THE UNIVERSITY OF SYDNEY

MATH2022 LINEAR AND ABSTRACT ALGEBRA

Semester 1 **Week 7 Longer Solutions**

1. (a) We have

$$\begin{aligned}
\mathbb{Z}_2^2 &= \{(0,0),(0,1),(1,0),(1,1)\}\,, \\
\mathbb{Z}_2^3 &= \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}\,, \\
\mathbb{Z}_3^2 &= \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}\,, \\
\mathbb{Z}_2 \times \mathbb{Z}_3 &= \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}\,.
\end{aligned}$$

(b) For $\mathbb{Z}_2^2$, we have the following addition table:

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

For $\mathbb{Z}_2 \times \mathbb{Z}_3$, we have the following addition table:

+	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

(c) Put $\mathbf{v} = (1,1)$ and observe that

$$\mathbf{v}+\mathbf{v} \;=\; (0,2)\,, \qquad (0,2)+\mathbf{v} \;=\; (1,0)\,, \qquad (1,0)+\mathbf{v} \;=\; (0,1)\,,$$

$$(0,1)+\mathbf{v} \;=\; (1,2)\,, \qquad (1,2)+\mathbf{v} \;=\; (0,0)\,,$$

exhausting all elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$. (This works also choosing $\mathbf{v} = (1,2)$.)

(d) Let $\mathbf{v} = (1,0), \mathbf{w} = (0,1)$. As elements of $\mathbb{Z}_2^2$, we get $\mathbf{v}+\mathbf{v} = (0,0)$ and $\mathbf{v}+\mathbf{w} = (1,1)$, producing altogether all four elements of $\mathbb{Z}_2^2$. As elements of $\mathbb{Z}_3^2$, we get

$$\mathbf{v}+\mathbf{v} \;=\; (2,0)\,, \quad \mathbf{w}+\mathbf{w} \;=\; (0,2)\,, \quad (2,0)+\mathbf{v} \;=\; (0,0)\,, \quad \mathbf{v}+\mathbf{w} \;=\; (1,1)\,,$$

$$(2,0)+\mathbf{w} \;=\; (2,1)\,, \qquad (1,1)+\mathbf{w} \;=\; (1,2)\,, \qquad (2,1)+\mathbf{w} \;=\; (2,2)\,,$$

producing altogether all nine elements of $\mathbb{Z}_3^2$. (A more elegant way of showing this is to observe that $(a,b) = a\mathbf{v} + b\mathbf{w}$ as a, b range over $0, 1, 2$ and regarding $a\mathbf{v}$ and $b\mathbf{w}$ as appropriate integer multiples, that is, adding the vector to itself a certain number of times.)

Observe that if $\mathbf{v} \in \mathbb{Z}_2^2$ then $\mathbf{v} + \mathbf{v} = (0,0)$, so the only elements reached from $\mathbf{v}$ by addition are $\mathbf{v}$ and $(0,0)$. Further, if $\mathbf{v} \in \mathbb{Z}_3^2$ then $\mathbf{v} + \mathbf{v} + \mathbf{v} = (0,0)$, so now the only elements reached from $\mathbf{v}$ by addition are $\mathbf{v}$, $\mathbf{v} + \mathbf{v}$ and $(0,0)$. In no case can we have that a single element generates $\mathbb{Z}_2^2$ or $\mathbb{Z}_3^2$.

(e) Put $\mathbf{u} = (1,0,0)$, $\mathbf{v} = (0,1,0)$ and $\mathbf{w} = (0,0,1)$. If $\mathbf{x} \in \mathbb{Z}_2^3$ then $\mathbf{x} = (a,b,c)$ for some $a,b,c \in \mathbb{Z}_2$. But now we have

$$\mathbf{x} \;=\; a(1,0,0) + b(0,1,0) + c(0,0,1) \;=\; a\mathbf{u} + b\mathbf{v} + c\mathbf{w} \;,$$

where we may now regard a,b,c as integers from $\{0,1\}$. Thus we exhaust all nonzero elements of $\mathbb{Z}_2^3$ by applying addition in various combinations to $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$, and of course we also get $(0,0,0) = \mathbf{u} + \mathbf{u}$.

