MATH 223 Practice 1 — September, 2024, Duration: 2.5 hours

*This document has **6 questions** on **X pages**, for a total of 80 points.*

First Name: Answer Key	Last Name: Answer Key
Student Number: Answer Key	Section: Answer Key
Signature: Answer Key	

Question:	1	2	3	4	5	6
Points:						
Total:	/80					

12 Marks 1. Carefully define each of the following:

(a) A subspace U of a vector space V over F

Solution:
A subspace $U \subseteq V$ is a vector space over F such that for all $u \in U, u \in V$.

(b) A linearly independent set of vectors $\{v_1, v_2, \ldots, v_n\} \subset V$ (You may assume V is finite dimensional and over a field F)

Solution:
A set of vectors $\{v_1, v_2, \ldots, v_n\}$ is linearly independent if there exists only the trivial solution $c_1, c_2, \ldots, c_n = 0 \in F$ to the equation $0 \in V = c_1v_1 + c_2v_2 + \ldots + c_nv_n$.

(c) A linear transformation $T : U \mapsto V$ where U, V are over the field F

Solution:
A linear transformation is a function $T : U \mapsto V$ such that for all $a, b \in U$ and $c \in F$, $T(a + b) = T(a) + T(b)$ and $T(ca) = cT(a)$.

(d) The null space of a matrix A

Solution:
The null space of a matrix A is the set of vectors v such that $Av = 0$, v is in the domain of the linear transformation represented by A and 0 is in the image.

(e) Similar matrices $A \sim B$

Solution:
We say $A \sim B$ if A and B are both $n \times n$ and there exists an $n \times n$ invertible matrix P such that $A = PBP^{-1}$.

(f) An inner product $\langle \cdot, \cdot \rangle : V \times V \mapsto F$ where V is a vector space over $F = \mathbb{R}$ or $\mathbb{C}$

Solution:
An inner product is a map $\langle \cdot, \cdot \rangle : V \times V \mapsto F$ where V is a vector space over $F = \mathbb{R}$ or $\mathbb{C}$ such that for all $x, y, z \in V$ and $a, b \in F$, $\langle x, y \rangle = \overline{\langle y, x \rangle}$, $\langle ax + by, z \rangle = a\langle x, z \rangle + b\langle y, z \rangle$ and if $x \neq 0 \in V$, $\langle x, x \rangle > 0 \in \mathbb{R}$.

20 Marks 2. This following section will ask you to prove some basic results about vector spaces.

(a) Prove that for any finite dimensional vector space V, W with the same dimension n over the same field F, there exists a bijective linear transformation $T : V \mapsto W$.

Solution 1:

Proof. Let V, W be over the same field F with dimension n. If $n = 0$, we can trivially map $0 \in V$ to $0 \in W$. If $n \neq 0$, we know V and W have bases $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$. Let $T : V \mapsto W$ be the transformation that maps every v_i to w_i for $0 \leq i \leq n$ and define $T(c_1v_1 + c_2v_2 + \ldots + c_nv_n) = c_1T(v_1) + c_2T(v_2) + \ldots c_nT(v_n)$. We show that this is well-defined. Given any $v \in V$, we note that v can only be uniquely represented as a linear combination of the basis vectors of V. Notice then $T(v) = c_1T(v_1) + c_2T(v_2) + \ldots c_nT(v_n) = c_1w_1 + c_2w_2 + \ldots c_nw_n$ which is a linear combination of the basis vectors of W, and thus $T(v)$ can only be expressed as a unique linear combination of the basis vectors of W. Thus, T is well-defined. By our definition of T, T is linear. Now we show that T is bijective.

