1a) Observe that the product of two matrices $x, y \in \mathbb{R}$ has

$$xy = \begin{bmatrix} \cos(x)\cos(y) - \sin(x)\sin(y) & \cos(x)\sin(y) + \sin(x)\cos(y) \\ -\sin(x)\cos(y) - \cos(x)\sin(y) & -\sin(x)\sin(y) + \cos(x)\cos(y) \end{bmatrix}$$

or, using trig identities,

$$xy = \begin{bmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{bmatrix}$$

and that $(x+y) \in \mathbb{R}$. G is therefore closed under matrix multiplication, which we know also has the the associative property. Also observe that $\cos(0) = 1$ and $\sin(0) = 0$, meaning that $\theta \in \mathbb{R}$, $\theta = 0$ shows that the identity matrix is an element of G. Finally, consider the determinant of any element of G:

$$\det(a) = \cos^2(\theta) + \sin^2(\theta) = 1, \quad a \in G.$$

Given that $\det(a) \neq 0$, we know that a is invertible. Thus, G is a group under matrix multiplication. Furthermore, $G \leq GL_2(\mathbb{R})$ as any element of G is a 2×2 matrix over $\mathbb{R}$ with a nonzero determinant. Therefore, G is a subgroup of $GL_2(\mathbb{R})$.

* matrix multiplication between any two-by-two matrices is associative.

1b) Matrix multiplication is valid only if the dimensions of the two matrices are compatible, meaning that the numbers of columns of the first matrix matches the number of rows of the second. Observe that for any two elements $g_1, g_2 \in G$, and for $\bar{v} \in \mathbb{R}^2$, that

$(g_1 \cdot g_2)$ and

$(g_2 \cdot \bar{v})$ are compatible this way, and that for

$\bar{u} = g_2 \cdot \bar{v}$, $\bar{u} \in \mathbb{R}^2$ and

$g_3 = g_1 \cdot g_2$, $g_3 \in G$, that

$(g_1 \cdot \bar{u})$ and

$(g_3 \cdot \bar{v})$ are also compatible.

Therefore, through the compatibility and associative property of matrix multiplication,

$$g_1 \cdot (g_2 \cdot \bar{v}) = (g_1 \cdot g_2) \cdot \bar{v}, \quad g_1, g_2 \in G, \bar{v} \in \mathbb{R}^2.$$

Finally, consider $\bar{v} = \begin{bmatrix} a \\ b \end{bmatrix}$ and $e \in G$:

$$e \cdot \bar{v} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \bar{v}.$$

Therefore $e \cdot \bar{v} = \bar{v}$ for all $\bar{v} \in \mathbb{R}^2$, and thus matrix multiplication between M and $\bar{v}$ for $M \in G$ and $\bar{v} \in \mathbb{R}$ is an action of G on $\mathbb{R}^2$.

1c) The action $M \circ \bar{v} = M\bar{v}$ for $M \in G$ and $\bar{v} \in \mathbb{R}^2$ can be seen geometrically as a clockwise rotation of the vector $\bar{v}$ about the origin.