We show that it is not possible to generate $\mathbb{Z}_2^3$ using fewer than three elements. Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^3$. Clearly $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$. Thus the result of adding $\mathbf{x}$ and $\mathbf{y}$ together in any combination and with repetition produces an expression

$$a\mathbf{x} + b\mathbf{y}$$

for some positive integers a and b, where $a\mathbf{x}$ means adding $\mathbf{x}$ to itself a times, and similarly for $b\mathbf{y}$. But $2\mathbf{x} = 2\mathbf{y} = (0,0)$, so in evaluating this expression we may suppose that $a, b \in \{0,1\}$. Thus there are at most $2 \times 2 = 4$ possible evaluations of such expressions, so it is impossible to reach all 8 of the elements of $\mathbb{Z}_2^3$. This suffices to prove that it is not possible to generate $\mathbb{Z}_2^3$ with fewer than three elements.

2. Consider $\mathbf{v}, \mathbf{w} \in F^m$ and $\lambda, \mu \in F$. Suppose first that L respects addition and scalar multiplication. Then

$$L(\lambda\mathbf{v} + \mu\mathbf{w}) \;=\; L(\lambda\mathbf{v}) + L(\mu\mathbf{w}) \;=\; \lambda L(\mathbf{v}) + \mu L(\mathbf{w}) \;,$$

at the first step because L preserves addition, and at the second step because L preserves scalar multiplication. This verifies that L preserves linear combinations. Suppose conversely that L preserves linear combinations. Observe that

$$\mathbf{v} + \mathbf{w} = 1\mathbf{v} + 1\mathbf{w} \qquad \text{and} \qquad \lambda\mathbf{v} = \lambda\mathbf{v} + 0\mathbf{w} \;,$$

so that, since L preserves linear combinations,

$$L(\mathbf{v} + \mathbf{w}) \;=\; L(1\mathbf{v} + 1\mathbf{w}) \;=\; 1L(\mathbf{v}) + 1L(\mathbf{w}) \;=\; L(\mathbf{v}) + L(\mathbf{w}) \;,$$

and

$$L(\lambda\mathbf{v}) \;=\; L(\lambda\mathbf{v} + 0\mathbf{w}) \;=\; \lambda L(\mathbf{v}) + 0L(\mathbf{w}) \;=\; \lambda L(\mathbf{v}) \;,$$

which verifies that L preserves addition and scalar multiplication.

3. Let $\mathbf{v}_1, \mathbf{v}_2 \in F^2$ and $\lambda, \mu \in F$. Then $\mathbf{v}_1 = (x_1, y_1)$ and $\mathbf{v}_2 = (x_2, y_2)$ for some $x_1, x_2, y_1, y_2 \in F$. Hence

$$\begin{aligned}
L(\lambda\mathbf{v}_1 + \mu\mathbf{v}_2) &= L(\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2) \\
&= \big(a(\lambda x_1 + \mu x_2) + b(\lambda y_1 + \mu y_2), c(\lambda x_1 + \mu x_2) + d(\lambda y_1 + \mu y_2)\big) \\
&= \big(\lambda(ax_1 + by_1) + \mu(ax_2 + by_2), \lambda(cx_1 + dy_1) + \mu(cx_2 + dy_2)\big) \\
&= \big(\lambda(ax_1 + by_1), \lambda(cx_1 + dy_1)\big) + \big(\mu(ax_2 + by_2), \mu(cx_2 + dy_2))\big) \\
&= \lambda\big(ax_1 + by_1, cx_1 + dy_1\big) + \mu\big(ax_2 + by_2, cx_2 + dy_2\big) \\
&= \lambda L(\mathbf{v}_1) + \mu L(\mathbf{v}_2) \;,
\end{aligned}$$

which verifies that L is a linear transformation. Put

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad \text{and} \qquad \mathbf{v} = (x, y) \equiv \begin{bmatrix} x & y \end{bmatrix} .$$

We have $L(\mathbf{v}) = \mathbf{w}$ where

$$\mathbf{w} = (ax + by, cx + dy) \equiv \begin{bmatrix} ax + by & cx + dy \end{bmatrix} ,$$

and then

$$M\mathbf{v}^\top = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} = \mathbf{w}^\top .$$

4. (a) Let $\mathbf{v}_1 = (x_1, y_1)$ and $\mathbf{v}_2 = (x_2, y_2)$. Then

$$\begin{aligned} f(\mathbf{v}_1 + \mathbf{v}_2) &= f(x_1 + x_2, y_1 + y_2) \\ &= (x_1 + x_2, x_1 + x_2 + y_1 + y_2, 3x_1 + 3x_2 - 2y_1 - 2y_2) \\ &= (x_1, x_1 + y_1, 3x_1 - 2y_1) + (x_2, x_2 + y_2, 3x_2 - 2y_2) \\ &= f(\mathbf{v}_1) + f(\mathbf{v}_2) , \end{aligned}$$

verifying that f preserves addition. Let $\mathbf{v} = (x, y)$ and $\lambda \in \mathbb{R}$. Then

$$\begin{aligned} f(\lambda\mathbf{v}) &= f(\lambda x, \lambda y) = (\lambda x, \lambda x + \lambda y, 3\lambda x - 2\lambda y) \\ &= \lambda(x, x + y, 3x - 2y) = \lambda f(\mathbf{v}) , \end{aligned}$$

verifying that f preserves scalar multiplication, completing the verification that f is a linear transformation.

