THE UNIVERSITY OF SYDNEY

MATH2022 LINEAR AND ABSTRACT ALGEBRA

Semester 1 **Exercises for Week 2 (beginning 12 March)** 2018

Important Ideas and Useful Facts:

(i) Common notation: The most common arithmetics, under usual addition and multiplication, are formed by the following sets:

(a) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, the set of *natural* numbers;

(b) $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$, the set of *integers*;

(c) $\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\}$, the set of *rational* numbers;

(d) $\mathbb{R}$, the set of *real* numbers;

(e) $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, the set of *complex* numbers, where $i = \sqrt{-1}$.

(ii) Arithmetic of integers modulo n: Let n be a positive integer. Then $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ forms an arithmetic with respect to *addition and multiplication modulo n*, which are the usual operations of addition and multiplication as integers, followed by taking the remainder after division by n.

(iii) Fields and scalars: A *field* F is an arithmetic with addition and multiplication, having at least two distinct elements 0 and 1, such that

(a) addition and multiplication are associative and commutative;

(b) multiplication distributes over addition;

(c) 0 and 1 behave as additive and multiplicative identity elements respectively;

(d) every element of F has an additive inverse (negative) and every nonzero element of F has a multiplicative inverse.

Elements of a field are called *scalars*. The most common fields are $F = \mathbb{Q}$, $F = \mathbb{R}$, $F = \mathbb{C}$ and $F = \mathbb{Z}_p$ where p is a prime number (in particular $F = \mathbb{Z}_2 = \{0, 1\}$).

(iv) Matrices: A *matrix* is an array of objects or numbers, called *entries*. Entries will typically be scalars drawn from some underlying field. If a matrix M has m rows and n columns then we say that M is $m \times n$. We call a matrix M *square* if M is $n \times n$ for some n. A matrix consisting of one row is called a *row vector*. A matrix consisting of one column is called a *column vector*.

(v) Addition, subtraction and scalar multiplication of matrices: To *add* or *subtract* matrices of the same size, simply add or subtract the corresponding entries. To form the *negative* of a matrix, take the negatives of its entries. To *multiply a matrix by a scalar*, multiply its entries by the scalar.

(vi) Zero and identity matrices: The *zero matrix* has all of its entries equal to 0, denoted by 0 or $0_{m\times n}$. The *identity matrix* is a square matrix with *diagonal* entries equal to 1 and all entries off the diagonal equal to 0, denoted by I or I_n.

(vii) Matrix multiplication: If A is $m \times n$ and B is $n \times p$ then the *matrix product* AB is defined and is $m \times p$. The (i, k)-entry of AB is the "dot product" of the ith row of A with the kth column of B, which can be expressed using sigma notation:

$$\sum_{j=1}^{n} a_{ij}b_{jk} \;=\; a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk}$$

where a_{ij}, b_{jk} denote typical (i, j) and (j, k)-entries of A and B respectively.

(viii) General laws of matrix arithmetic: If A, B, C are matrices of appropriate sizes for which the expressions make sense, and λ and μ are scalars, then the following properties hold:

$$A + B = B + A\,, \qquad (A + B) + C = A + (B + C)\,, \qquad A + 0 = 0 + A = A\,,$$
$$-(-A) = A\,, \qquad A + (-A) = A - A = 0\,, \qquad \lambda(\mu A) = (\lambda\mu)A\,,$$
$$\lambda(A + B) = \lambda A + \lambda B\,, \qquad (\lambda + \mu)A = \lambda A + \mu A\,, \qquad IA = AI = A\,,$$
$$(AB)C = A(BC)\,, \qquad A(B + C) = AB + AC\,, \qquad (A + B)C = AC + BC\,,$$
$$\lambda(BC) = (\lambda B)C = B(\lambda C)\,, \qquad 0A = 0 = A0\,.$$

(ix) Matrix transpose and symmetric matrices: The *transpose* of a matrix $A = [a_{ij}]_{m\times n}$ is a matrix $A^\top = [b_{ij}]_{n\times m}$ where $b_{ij} = a_{ji}$ for $i = 1,\ldots,n$ and $j = 1,\ldots,m$, that is, $A^\top$ is obtained from A by writing all of the rows as columns (or, equivalently, all of the columns as rows). A matrix A is called *symmetric* if $A^\top = A$ (so necessarily A is square). If A, B and C are matrices for which the following expressions make sense, then

$$(A + B)^\top \;=\; A^\top + B^\top\,,\;\; (BC)^\top \;=\; C^\top B^\top\,,\;\; (A^\top)^\top \;=\; A\,.$$

(x) Invertible matrices: The *inverse* of a matrix A is a matrix A^{-1} such that

$$AA^{-1} \;=\; A^{-1}A \;=\; I_n$$

for some positive integer n. Only square matrices have inverses. When it exists, A^{-1} is unique. A matrix is *invertible* if its inverse exists. If A and B are invertible matrices of the same size then AB and A^{-1} are invertible and

$$(AB)^{-1} \;=\; B^{-1}A^{-1} \quad \text{and} \quad (A^{-1})^{-1} \;=\; A\,.$$

(xi) Groups: A *group* is a (nonempty) set G with an associative binary operation, typically denoted by justaposition, containing an element e that acts as a two-sided identity element, that is,

$$ge \;=\; eg \;=\; g \quad \text{for all } g \in G,$$

and such that all elements of G are invertible with respect to e, that is, for all $g \in G$, there exists some $h \in G$ such that

$$gh \;=\; hg \;=\; e\,,$$

in which case we write $h = g^{-1}$. If the binary operation is commutative then we say that G is *abelian*.