- For injectivity, assume for the sake of contradiction that T is not injective. Then, there exists $v_\alpha \neq v_\beta$ such that $T(v_\alpha) = T(v_\beta)$. It follows that

$$v_\alpha = \alpha_1v_1 + \alpha_2v_2 + \ldots + \alpha_nv_n \neq \beta_1v_1 + \beta_2v_2 + \ldots + \beta_nv_n = v_\beta$$

  Now, obtain the expression $(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \ldots + (\alpha_n - \beta_n)v_n = v_\alpha - v_\beta$ and note that $v_\alpha - v_\beta \neq 0$, so there exists i where $0 \leq i \leq n$ such that $(\alpha_i - \beta_i) \neq 0$. Then, applying the transformation on both sides gives

$$(\alpha_1 - \beta_1)T(v_1) + (\alpha_2 - \beta_2)T(v_2) + \ldots + (\alpha_n - \beta_n)T(v_n) = T(v_\alpha - v_\beta)$$
$$(\alpha_1 - \beta_1)w_1 + (\alpha_2 - \beta_2)w_2 + \ldots + (\alpha_n - \beta_n)w_n = 0$$

  And since there exists $(\alpha_i - \beta_i) \neq 0$, it follows that this is a linear dependence relation on $\{w_1, w_2, \ldots, w_n\}$, contradicting the linear independence of a basis. Hence, T is injective.

- For surjectivity, let $w \in W$, so $w = c_1w_1 + c_2w_2 + \ldots + c_nw_n$. Then,

$$\begin{aligned} w &= c_1T(v_1) + c_2T(v_2) + \ldots + c_nT(c_n) \\ &= T(c_1v_1 + c_2v_2 + \ldots c_nv_n) \end{aligned}$$

  and $c_1v_1 + c_2v_2 + \ldots c_nv_n \in V$, so every $w \in W$ has a non-empty preimage as required.

Thus, there exists a bijective linear transformation between V and W as required. $\square$

Solution 2:

Proof. Let V, W be over the same field F with dimension n. If $n = 0$, we can trivially map $0 \in V$ to $0 \in W$. If $n \neq 0$, we know V and W have bases $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$. Let $T : V \mapsto W$ be the transformation that maps every v_i to w_i for $0 \leq i \leq n$ and define $T(c_1v_1 + c_2v_2 + \ldots + c_nv_n) = c_1T(v_1) + c_2T(v_2) + \ldots c_nT(v_n)$. We show that this is well-defined. Given any $v \in V$, we note that v can only be uniquely represented as a linear combination of the basis vectors of V. Notice then $T(v) = c_1T(v_1) + c_2T(v_2) + \ldots c_nT(v_n) = c_1w_1 + c_2w_2 + \ldots c_nw_n$ which is a linear combination of the basis vectors of W, and thus $T(v)$ can only be expressed as a unique linear combination of the basis vectors of W. Thus, T is well-defined. By our definition of T, T is linear. Now we show that T is bijective by constructing an explicit inverse. Let $T^{-1} : W \mapsto V$ be the transformation that maps every w_i to v_i for $0 \leq i \leq n$ and define $T^{-1}(c_1w_1 + c_2w_2 + \ldots + c_nw_n) = c_1T^{-1}(w_1) + c_2T^{-1}(w_2) + \ldots c_nT^{-1}(w_n)$. Let $v \in V$ so $v = c_1v_1 + c_2v_2 + \ldots + c_nv_n$. Then,

$$\begin{aligned} T^{-1}T(v) &= T^{-1}(c_1w_1 + c_2w_2 + \ldots + c_nw_n) \\ &= c_1T^{-1}(w_1) + c_2T^{-1}(w_2) + \ldots c_nT^{-1}(w_n) \\ &= c_1v_1 + c_2v_2 + \ldots + c_nv_n \\ &= v \end{aligned}$$

So T^{-1} is an inverse for T as required. Thus, there exists a bijective linear transformation between V and W. $\square$

(b) Let A be an $n \times n-$matrix with complex entries. Prove that $1 \leq$ geo. multi. of $\lambda \leq$ alg. multi. of λ where λ is an eigenvalue of A. (Hint: Jordan normal form)

Solution:

Proof. Let A be an $n \times n-$matrix with complex entries. Suppose the eigenspace of λ is 0 dimensional, so it is $\{0\}$. Then, there are no non-zero eigenvectors for λ, a contradiction to λ being an eigenvalue. Hence, the geometric and algebraic multiplicity of λ must be at least 1. All that remains is to show that the geometric multiplicity must be lesser than or equal to the algebraic multiplicity. Now, we know since A admits complex entries, then $A \sim B$ for some upper triangular matrix B, namely, the Jordan normal form of A, which has eigenvalues of A on the diagonal. Let λ be an eigenvalue with algebraic multiplicity k. Then, apply $-\lambda I$ to B. For all diagonal entries that are not λ, the diagonal entries become non-zero. Thus, rank$(B - \lambda I)$ is at least $n - k$. By rank theorem, nullity$(B - \lambda I)$ is at most k, so the result follows. $\square$

(c) Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be distinct eigenvalues for eigenvectors $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ for some $n \times n-$matrix A. Prove that $\{v_1, v_2, \ldots, v_n\}$ is linearly independent.

Solution:

Proof. Assume for the sake of contradiction that $\{v_1, v_2, \ldots, v_n\}$ is linearly dependent. Then, pick $v_i \in \{v_1, v_2, \ldots, v_n\}$ such that $v_i = c_1v_1 + c_2v_2 + \ldots c_{i-1}v_{i-1} + c_{i+1}v_{i+1} + \ldots + c_nv_n$, $\{v_1, v_2, \ldots, v_n\} \setminus \{v_i\}$ is linearly independent. Now, apply A to both sides of the equation and obtain

$$\lambda_i v_i = c_1\lambda_i v_1 + c_2\lambda_2 v_2 + \ldots c_{i-1}\lambda_{i-1}v_{i-1} + c_{i+1}\lambda_{i+1}v_{i+1} + \ldots + c_n\lambda_n v_n$$

Subtract λ_i times $v_i = c_1v_1 + c_2v_2 + \ldots c_{i-1}v_{i-1} + c_{i+1}v_{i+1} + \ldots + c_nv_n$ and obtain the following equation:

$$0 = c_1(\lambda_1 - \lambda_i)v_1 + \ldots c_{i-1}(\lambda_{i-1} - \lambda_i)v_{i-1} + c_{i+1}(\lambda_{i+1} - \lambda_i)v_{i+1} + \ldots + c_n(\lambda_n - \lambda_i)v_n$$

Since $\lambda_i \neq \lambda_{j \neq i}$, this is a linear dependence relation for $\{v_1, v_2, \ldots, v_n\} \setminus \{v_i\}$ which is a contradiction to this set being linearly independent. Hence, we have that $\{v_1, v_2, \ldots, v_n\}$ is linearly independent as required. $\square$

(d) Prove that a matrix A has an eigenvalue $\lambda = 0$ if and only if $\det(A) = 0$.

Solution:

Proof. We prove each direction in turn.

- For one direction, assume A has an eigenvalue $\lambda = 0$. Then, consider the characteristic polynomial for A when $\lambda = 0$, so

$$\begin{aligned} 0 = p(\lambda) &= a_n \cdot 0^n + a_{n-1} \cdot 0^{n-1} + \ldots + a_1 \cdot 0 + \det(A) \\ &= \det(A) \end{aligned}$$

  so $\det(A) = 0$ as required.
- For the other direction, assume $\det(A) = 0$ and consider the characteristic polynomial for λ. Then,

$$\begin{aligned} 0 = p(\lambda) &= a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda \\ &= \lambda(a_n\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \ldots + a_1) \end{aligned}$$

  so $\lambda = 0$ is a solution to the characteristic polynomial, $\lambda = 0$ is an eigenvalue for A as required.

This proves both directions and hence the result follows. □

12 Marks

3. Let $O_2(\mathbb{R})$ denote the set of $n \times n-$matrices that preserve the norm of vectors and angle between vectors, identically, the set of matrices such that $A^T = A^{-1}$.

   (a) Prove that for all $A \in O_2(\mathbb{R})$, $\det(A) = \pm 1$.