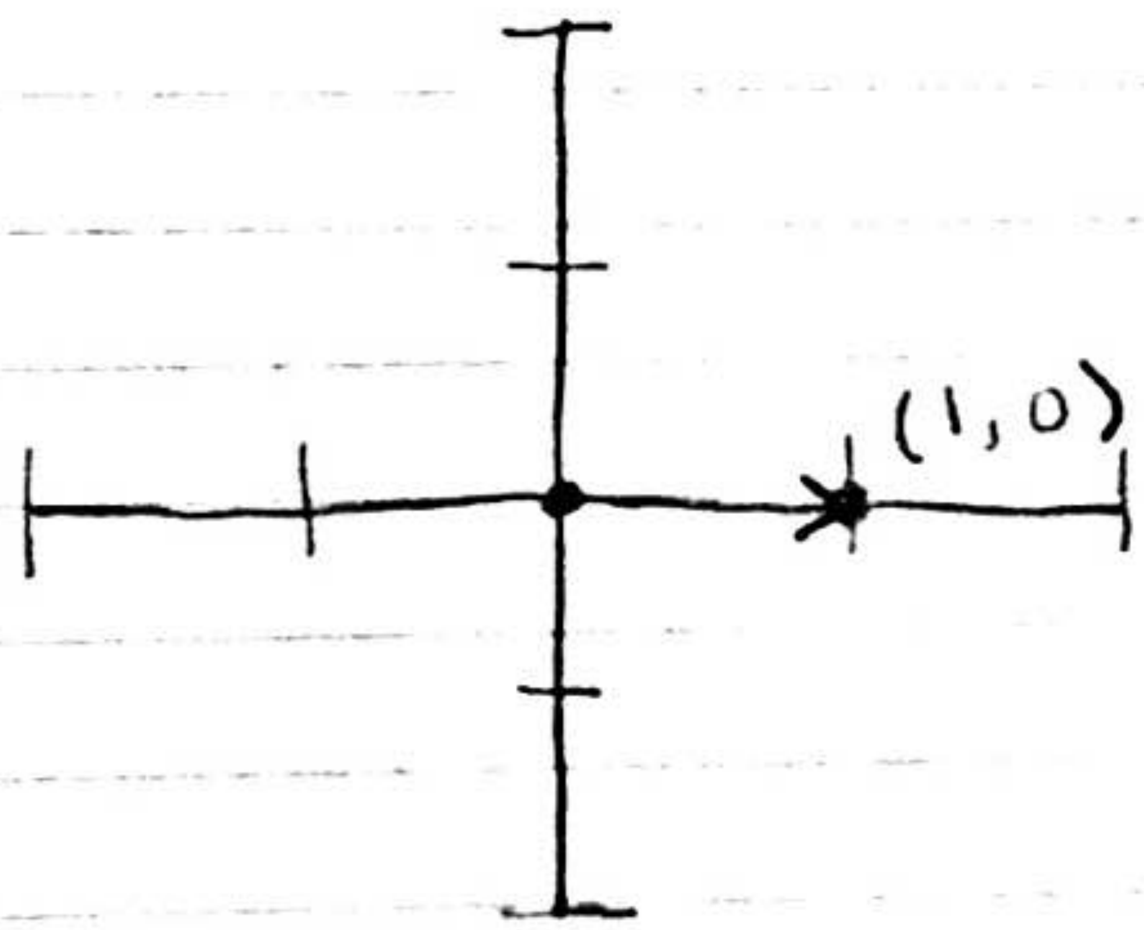
First, consider the mappings:

$$M\bar{v} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ for } \bar{v} = \begin{bmatrix} x \\ y \end{bmatrix}.$$