(xii) Important and common examples of groups:

(a) If F is a field then $(F, +)$, the field under addition, and $(F\backslash\{0\}, \cdot)$, the set of nonzero elements under multiplication, are abelian groups with identity elements 0 and 1 respectively.

(b) If n is a positive integer then $(\mathbb{Z}_n, +)$ is a *cyclic* group, generated by the element 1 under addition (with 0 as the additive identity element).

(c) If F is a field and $n \geq 1$ then $\mathrm{GL}_n(F) = \{\text{invertible } n \times n \text{ matrices over } F\}$ is a group under matrix multiplication, called the *general linear group*, which is nonabelian if $n \geq 2$.

(d) If X is a set then $S_X = \{\text{permutations of } X\}$ is a group under composition of permutations, called the *symmetric group*, which is nonabelian if $|X| \geq 3$.

Questions labelled with an asterisk are suitable for students aiming for a distinction or higher.

Tutorial Exercises:

1. Consider the following matrices:

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \qquad B = \begin{bmatrix} -6 & 3 \\ 4 & 1 \end{bmatrix} \qquad C = \begin{bmatrix} 2 & 4 & 5 \end{bmatrix}$$

$$D = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \qquad E = \begin{bmatrix} 1 & 2 & 0 & 4 \\ 6 & -1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{bmatrix} \qquad F = \begin{bmatrix} 0 \\ 1 \\ 2 \\ -3 \end{bmatrix}$$

Evaluate the following expressions over $\mathbb{R}$, $\mathbb{Z}_7$ and $\mathbb{Z}_{13}$:

(a) $2A$ (b) $-B$ (c) $A+B$ (d) $A-B$ (e) $A^2 = AA$

(f) AB (g) BA (h) CD (i) $EF-3D$ (j) CEF

2. Explain why the matrix equations

$$AB = BA = I_n$$

imply that A and B are square matrices of the same size.

3. Verify directly that if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $ad-bc \neq 0$ then $AB = BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ where $B = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, so that A^{-1} exists and equals B. What simplification occurs if entries come from $\mathbb{Z}_2$?

4. Consider the following matrices over $\mathbb{R}$, where θ is a real number:

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \qquad T_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

Verify the following for all $\theta, \phi \in \mathbb{R}$ and positive integers n:

(a) $T_\theta^{-1} = T_\theta$ (b) $R_\theta R_\phi = R_{\theta+\phi}$ (c) $R_{2\pi} = I = R_{2\pi/n}^n$

(d) $T_\theta T_\phi = R_{\theta-\phi}$ (e) $T_\phi R_\theta T_\phi = R_{-\theta} = R_\theta^{-1}$

5. If today is Monday, what day of the week will it be after 100^{100} days have elapsed?

6.* It has been predicted that a meteor will strike the earth after 100^{100} hours have elapsed from 9 am next Monday. At what time, and on what day of the week, do you predict the meteor will strike?

7.* Consider the matrix $M = \begin{bmatrix} 3 & -1 \\ 4 & -1 \end{bmatrix}$.

(a) Verify that $M^2 = 2M - I$.

(b) Deduce that $M^3 = 3M - 2I$ and guess a general formula for powers of M. Verify your guess is correct by induction.

(c) Evaluate M^5, M^{10}, M^{100} and M^{-100}.

Further Exercises:

8. Evaluate the following when they exist in $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_9$ and $\mathbb{Z}_{24}$:

$$\frac{1}{2}, \ \frac{1}{3}, \ \frac{1}{4}, \ \frac{3}{5}, \ \frac{5}{6}$$

9. Explain briefly why the associative law for matrix multiplication implies that every square matrix commutes with its square.

10. Find a 2×2 matrix M over any field F such that $M^2 = 0$, the zero matrix, but all entries of M are nonzero.

11. Explain briefly why a square matrix with a row or column of zeros cannot be invertible.

12. Suppose that A and B are invertible square matrices of the same size. Verify that

$$\big((AB)^{-1}\big)^\top = \big(A^{-1}\big)^\top \big(B^{-1}\big)^\top \qquad \text{and} \qquad \big((AB)^\top\big)^{-1} = \big(A^\top\big)^{-1} \big(B^\top\big)^{-1}.$$

13.* Let G be a group with identity element e.

(a) Verify that if $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$.

(b) Verify that if $a^2 = e$ for all $a \in G$ then G is abelian.

(c) Prove that G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

14.* A collection G of square matrices over a field F forms a group under multiplication. Prove either that every matrix in G is invertible or that every matrix in G is not invertible.

15.* Let F be a field.

(a) Which part of the definition of a field guarantees that $0 + 0 = 0$. Explain why the zero is unique. Explain also why the multiplicative identity element 1 is unique.

(b) Explain why $-a$, the negative of $a \in F$, is unique and why a^{-1}, the multiplicative inverse of a, which exists when $a \neq 0$, is unique.

(c) Use distributivity and other parts of the definition of a field to explain why $0a = 0$ for all $a \in F$.

(d) Explain why the equation $ab = 0$ implies $a = 0$ or $b = 0$ for $a, b \in F$. Deduce that $\mathbb{Z}_n$ is not a field if n is a composite integer.

(e) Use parts (b) and (c) to deduce that $-(ab) = (-a)b = a(-b)$ and $(-a)(-b) = ab$ for all $a, b \in F$.

16.* Recall that addition and multiplication in $\mathbb{Z}_n = \{0, 1, \ldots, n\}$ are as in $\mathbb{Z}$ except that each operation is completed by taking the remainder after division by n. Prove carefully that addition and multiplication in $\mathbb{Z}_n$ are associative.