Solution:

Proof. Let $A \in O_2(\mathbb{R})$, so $A^T = A^{-1}$. It follows that

$$\begin{aligned} AA^T &= I \\ \det(A)\det(A^T) &= \det(I) \\ \det(A)\det(A) &= 1 \\ (\det(A))^2 &= 1 \end{aligned}$$

so $\det(A) = \pm 1$ as required. □

(b) Let $SO_2(\mathbb{R})$ be the set of matrices in $O_n(\mathbb{R})$ such that they have a determinant of 1. Prove that $SO_2(\mathbb{R})$ is the set of rotation matrices for $\mathbb{R}^2$. (Hint: Consider what any $A \in SO_2(\mathbb{R})$ does to e_1 and e_2)

Solution:

Proof. Let $A \in SO_2(\mathbb{R})$. We prove both inclusions in turn.

- For one inclusion, Since $A \in O_n(\mathbb{R})$, A must preserve the norm of v for any $v \in \mathbb{R}^2$. Let e_1, e_2 be the basis vectors of $\mathbb{R}^2$. Then, the possible points of Ae_1 and Ae_2 must lie on the unit circle. Since $A \in SO_2(\mathbb{R})$, $\det(A) = 1$ so the orientation of e_1 relative to e_2 is preserved. Since the angle between e_1 and e_2 is also preserved from $A \in O_n(\mathbb{R})$, it follows that A must be a rotation matrix as required, so $SO_2(\mathbb{R}) \subseteq \{\text{rotation matrices}\}$.
- For the other inclusion, let A be a rotation matrix. Then,

$$\begin{aligned} AA^T &= \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix} \cdot \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix} \\ &= \begin{pmatrix} \cos^2 x + \sin^2 x & \sin\cos x - \sin\cos x \\ \cos\sin x - \cos\sin x & \sin^2 x + \cos^2 x \end{pmatrix} \\ &= I \end{aligned}$$

So $A^T = A^{-1}$, $A \in O_2(\mathbb{R})$. Also notice that

$$\begin{aligned} \begin{vmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{vmatrix} &= \cos^2 x + \sin^2 x \\ &= 1 \end{aligned}$$

so $\det(A) = 1, A \in SO_2(\mathbb{R})$ as required. $\square$

This proves both inclusions so $SO_2(\mathbb{R})$ must be the set of rotation matrices in $\mathbb{R}^2$ as required.

(c) Prove that for all $A \in O_2(\mathbb{R}) \backslash SO_2(\mathbb{R})$, one of the eigenvalues of A is 1 and the other is -1.

Solution:

Proof. Let $A \in O_2(\mathbb{R}) \backslash SO_2(\mathbb{R})$ so $\det(A) = -1$. Now assume for the sake of contradiction that the eigenvalues of A are not real, so the roots of the characteristic polynomial are not real. Then, by the fundamental theorem of algebra, the roots of the characteristic polynomial, i.e. eigenvalues of A, are complex conjugates $z, \bar{z}$. Notice, $z\bar{z} \geq 0$, and we know the product of eigenvalues will yield the determinant, but the determinant is -1, a contradiction. Hence, the eigenvalues of A must be real. It follows that $\lambda_1 = \pm 1, \lambda_2 = \pm 1$ since $A \in O_2(\mathbb{R})$ and thus A must preserve the norm of the vectors. Once again, since the product of eigenvalues will yield the determinant, $\lambda_1 \lambda_2 = -1$ so one of λ_1, λ_2 must be 1 and the other must be -1. Hence, the result follows. $\square$

10 Marks

4. Let $GL_n(\mathbb{R})$ denote the set of $n \times n$ invertible matrices.

   (a) Let $\sim$ be a relation on $GL_n(\mathbb{R})$ where $A \sim B$ if and only if $\det(A) = \det(B)$. Prove that $\sim$ is an equivalence relation.

Solution:

Proof. We prove that $\sim$ is reflexive, symmetric, and transitive.