(b) Observe the effects on standard basis vectors:

$$f(1, 0) = (1, 1, 3) , \qquad f(0, 1) = (0, 1, -2) ,$$

$$g(1, 0, 0) = (1, 0, 1, 1) , \quad g(0, 1, 0) = (2, 2, -3, 1) , \quad g(0, 0, 1) = (0, -1, 0, 1) .$$

Hence, transposing these into columns, we get

$$M_f = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 3 & -2 \end{bmatrix} \qquad \text{and} \qquad M_g = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & -1 \\ 1 & -3 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

(c) We have the composite rule

$$\begin{aligned} (gf)(x, y) &= g(f(x, y)) = g(x, x + y, 3x - 2y) \\ &= (x+2(x + y), 2(x + y) - (3x - 2y), x - 3(x + y), x + (x + y) + (3x - 2y)) \\ &= (3x + 2y, -x + 4y, -2x - 3y, 5x - y) . \end{aligned}$$

Its effect on standard basis vectors is as follows:

$$(gf)(1, 0) = (3, -1, -2, 5) \qquad \text{and} \qquad (gf)(0, 1) = (2, 4, -3, -1) ,$$

so that, transposing into columns, we get

$$M_{gf} = \begin{bmatrix} 3 & 2 \\ -1 & 4 \\ -2 & -3 \\ 5 & -1 \end{bmatrix}.$$

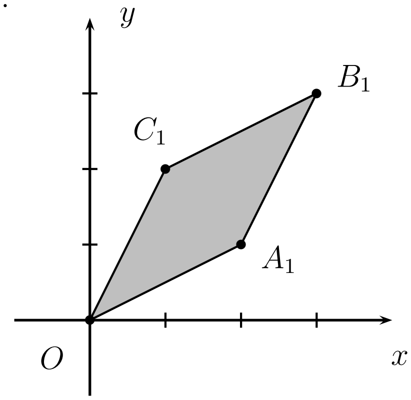
This should be the same as the following matrix product:

$$M_g M_f = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & -1 \\ 1 & -3 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 3 & -2 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ -1 & 4 \\ -2 & -3 \\ 5 & -1 \end{bmatrix},$$

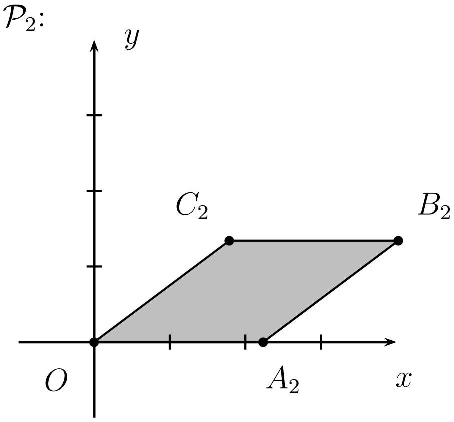
which checks out correctly.

5. (a) We have

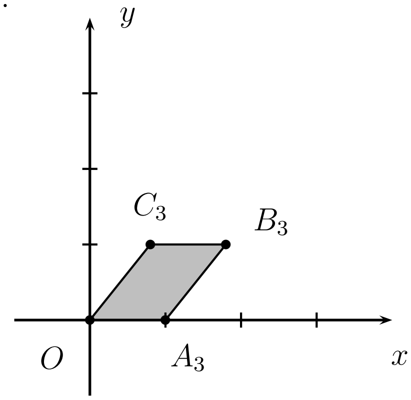
(i) $\mathcal{P}_1$:



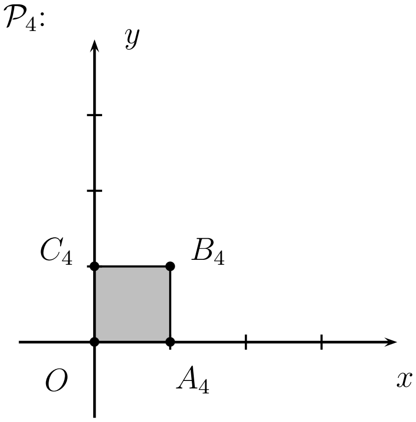
(ii) $\mathcal{P}_2$:



(iii) $\mathcal{P}_3$:



(iv) $\mathcal{P}_4$:



To get from $\mathcal{P}_1$ to $\mathcal{P}_2$, we rotate the xy-plane $\tan^{-1} 0.5 \approx 26.6$ degrees clockwise. To get from $\mathcal{P}_2$ to $\mathcal{P}_3$, we dilate in the x-direction by a factor of $\frac{1}{\sqrt{5}}$ and in the y-direction by a factor of $\frac{\sqrt{5}}{3}$. To get from $\mathcal{P}_3$ to $\mathcal{P}_4$, we apply a shear that shifts points proportional to their y-values sideways left by a factor of $\frac{4}{5}$ (or sideways right by a factor of $-\frac{4}{5}$).

(b) The respective linear transformations in part (a) are achieved by the following matrices (acting by premultiplication on the column vectors corresponding to points in the xy-plane):

$$R = \frac{1}{\sqrt{5}}\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}, \qquad D = \begin{bmatrix} \frac{1}{\sqrt{5}} & 0 \\ 0 & \frac{\sqrt{5}}{3} \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & -\frac{4}{5} \\ 0 & 1 \end{bmatrix}.$$

Then

$$\begin{aligned} SDRM_1 &= \begin{bmatrix} 1 & \frac{4}{5} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{5}} & 0 \\ 0 & \frac{\sqrt{5}}{3} \end{bmatrix}\frac{1}{\sqrt{5}}\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -\frac{4}{5} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{5} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}\begin{bmatrix} 5 & 4 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{4}{5} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{4}{5} \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, \end{aligned}$$

as required. Thus

$$M_1 = (SDR)^{-1} = R^{-1}D^{-1}S^{-1} = \frac{1}{\sqrt{5}}\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} \sqrt{5} & 0 \\ 0 & \frac{3}{\sqrt{5}} \end{bmatrix}\begin{bmatrix} 1 & \frac{4}{5} \\ 0 & 1 \end{bmatrix},$$

which is a product of a rotation matrix, diagonal matrix and shear matrix, in that order, as required.

(c) Observe, using the factorisation of M_1 from part (b), that

$$\begin{aligned} M_2 &= \begin{bmatrix} 2 & 1 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\frac{1}{\sqrt{5}}\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} \sqrt{5} & 0 \\ 0 & \frac{3}{\sqrt{5}} \end{bmatrix}\begin{bmatrix} 1 & \frac{4}{5} \\ 0 & 1 \end{bmatrix} \\ &= \frac{1}{\sqrt{5}}\begin{bmatrix} 2 & -1 \\ -1 & -2 \end{bmatrix}\begin{bmatrix} \sqrt{5} & 0 \\ 0 & \frac{3}{\sqrt{5}} \end{bmatrix}\begin{bmatrix} 1 & \frac{4}{5} \\ 0 & 1 \end{bmatrix}, \end{aligned}$$

which is a product of a reflection matrix, diagonal matrix and shear matrix, in that order, as required.

6. Let $\mathbf{v}, \mathbf{w} \in F^m$ and $\lambda, \mu \in F$. Then

$$\begin{aligned} (L_2L_1)(\lambda\mathbf{v} + \mu\mathbf{w}) &= L_2\big(L_1(\lambda\mathbf{v} + \mu\mathbf{w})\big) = L_2\big(\lambda L_1(\mathbf{v}) + \mu L_1(\mathbf{w})\big) \\ &= \lambda L_2\big(L_1(\mathbf{v})\big) + \mu L_2\big(L_1(\mathbf{w})\big) = \lambda(L_2L_1)(\mathbf{v}) + \mu(L_2L_1)(\mathbf{w}), \end{aligned}$$

at the first and last steps by definition of composition of functions, and at the second and third steps by the fact that L_1 and L_2 respectively preserve linear combinations. This verifies that L_2L_1 preserves linear combinations, so is also a linear transformation.