Therefore,

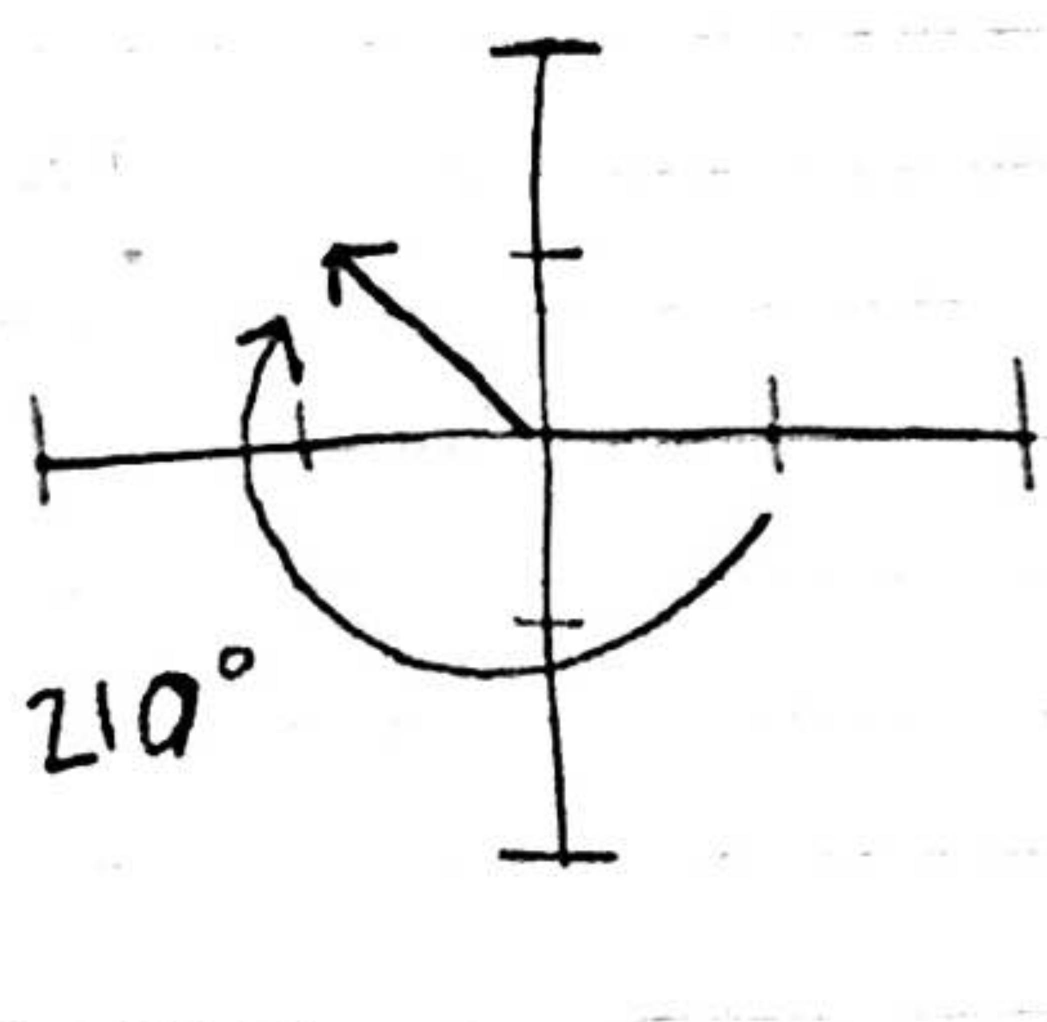
$$M\bar{v} = x \begin{bmatrix} \cos\theta \\ -\sin\theta \end{bmatrix} + y \begin{bmatrix} \sin\theta \\ \cos\theta \end{bmatrix}.$$

Consider the unit vector $\bar{u} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$:



A rotation of $210°$, given by $\theta = \frac{7\pi}{6}$, can be seen:

$$M\bar{u}\Big|_{\theta = \frac{7\pi}{6}} = \begin{bmatrix} -0.866 \\ 0.500 \end{bmatrix}:$$



2a) Let $|x| = n$ and $x^k = 1 = e$.

By virtue of the Euclidean Algorithm, there exists $q, r \in \mathbb{Z}$ such that

$$k = qn + r, \quad 0 \leq r < n.$$

Therefore $x^k = x^{qn+r} = (x^n)^q (x^r) = x^r = 1 = e$. We know, however, that $|x| = n$, meaning n is the smallest integer that exponentiates x to equal the identity element. Therefore, as $0 \leq r < n$:

$$r = 0 \text{ and}$$
$$k = qn.$$

Thus, $n | k$.

2b) Observe that $\phi(1_G) = 1_H$ and $\phi(x^n) = (\phi(x))^n$, meaning that for $|x| = n$, $x^n = 1_G$, and therefore

$$(\phi(x))^n = \phi(x^n) = \phi(1_G) = 1_H.$$

Observe, however, that if $|\phi(x)| = \ell$ and $(\phi(x))^n = 1_H$, then, using the proof above, $\ell | n$.

Thus, $|\phi(x)|$ divides n.