- For reflexivity, we have $\det(A) = \det(A)$ so $A \sim A$.
- For symmetry, assume $A \sim B$, so $\det(A) = \det(B)$. Then, $\det(B) = \det(A)$ so $B \sim A$ as required,
- For transitivity, assume $A \sim B$ and $B \sim C$, so $\det(A) = \det(B)$ and $\det(B) = \det(C)$. It follows that $\det(A) = \det(C)$ so $A \sim C$.

This proves that $\sim$ is reflexive, symmetric, and transitive so $\sim$ is an equivalence relation on $GL_n(\mathbb{R})$ as required. $\square$

(b) Prove that $O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$ and $O_n(\mathbb{R})$ is closed under matrix multiplication. Prove or disprove that for all $A \in GL_n(\mathbb{R})$ and for all $B \in O_n(\mathbb{R})$, $ABA^{-1} \in O_n(\mathbb{R})$.

Solution:

Proof. Let $A \in O_n(\mathbb{R})$. Then, $\det(A) = \pm 1 \neq 0$, so $A \in GL_n(\mathbb{R})$. Thus, $O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. Let $A, B \in O_n(\mathbb{R})$. Then, $(AB)^T = B^T A^T$ so $(AB)(AB)^T = ABB^T A^T = I$, so $(AB)^T = (AB)^{-1}$. Hence, $O_n(\mathbb{R})$ is closed under matrix multiplication. $\square$

We disprove that for all $A \in GL_n(\mathbb{R})$ and for all $B \in O_n(\mathbb{R})$, $ABA^{-1} \in O_n(\mathbb{R})$.

Disproof. Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ so $A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}$ and $B = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$, which is the rotation matrix for rotating by $\pi/4$ radians counterclockwise. Then,

$$\begin{aligned} ABA^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \\ &= \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \end{aligned}$$

However,

$$\begin{aligned} (ABA^{-1})(ABA^{-1})^T &= \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & \sqrt{2} \\ -1/\sqrt{2} & \sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \\ &\neq I \end{aligned}$$

so $ABA^{-1} \notin O_n(\mathbb{R})$. $\square$

$\boxed{\text{12 Marks}}$ 5. Let $\langle A \rangle = \left\{ B : B = A^k, \det(A) \neq 0, k \in \mathbb{Z} \right\}$ where A is an $n \times n$-matrix and assume $\langle A \rangle$ is closed under matrix multiplication.

(a) Prove that for all $B, C \in \langle A \rangle, BC = CB$. Prove that if $\langle A \rangle$ is finite, $\det(A) = \pm 1$.

Solution:

Proof. Let $B, C \in \langle A \rangle$. Then, $B = A^k$ and $C = A^\ell$ for some $k, \ell \in \mathbb{Z}$. It follows that $BC = A^k A^\ell = A^{k+\ell} = A^\ell A^k = CB$ so $BC = CB$ as required. For the second part, notice A is invertible and $\langle A \rangle$ is finite. We prove the contrapositive. Assume $\det(A) \neq \pm 1$. Then, $\det(A^n) = (\det(A))^n \neq 1$ for all $n \in \mathbb{N}$, so $\langle A \rangle$ is infinite. This proves the contrapositive and thus the original statement. $\square$

(b) Prove that if m is the smallest positive integer such that $B^m = I$ for all $B \in \langle A \rangle$, then $\langle A \rangle$ has m elements.

Solution:

Proof. Let m be as stated. Notice $I \in \langle A \rangle$ by definition. By Euclidean division, we know for all $B \in \langle A \rangle, B = A^k = A^{qm+r}$ for some $0 \leq r < m$ and thus $B = A^{qm}A^r = IA^r = A^r$. Since $A \in \langle A \rangle$, by closure under multiplication, we know that for all r such that $1 \leq r < m$, $A^r \in \langle A \rangle$, and also $I = A^0 \in \langle A \rangle$. Hence, there are at least m elements in $\langle A \rangle$. Notice $A^{m-1} \cdot A = A^m = I$ so by our choice of m, there can be at most m elements. It follows that there must be exactly m elements as required. $\square$