7. (a) The effects on standard basis vectors are as follows:

$$f(1,0) = (2,1) \quad f(0,1) = (1,2), \quad g(1,0) = (0,1), \quad g(0,1) = (-1,0),$$
$$h(1,0) = (0,1), \quad h(0,1) = (1,0).$$

Transposing into columns produces the following matrices:

$$M_f = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \quad M_g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad M_h = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

(b) We have the following composite rules:

$$\begin{aligned}(gf)(x,y) &= g(f(x,y)) = g(2x+y,x+2y) = (-x-2y,2x+y)\,,\\ (g^2f)(x,y) &= g(gf(x,y)) = g(-x-2y,2x+y) = (-2x-y,-x-2y)\,,\\ (g^3f)(x,y) &= g(g^2f(x,y)) = g(-2x-y,-x-2y) = (x+2y,-2x-y)\,.\end{aligned}$$

We also have the following matrix products:

$$M_gM_f = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} -1 & -2 \\ 2 & 1 \end{bmatrix} = M_{gf}\,,$$

yielding the rule $(gf)(x,y) = (-x-2y,2x+y)$, matching the direct calculation;

$$M_g\big(M_gM_f\big) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -1 & -2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} -2 & -1 \\ -1 & -2 \end{bmatrix} = M_{g^2f}\,,$$

yielding the rule $(g^2f)(x,y) = (-2x-y,-x-2y)$, matching the direct calculation;

$$M_g\big(M_gM_gM_f\big) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -2 & -1 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -2 & -1 \end{bmatrix} = M_{g^3f}\,,$$

yielding the rule $(g^3f)(x,y) = (x+2y,-2x-y)$, matching the direct calculation.

(c) Observe that $(0,0)$ is fixed by all of these linear transformations. For the images of the other points we have

$$f(1,0) = (2,1)\,,\quad f(0,1) = (1,2)\,,\quad f(1,1) = (3,3)\,,$$

producing a parallelogram in the first quadrant;

$$gf(1,0) = (-1,2)\,,\quad gf(0,1) = (-2,1)\,,\quad gf(1,1) = (-3,3)\,,$$

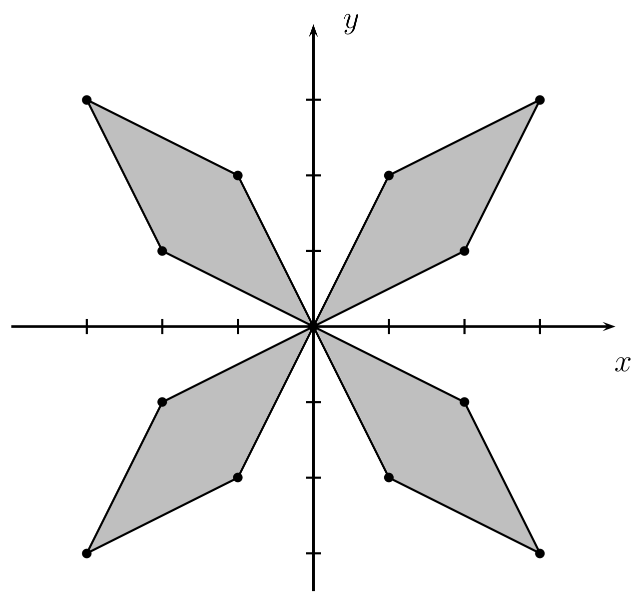
producing a parallelogram in the second quadrant;

$$g^2f(1,0) = (-2,-1)\,,\quad g^2f(0,1) = (-1,-2)\,,\quad g^2f(1,1) = (-3,-3)\,,$$

producing a parallelogram in the third quadrant;

$$g^3f(1,0) = (1,-2)\,,\quad g^3f(0,1) = (2,-1)\,,\quad g^3f(1,1) = (3,-3)\,,$$

producing a parallelogram in the fourth quadrant, thus producing the following images:



(d) We have

$$M_f^{-1} = \frac{1}{3}\begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}, \quad M_g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad M_h^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

yielding the rules

$$f^{-1}(x,y) = \frac{1}{3}(2x-y,-x+2y), \quad g^{-1}(x,y) = (y,-x), \quad h^{-1}(x,y) = (y,x).$$

We also have

$$M_{gf}^{-1} = \frac{1}{3}\begin{bmatrix} 1 & 2 \\ -2 & -1 \end{bmatrix},$$

yielding the rule

$$(gf)^{-1}(x,y) = \frac{1}{3}(x+2y,-2x-y).$$

This should coincide with the rule for $f^{-1}g^{-1}$, which we can find by direct composition:

$$\begin{aligned}(f^{-1}g^{-1})(x,y) &= f^{-1}(g^{-1}(x,y)) = f^{-1}(y,-x) \\ &= \frac{1}{3}(2y+x,-y-2x) = \frac{1}{3}(x+2y,-2x-y),\end{aligned}$$

which matches exactly the previous calculation.

