σ, and suppose that there are m_i cycles of length n_i. Then the centralizer of σ is of order $\prod_{i=1}^{k} n_i^{m_i} m_i!$. This agrees with our evaluation for the above exercise.

Exercise 2.25. (Toronto, 2003) Let $D_{12} = \langle r, s \mid r^6 = s^2 = 1, rs = sr^{-1}\rangle$ be the dihedral group of order 12. Determine whether D_{12} is a nilpotent group.

[19] See `http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/092216notes.pdf`.

[20] See `http://math.stackexchange.com/questions/85817/`.

Solution 2.26. It is known that the center of a diehdral group of the form D_{2n} consists of the identity isometry and the half-turn isometry[21]. Therefore,

$$Z(D_{12}) = \left\{1, r^3\right\}.$$

Writing $G = D_{12}$, we thus have that $Z_0 = \{1\}$, and $Z_1 = \{1, r^3\}$.

Now, consider the quotient group $D_{12}/Z(D_{12})$. Since $Z(D_{12}) = \{1, r^3\}$, we have that $D_{12}/Z(D_{12})$ is a group of order 6. This quotient group consists of the following cosets:

$$\begin{aligned}
&1\{1, r^3\} = \{1, r^3\},\\
&r\{1, r^3\} = \{r, r^4\},\\
&r^2\{1, r^3\} = \{r^2, r^5\},\\
&s\{1, r^3\} = \{s, sr^3\},\\
&sr\{1, r^3\} = \{sr, sr^4\},\\
&sr^2\{1, r^3\} = \{sr^2, sr^5\}.
\end{aligned}$$

Now, consider the groups of order 6, up to isomorphism. By the Fundamental Theorem of Finitely-Generated Abelian Groups, the only abelian group of order 6 is $\mathbb{Z}/6\mathbb{Z} \cong C_6$, up to isomorphism. The only non-abelian group of order 6 is $D_3 \cong S_3$, up to isomorphism. It is clear that $D_{12}/Z(D_{12}) \cong D_3$, since the quotient group $D_{12}/Z(D_{12})$ cannot be cyclic, since

$$s\{1, r^3\} \cdot s\{1, r^3\} = s^2\{1, r^3\} = 1\{1, r^3\}.$$

It is known that the center of a dihedral group of the form D_m for an odd natural number m is trivial. So, we have that $Z(D_{12}/Z(D_{12}))$ is trivial. We thus have that

$$Z(D_{12}/Z(D_{12})) = \{\{1, r^3\}\}.$$

Therefore,

$$\bigcup Z(D_{12}/Z(D_{12})) = \{1, r^3\}.$$

But this shows that $Z_1 = Z_2 \neq G$:

$$\begin{aligned}
Z_0 &= \{1\}\\
Z_1 &= \{1, r^3\}\\
Z_2 &= \{1, r^3\} \neq G.
\end{aligned}$$

Since $Z_1 = Z_2 \neq G$, we may conclude that D_{12} is not a nilpotent group.

Exercise 2.27. (Toronto, 1999) If T is a diagonalizable linear operator on a vector space V of finite dimension, and if the characteristic polynomial of T has only one root, show that T is a scalar multiple of the identity.

Solution 2.28. Let A denote the matrix corresponding to T. Since A is diagonalizable, we have that there exists a diagonalizing matrix P such that PAP^{-1} is equal to a diagonal matrix consisting ot the eigenvalue(s) of A along the main diagonal. But since the characteristic polynomial of A has only one root, the matrix A has only one eigenvalue, which shows that $PAP^{-1} = \lambda I_n$ for some $n \in \mathbb{N}$, since V is finite-dimensional, letting λ denote teh unique root of the characteristic polynomial of A. Since $PAP^{-1} = \lambda I_n$, we have that $P^{-1}(\lambda I_n)P = A$, and we thus have that $\lambda P^{-1} I_n P = A$, so that $A = \lambda P^{-1}P = \lambda I_n$.