(c) Prove that if $\langle A\rangle$ is finite with k elements, then every $\langle B\rangle \subseteq \langle A\rangle$ has d elements such that $d \mid k$, and that there could only be one $\langle B\rangle$ for each divisor of k. You may use the fact that $\langle A\rangle = \left\{I, A, A^2, \ldots, A^{k-1}\right\}$ and that $|\langle A^s\rangle| = \frac{n}{\gcd(n,s)}$ for all $s \neq 0 \in \mathbb{Z}$. (Note $\langle B\rangle$ also has to be closed under multiplication)

Solution:

Proof. Assume $\langle A\rangle$ is finite with k elements and let $\langle B\rangle \subseteq \langle A\rangle$ be closed under multiplication. Notice if $\langle B\rangle = \{I\}$ then we are done. Hence, assume $\langle B\rangle \neq \{I\}$ and let m be the smallest natural number such that $A^m \in \langle B\rangle$ for some $A^p \in \langle B\rangle$, $0 \leq p < k$. Then, by Euclidean division, $A^p = A^{qm+r}$ where $0 \leq r < m$. Notice $A^r = A^{-qm+p}$ and $A^{-qm}, A^p \in \langle B\rangle$. By our choice of m, $r = 0$ as otherwise we have that $r < m$ and $A^r \in \langle B\rangle$. Hence, it follows that $A^p = A^{qm}$ for some $q \in \mathbb{Z}$ and thus $\langle B\rangle = \langle A^m\rangle$, which has m elements. Now we show $m \mid k$. For $A^k = I$, by Euclidean division, $A^k = A^{qm+r}$ where $0 \leq r < m$. Notice we have $A^{qm+r} \in \langle B\rangle$ so $A^r = A^{-qm} \in \langle B\rangle$. By our choice of m, $r = 0$ as otherwise we have an $r < m$ such that $A^r \in \langle B\rangle$. It follows that $k = qm$ so $m \mid k$. Finally, we show that $\langle B\rangle$ is unique for each divisor of k. Once again, if $\langle B\rangle = \{1\}$, we are done, so assume $\langle B\rangle \neq \{1\}$. Then, assume $p \mid k$ for some $p \in \mathbb{Z}$. Notice $|\langle A^{k/p}\rangle| = \frac{k}{\gcd(k,k/p)} = \frac{k}{k/p} = p$. We show that if we have another $\langle B\rangle$ with the same number of elements, $\langle B\rangle = \langle A^{k/p}\rangle$. Assume $|\langle A^q\rangle| = p$ for some $q \in \mathbb{Z}$ such that $q \mid k$. Then, $p = \frac{k}{\gcd(k,q)} = \frac{k}{q}$ so it follows that $q = \frac{k}{p}$ and thus $\langle A^{k/p}\rangle = \langle A^q\rangle$. Hence, for any divisor of k, we have one unique $\langle B\rangle$ as required. □

14 Marks

6. Let A be a $n \times n$ permutation matrix, so every column of A has one entry that is 1 and every row of A has one entry that is 1, and the matrix is 0 everywhere else, and let A_n be the set of $n \times n$ permutation matrices.

(a) Prove that if $n \geq 2$, then there exists a permutation matrix $A \neq I \in A_n$ such that $A^k = I$ for some $k \in \mathbb{N}$.

Solution:

Proof. We proceed on induction for n.

- For the base case, let $n = 2$. Then, notice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a permutation matrix and $A^2 = I$, so $A^k = I$ for some $k \in \mathbb{N}$.
- For the inductive step assume there exists a permutation matrix $A \neq I \in A_n$ such that $A^k = I$ for some $k \in \mathbb{N}$. Then, take such A and let B be the $(n+1) \times (n+1)-$matrix where the top left corner of B is A, and everywhere else on the remaining row/column is 0 except for the bottom right entry, which is 1. Observe that B is a permutation matrix. It follows that

$$B^k = \left(\begin{array}{c|c} \begin{matrix} & \\ & A \\ & \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \cdots\cdots 0 & 1 \end{array}\right)^k = \left(\begin{array}{c|c} \begin{matrix} & \\ & A^k \\ & \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \cdots\cdots 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} \begin{matrix} & \\ & I \\ & \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \cdots\cdots 0 & 1 \end{array}\right) = I$$

  so the inductive step holds.