(e) The effect of g is to rotate the four rhombus shapes, which are the images of the unit square, one quarter of a turn anticlockwise about the origin, fixing the overall configuration of the four shapes. The effect of h, which interchanges the coordinates, is to reflect the images through the line $y = x$, so that the shapes in the first and third quadrants are fixed, and the shapes in the second and fourth quadrants are interchanged, though in all cases the orientation of the vertices of any of the four shapes is reversed. Observe that

$$M_{g^4} = M_g^4 = (M_g^2)^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I,$$

$$M_{h^2} = M_h^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I,$$

$$M_{hgh} = M_h M_g M_h = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = M_{g^{-1}},$$

so that $g^4 = h^2 = \mathrm{id}$ where id is the identity function on $\mathbb{R}^2$, and the rule for hgh is just the rule for g^{-1}.

8. (a) If A or B is empty then $A \times B$ is empty. In general, if $|A|$ and $|B|$ are finite then

$$|A \times B| = |A||B|$$

(where $|X|$ is the size of a set X), since for each of $|A|$ choices for the first element of an order pair in $A \times B$ there are $|B|$ choices for the second element.

(b) Let A, B and C be nonempty sets, so there exists some $a \in A$, $b \in B$ and $c \in C$. Put

$$\alpha \;=\; ((a,b),c)\;.$$

Then $\alpha \in (A \times B) \times C$, being an ordered pair whose first element is in $A \times B$ (itself an ordered pair), and second element is in C. But all elements of $A \times B \times C$ are ordered triples, with three entries, so $\alpha \notin A \times B \times C$. Hence the sets cannot be equal. However, the map

$$((a,b),c) \mapsto (a,b,c)$$

for $a \in A$, $b \in B$, $c \in C$, is clearly a bijection from $(A \times B) \times C$ to $A \times B \times C$.

(c) Since A and B are different sets, either (i) there exists $a \in A$ such that $a \notin B$, or (ii) there exists $b \in B$ such that $b \notin A$. Suppose the first case (i) holds. Since B is nonempty, there exists some $c \in B$, and then $(a,c) \in A \times B$, but $(a,c) \notin B \times A$, since $a \notin B$. Suppose now the second case (ii) holds. Since A is nonempty, there exists some $d \in A$, and then $(d,b) \in A \times B$, but $(d,b) \notin B \times A$, since $b \notin A$. In both cases, we have shown that $A \times B$ and $B \times A$ are different sets. However, the map $(a,b) \mapsto (b,a)$, for $a \in A$, $b \in B$, is clearly a bijection from $A \times B$ to $B \times A$.

(d) Put

$$A \;=\; \{(a_1, a_2, a_3 \ldots) \mid a_1, a_2, a_3 \ldots \in \mathbb{Z}_2\}\;,$$

the set of all infinite sequences with entries from $\mathbb{Z}_2$. Certainly A has at least two elements (in fact infinitely many elements). Let $\phi : A \to A \times A$ where

$$\phi : (a_1, a_2, a_3 \ldots) \mapsto \big((a_1, a_3, a_5, \ldots), (a_2, a_4, a_6, \ldots)\big)$$

for $a_1, a_2, a_3 \ldots \in \mathbb{Z}_2$, which is clearly one-one and onto, so ϕ is a bijection. This proves there exists a bijection between A and A^2, which starts an induction. Suppose, as inductive hypothesis, that there exists a bijection $\psi : A \to A^k$, where $k \geq 1$. Then the following map is also clearly a bijection:

$$\overline{\psi} : A \times A \to A^k \times A\,, \quad (a,b) \mapsto (a\psi, b)\,,$$

where $a, b \in A$. We also have the following bijection, analogous to the bijection in part (b):

$$\theta : A^k \times A \to A^{k+1}\,, \quad \big((a_1, \ldots, a_k), a_{k+1}\big) \mapsto (a_1, \ldots, a_k, a_{k+1})\;,$$

for $a_1, \ldots, a_{k+1} \in A$. Then the composite $\phi\overline{\psi}\theta : A \to A^{k+1}$ is a bijection (composing from left to right), establishing the inductive step. This proves there exists a bijection between A and A^n for all positive integers n.