[21] See `https://en.wikipedia.org/wiki/Center_(group_theory)`. As stated in this article, "The center of the dihedral group D_n, is trivial when n is odd. When n is even, the center consists of the identity elements together with the 180° rotation of the polygon."

2.2 University of British Columbia comprehensive exam questions

Exercise 2.29. (U.B.C., 2012) Let G be a group, H a subgroup. Recall that the *normalizer* fo H in G is the subgroup $N_G(H) = \{x \in G \mid xHx^{-1} = H\}$. Now let H_1, H_2 be subgroups of G that are conjugate to each other. Show that their normalizers $N_G(H_1)$, $N_G(H_2)$ are also conjugate to each other.

Solution 2.30. Since H_1 and H_2 are conjugate to each other, let $g \in G$ be such that $gH_1g^{-1}H_2$. By definition of the normalizer of a subgroup, we have that:

$$N_G(H_2) = \{x \in G \mid xH_2x^{-1} = H_2\}.$$

Since $gH_1g^{-1} = H_2$, we have that:

$$N_G(H_2) = \{x \in G \mid xgH_1g^{-1}x^{-1} = H_2\}.$$

Equivalently,

$$\begin{aligned} N_G(H_2) &= \{x \in G \mid xgH_1g^{-1}x^{-1} = gH_1g^{-1}\} \\ &= \{x \in G \mid g^{-1}xgH_1g^{-1}x^{-1}g = H_1\} \\ &= \{x \in G \mid g^{-1}xgH_1(g^{-1}xg)^{-1} = H_1\} \\ &= \{x \in G \mid g^{-1}xg \in N_G(H_1)\} \\ &= \{x \in G \mid x \in gN_G(H_1)g^{-1}\} \\ &= gN_G(H_1)g^{-1}. \end{aligned}$$

3 Terminology

Exercise 3.1. What is a nilpotent group?

Solution 3.2. See Exercise 1.78 and Exercise 2.17.

Exercise 3.3. What is a prime ideal?

Solution 3.4. A proper ideal P of an integral domain D is called a prime ideal if

$$ab \in P \Longrightarrow (a \in P \vee b \in P)$$

for $a, b \in D$.

Exercise 3.5. What is the centralizer of a subset of a group?

Solution 3.6. Let $A \subseteq G$. We define the centralizer of A in G as the set

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

Exercise 3.7. What is a Sylow p-subgroup?

Solution 3.8. A Sylow p-subgroup is a maximal p-subgroup.

Exercise 3.9. What is a Noetherian ring?

Solution 3.10. A commutative ring R with 1 is called Noetherian if every ideal of R is finitely generated.

Exercise 3.11. What is a Gröbner basis?

Solution 3.12. A Gröbner basis for an ideal I in the polynomial ring $F[x_1, x_2, \dots, x_n]$ is a finite set of generators $\{g_1, g_2, \dots, g_m\}$ for I whose leading terms generate the ideal of all leading terms in I, i.e.,

$$I = (g_1, g_2, \dots, g_m)$$

and

$$\text{LT}(I) = (\text{LT}(g_1), \text{LT}(g_2), \dots, \text{LT}(g_m)).$$

Exercise 3.13. What is an irreducible element in an integral domain R?

Solution 3.14. An irreducible element of R is a nonzero, nonunit element a of R such that: for all $b, c \in R$, if $a = bc$, then b or c is a unit.

Exercise 3.15. What is a prime element in an integral domain R?

Solution 3.16. A prime element of R is a nonzero, nonunit element $a \in R$ such that: for all $b, c \in R$, if $a|bc$, then $a|b$ or $a|c$.

Exercise 3.17. What are associate elements in R?

Solution 3.18. Two nonzero elements $a, b \in R$ are said to be associate elements in R if there exists a unit u such that $a = bu$.

Exercise 3.19. What is a solvable group?

Solution 3.20. A finite group G is solvable if there exists a subnormal series of the form

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

such that H_{i+1}/H_i is abelian for all indices i.