By the principle of mathematical induction, the result follows for all $n \geq 2$. $\square$

(b) Let S_n be the set of bijections from $\{1, 2, 3, \ldots, n\}$ to itself. Construct a bijection $\varphi : S_n \mapsto A_n$ between the set of permutation matrices such that for all $\sigma, \tau \in S_n$, $\varphi(\sigma \circ \tau) = \varphi(\sigma)\varphi(\tau)$.

Solution:

Proof. Let S_n and A_n be as stated. Then, let each permuted element $j \mapsto i$ where $1 \leq i, j \leq n$ correspond to a 1 in the $i-$th row in the $j-$th column, and let the rest of the column be zero. Notice that since for all $\sigma \in S_n$, σ is bijective, it follows that σ is injective so there does not exist any rows with more than one 1. Since σ is also surjective, we know every column contains 1 and by the well-definition of a function, we know each column cannot contain more than one 1. It follows that this produces a permutation matrix A. Let φ be the function that maps every σ to its corresponding permutation matrix A_σ as shown above. Then, for all $\sigma, \tau \in S_n$, notice

$$\varphi(\sigma)\varphi(\tau)(x) = \varphi(\sigma)A_\tau(x) = A_\sigma A_\tau(x) = (A_\sigma A_\tau)(x)$$

and from the permutation of column vectors of τ by σ, we have $(A_\sigma A_\tau)(x) = A_{\sigma\circ\tau} = \varphi(\sigma \circ \tau)$ so $\varphi(\sigma \circ \tau) = \varphi(\sigma)\varphi(\tau)$ as required. As for bijections, notice we can find an inverse $\varphi^{-1} : A_n \mapsto S_n$ where for every $j-$th column, on the $i-$th row that contains a one, we map that to a permutation $j \mapsto i$. Since we constructed an inverse, this gives a bijection as required. $\square$

(c) Prove that if G is a non-empty finite set of $m \times m-$matrices with real entries such that for all $B, C \in G$, $BC^{-1} \in G$, then, there exists $n \in \mathbb{N}$ such that one can find an injection $f : G \mapsto A_n$ where for all $B, C \in G$, $f(BC) = f(B)f(C)$.

Solution:

Proof. We found a bijection $\varphi : S_n \mapsto A_n$ such that $\varphi(\sigma \circ \tau) = \varphi(\sigma)\varphi(\tau)$ for all $\sigma, \tau \in S_n$ so it suffices to find an injection $g : G \mapsto S_n$ where for all $B, C \in G$, $f(BC) = f(B)f(C)$, and we can just take the composition $f = \varphi \circ g$. Since G is non-empty, we know there exists $B \in G$ and notice by its definition, $BB^{-1} \in G$ so $I \in G$. Applying the definition again yields $IB^{-1} = B^{-1} \in G$ so we know G has an identity element and every element of G has an inverse. For all $B \in G$, construct the map $B_L : G \mapsto G$ such that for all $X \in G$, $B_L(X) = BX$. We show this map is a bijection from G to itself. This is clear since we can construct the inverse ${B^{-1}}_L$ where ${B^{-1}}_L(B_L(X)) = {B^{-1}}_L(BX) = B^{-1}BX = X$. Let $f : G \mapsto S_n$ be the map that sends each B to B_L. We show g is injective. Notice if $B_L = C_L$, then $B_L X = C_L X$ for all $X \in G$ so $B = B_L \cdot 1 = C_L \cdot 1 = C$. Thus, g is injective. For checking $g(BC) = g(B)g(C)$, notice $g(BC)X = (BC)_L X = BCX = B(C(X)) = B_L C_L X = g(B)g(C)X$ so $g(BC) = g(B)g(C)$ as required. Taking the composition $f = \varphi \circ g$ gives an injection $f : G \mapsto A_n$ as required. ☐