9. Suppose that $A_1, \ldots, A_k$ are abelian groups with respect to addition. Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in A_1 \times \ldots \times A_k$, so that

$$\mathbf{a} = (a_1, \ldots, a_k)\,, \quad \mathbf{b} = (b_1, \ldots, b_k)\,, \quad \mathbf{c} = (c_1, \ldots, c_k)$$

for some $a_1, b_1, c_1 \in A_1, \ldots, a_k, b_k, c_k \in A_k$. Then, using coordinatewise addition, and associativity in each coordinate,

$$\begin{aligned}
\big(\mathbf{a} + \mathbf{b}\big) + \mathbf{c} &= (a_1 + b_1, \ldots, a_k + b_k) + (c_1, \ldots, c_k) \\
&= ((a_1 + b_1) + c_1, \ldots, (a_k + b_k) + c_k) \\
&= (a_1 + (b_1 + c_1), \ldots, a_k + (b_k + c_k)) \\
&= (a_1 + \ldots + a_k) + (b_1 + c_1, \ldots, b_k + c_k) = \mathbf{a} + \big(\mathbf{b} + \mathbf{c}\big)
\end{aligned}$$

and further, using commutativity in each coordinate,

$$\mathbf{a}+\mathbf{b} \;=\; (a_1+b_1,\ldots,a_k+b_k) \;=\; (b_1+a_1,\ldots,b_k+a_k) \;=\; \mathbf{b}+\mathbf{a}\,,$$

which verifies associativity and commutativity in $A_1\times\ldots\times A_k$. Put

$$\mathbf{0}=(0,\ldots,0) \quad\text{and}\quad -\mathbf{a}=(-a_1,\ldots,-a_k)$$

both elements of $A_1\times\ldots\times A_k$. Observe that

$$\mathbf{0}+\mathbf{a} \;=\; (0+a_1,\ldots,0+a_k) \;=\; (a_1,\ldots,a_k) \;=\; \mathbf{a}\,,$$

and similarly $\mathbf{a}+\mathbf{0}=\mathbf{a}$, and further that

$$\mathbf{a}+(-\mathbf{a}) \;=\; (a_1-a_1,\ldots,a_k-a_k) \;=\; (0,\ldots,0) \;=\; \mathbf{0}\,,$$

and similarly $(-\mathbf{a})+\mathbf{a}=\mathbf{0}$. These observations show that $A_1\times\ldots\times A_k$ has an additive identity element and additive inverses, completing the verification that $A_1\times\ldots\times A_k$ is an abelian group.

10. (a) Utilising explorations from the first exercise, an isomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_2\times\mathbb{Z}_3$ maps the additive generator 1 of $\mathbb{Z}_6$ to one of the two additive generators of $\mathbb{Z}_2\times\mathbb{Z}_3$, namely $(1,1)$ or $(1,2)$, thus inducing the following two isomorphisms:

$$\phi_1: 1\mapsto(1,1)\,,\; 2\mapsto(0,2)\,,\; 3\mapsto(1,0)\,,\; 4\mapsto(0,1)\,,\; 5\mapsto(1,2)\,,\; 0\mapsto(0,0)\,,$$
$$\phi_2: 1\mapsto(1,2)\,,\; 2\mapsto(0,1)\,,\; 3\mapsto(1,0)\,,\; 4\mapsto(0,2)\,,\; 5\mapsto(1,1)\,,\; 0\mapsto(0,0)\,.$$

There can be no other isomorphisms, because none of the remaining elements, namely, $(0,0)$, $(1,0)$, $(0,1)$ and $(0,2)$, can generate $\mathbb{Z}_2\times\mathbb{Z}_3$, since each of them has 0 in one or both coordinates.

(b) Put $\alpha=(1,1,1)\in\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_5$. If k is a positive integer then $k\alpha$ means the result of adding α to itself k times. Then

$$k\alpha \;=\; k(1,1,1) \;=\; (\overline{k},\widehat{k},\widetilde{k})\,,$$

where $\overline{k}$, $\widehat{k}$, $\widetilde{k}$ are the remainders after dividing k by 2, 3 and 5 respectively. Certainly then

$$30(1,1,1) \;=\; (\overline{30},\widehat{30},\widetilde{30}) \;=\; (0,0,0)\,.$$

If $0<k<30$ then at least one of $\overline{k}$, $\widehat{k}$ or $\widetilde{k}$ is nonzero, since 30 is the least common multiple of 2, 3 and 5. These facts establish that $\langle\alpha\rangle$ contains exactly 30 ordered triples, so that

$$\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_5 \;=\; \langle\alpha\rangle\,,$$

since the sets have the same size. Hence $\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_5$ is a cyclic group isomorphic to $\mathbb{Z}_{30}$, since they are both cyclic groups of the same size.

We show $\mathbb{Z}_2\times\mathbb{Z}_2\times Z_5$ is not isomorphic to $\mathbb{Z}_{20}$. Suppose to the contrary that they are isomorphic. Then the image of the generator 1 of $\mathbb{Z}_{20}$ must be a generator α, say, of $\mathbb{Z}_2\times\mathbb{Z}_2\times Z_5$. Then α added to itself repeatedly must produce all 20 of the elements in $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_5$. But

$$\alpha \;=\; (a,b,c)$$

for some $a,b\in\mathbb{Z}_2$ and $c\in\mathbb{Z}_5$. But $10\alpha=(0,0,0)$, since 10 is a multiple of 2 and 5, so adding α to itself repeatedly cycles through only 10 elements, not 20, which is a contradiction. This proves $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_5$ is not isomorphic to $\mathbb{Z}_{20}$.