$Aut(G)$ is a group under function composition:

Let $f, g \in Aut(G)$ and $x, y \in G$.
Then $f(g(xy)) = f(g(x)g(y))$
$= f(g(x))f(g(y))$,
Or if we let $\circ$ show the composition operation:
$$f \circ g(xy) = f \circ g(x)\, f \circ g(y), \text{ for all } x, y \in G.$$
$f \circ g$ inherits bijectivity from f and g, and maps $G \to G$.
Therefore $Aut(G)$ is closed under composition as $f \circ g$ is also an automorphism.
Let $h \in Aut(G)$.
$f \circ (g \circ h)(x) = f(g(h(x))) = (f \circ g) \circ h(x)$
as G is associative. Therefore $Aut(G)$ is also associative.

Also, let us consider the identity and inverses:

Let $e \in Aut(G)$ such that for all $x \in G$, $e(x) = x$.
Observe that $e \circ g = e(g(x)) = g(x) = g$
and that $g \circ e = g(e(x)) = g(x) = g$.
Therefore $e \circ g = g \circ e = g$ for all $g \in G$, meaning e is the identity automorphism of $Aut(G)$.

Finally, reconsider $x, y \in G$:

$xy = e(xy) = f \circ f^{-1}(xy) = f(f^{-1}(xy))$ and
$xy = e(x)e(y) = f \circ f^{-1}(x)\, f \circ f^{-1}(y)$
$= f(f^{-1}(x))f(f^{-1}(y))$ and therefore
$f(f^{-1}(xy)) = f(f^{-1}(x))f(f^{-1}(y))$, for all $x, y \in G$.
Since $Aut(G)$ is one-to-one, and as $f \circ f^{-1} \in Aut(G)$, $f^{-1} \in Aut(G)$ as $f^{-1}(x)$ and $f^{-1}(y)$ must map to G. Therefore, $Aut(G)$ is a group.

4b) Let $x, y \in G$.

$$\phi_g(xy) = g(xy)g^{-1} = g(x(g^{-1}g)y)g^{-1}$$
$$(gxg^{-1})(gyg^{-1})$$
$$= \phi_g(x)\,\phi_g(y).$$

Therefore ϕ_g is a homomophism of G.
Suppose $\phi_g(x) = \phi_g(y)$.
Then $gxg^{-1} = gyg^{-1}$, which if we multiply g^{-1} on the left and g on the right,

$$g^{-1}(gxg^{-1})g = g^{-1}(gyg^{-1})g$$
$$(g^{-1}g)x(g^{-1}g) = (g^{-1}g)y(g^{-1}g)$$
$$x = y$$

Therefore ϕ_g is one-to-one, or injective.

Finally, given $b \in G$, let $x = g^{-1}bg$.

Then $\phi_g(x) = g(g^{-1}bg)g^{-1} = (gg^{-1})b(gg^{-1}) = b$.
Therefore ϕ_g is onto, or surjective.
Thus, ϕ_g is a bijective homomorphism that maps $G \to G$, meaning $\phi_g \in Aut(G)$

5a) Let G be an abelian group and $x, y \in G$ such that $|x| = m$ and $|y| = n$.

Suppose $|xy| = \phi$.

Observe that

$(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = e$, and
$(xy)^{\phi} = e$.

Given $|xy| = \phi$, $0 \le \phi \le mn$, and as $e^a = e$ for $a \in \mathbb{Z}$ and that e is the unique identity element of G, $\phi \mid mn$.

Let $d = \gcd(m,n)$ and $L = \operatorname{lcm}(m,n)$.

Recall that $mn = dL$ from Prop. 1.0.6; Thus $\phi \mid dL$.

Observe, however, that if $\phi \mid d$, then as $d \mid m$ and $m \mid L$, $\phi \mid L$.

Therefore $\phi = |xy|$ divides $\operatorname{lcm}(m,n)$.

5b) $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups with the identity being the only common element.

Therefore

$x^m \neq y^n$ unless $m=n$.

Consider $m=n$:

If $|x| = m = |y| = n$, then

$|xy| = xy^{\phi}$ for $\phi = m = n$ as

$xy^{\theta} = x^{\theta} = y^{\theta}$, where ϕ is the smallest element such that $x^{\theta} = y^{\theta} = e$.

Consider $m \neq n$:

Then $x^m \neq y^n$ and $(xy)^{\theta} = e$.