11. We have that $\phi : G \to H$ and $\psi : H \to K$ are group isomorphisms. In particular ϕ and ψ are bijections. Certainly $\phi^{-1} : H \to G$ and $\phi\psi : G \to K$ are also bijections. Let $h_1, h_2 \in H$. Then, since ϕ is onto, we have $h_1 = g_1\phi$ and $h_2 = g_2\phi$ for some $g_1, g_2 \in G$, so that

$$g_1 = h_1\phi^{-1} \quad \text{and} \quad g_2 = h_2\phi^{-1} .$$

Hence, since ϕ preserves the group operation,

$$(h_1h_2)\phi^{-1} \;=\; \big((g_1\phi)(g_2\phi)\big)\phi^{-1} \;=\; \big((g_1g_2)\phi\big)\phi^{-1} \;=\; g_1g_2 \;=\; (h_1\phi^{-1})(g_2\phi^{-1}) ,$$

which verifies that ϕ^{-1} is a group isomorphism. Now let $a, b \in G$. Then, since both ϕ and ψ preserve the respective group operations,

$$(ab)(\phi\psi) \;=\; \big((ab)\phi\big)\psi \;=\; \big((a\phi)(b\phi)\big)\psi \;=\; \big((a\phi)\psi\big)\big((b\phi)\psi\big) \;=\; \big(a(\phi\psi)\big)\big(b(\phi\psi)\big) ,$$

which verifies that $\phi\psi$ is a group isomorphism.

12. Observe that $\alpha^6 = \beta^2 = 1$ and also that

$$\beta^{-1}\alpha\beta \;=\; \beta\alpha\beta \;=\; (3\;2\;1)(4\;5) \;=\; \alpha^{-1} \;=\; \alpha^5 ,$$

so that $\beta\alpha = \alpha^5\beta$. Thus any combination of α's and β's can be rewritten as a power of α followed by a power of β, and then these powers reduce to produce an expression of the form $\alpha^i\beta^j$ where $0 \leq i \leq 5$ and $0 \leq j \leq 1$. This verifies that

$$\begin{aligned} G \;&=\; \{\alpha^i\beta^j \mid 0 \leq i \leq 5\,,\; 0 \leq j \leq 1\} \\ &=\; \{1\,,\; (1\;2\;3)(4\;5)\,,\; (1\;3\;2)\,,\; (4\;5)\,,\; (1\;2\;3)\,,\; (1\;3\;2)(4\;5)\,, \\ &\qquad (1\;3)\,,\; (1\;2)(4\;5)\,,\; (2\;3)\,,\; (1\;3)(4\;5)\,,\; (1\;2)\,,\; (2\;3)(4\;5)\} ,\end{aligned}$$

noting that we get 12 distinct permutations. Let H be the symmetry group of the hexagon, which also contains 12 elements, six rotations and six reflections. Let R be the one sixth (60 degree) rotation of the hexagon and T any reflection. Then

$$H \;=\; \{R^iT^j \mid 0 \leq i \leq 5\,,\; 0 \leq j \leq 1\} ,$$

and, since also $H^6 = T^2 = 1$ and $T^{-1}HT = H^{-1}$, the multiplication in H is given by the rule

$$R^iT^jR^kT^\ell \;=\; \begin{cases} R^{i+k}T^\ell & \text{if } j = 0, \\ R^{i-k}T^{1+\ell} & \text{if } j = 1, \end{cases}$$

where addition of the exponents of R can be taken mod 6 and addition of the exponents of T can be taken mod 2. But, from the earlier equations, the multiplication in G is given by the rule

$$\alpha^i\beta^j\alpha^k\beta^\ell \;=\; \begin{cases} \alpha^{i+k}\beta^\ell & \text{if } j = 0, \\ \alpha^{i-k}\beta^{1+\ell} & \text{if } j = 1, \end{cases}$$

where addition of the exponents of α can be taken mod 6 and addition of the exponents of β can be taken mod 2. Thus the bijection

$$\phi : G \to H\,,\;\; \alpha^i\beta^j \mapsto R^iT^j ,$$

for $0 \leq i \leq 5$ and $0 \leq j \leq 1$, preserves multiplication so is a group isomorphism.