DMLA Term 2

1 Divisibility and Primes

The notation $a|b$ means that a is a factor of b

1.1 Properties of divisibility

The following statements about divisibility hold

1. if $a|b$ then $a|(bc)$ for all c
2. If $a|b$ and $b|c$ then $a|c$
3. If $a|b$ and $a|c$ then $a|(sb + tc)$ for all s, t
4. For all $c \neq 0$, $a|b$ iff $(ca)|(cb)$

1.2 The division algorithm

Let a be an integer and d a positive integer. Then there exist unique numbers q and r, with $0 \leqslant r < d$, such that $a = qd + r$
In the equality in the division algorithm

- q is the quotient, denoted qent(a, d) or a div d, and
- r is the remainder, denoted rem(a, d) or a mod d

1.3 Fundamental properties of primes

1.3.1 Fundamental theorem of Arithmetic

Every positive integer $n > 1$ can be uniquely represented as $n = p_1 \cdot p_2 \cdots p_k$ where the numbers $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$ are all prime

1.3.2 The infinitude of primes

There are infinitely many prime numbers

1.3.3 The prime number theorem

The number of primes not exceeding x approaches $x/ln(x)$ as x grows infinitely

1.4 The greatest common divisor

A linear combination of a and b is any number in the form $sa + tb$

gcd(a,b) is equal to the smallest positive linear combination of a and b

1.5 Properties of the GCD

The following statements hold

1. $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$
2. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$
3. If $a|bc$ and $\gcd(a, b) = 1$ then al c

1.6 Euclid's Algorithm

If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$

1.7 Relatively prime numbers

Two numbers a and b are called relatively prime if $\gcd(a, b) = 1$

2 Modular Arithmetic

2.1 Basic Modular Arithmetic

If a,b are integers and m is a positive integer then a is congruent to b modulo m iff $m|(a-b)$. Notation

$$a \equiv b(\mod m)$$

If a,b,m are integers and $m > 0$ then $a \equiv b(\mod m)$ iff $\text{rem}(a, m) = \text{rem}(b, m)$
Let m be a positive integer and let $a \equiv b(\mod m)$ and $c \equiv d(\mod m)$. Then

$$a + c \equiv b + d(\mod m) \qquad \text{and} \qquad ac = bd(\mod m)$$

2.2 Multiplicative inverses

The easiest way to solve equation $ax = b$ is to multiply both parts by a^{-1}
We can't do this within integers, but we often can when working modulo m
Call $\bar{a}$ the (multiplicative) inverse of a modulo m if $\bar{a}a \equiv 1 \mod m$
Multiplicative inverses do not always exist

If $\gcd(a, m) = 1$ then the inverse of a modulo m exists, and is unique

2.3 The Chinese Remainder theorem

Let $m_1, ..., m_m$ be pairwise relatively prime positive integers and $a_1, ..., a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \,(\text{mod} m_1) \\ x &\equiv a_2 \,(\text{mod} m_2) \\ &\vdots \\ x &\equiv a_n \,(\text{mod} m_n) \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. That is, there is a unique solution x with $0 \leqslant x < m$ and every other solution is congruent to x modulo m

2.4 Fermat's Little Theorem

If p is a prime and a is not a multiple of p then $a^{p-1} \equiv 1 \mod p$. Furthermore, for every integer a, $a^p \equiv a \mod p$

2.5 Euler's Theorem

Remember Euler's ϕ-function: $\phi(n)$ is the number of integers $1 \leqslant a \leqslant n$ that are relatively prime with n. Euler's theorem generalises Fermat's Little Theorem to non-prime moduli

If n is a positive integer and $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \mod n$

2.6 Computing Euler's ϕ-function

If m_1 and $m_2$are relatively prime then $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$. If p is prime then $\phi(p^k) = p^k - p^{k-1}$

3 Matrices and Determinants

3.1 Matrices

A matrix is a rectangular array of numbers. The numbers in the array are called the entries of the matrix. The entry in row i and column j is denoted by a_{ij}

Assuming that the sizes of the matrices are such that the operations can be preformed, the following rules are valid:

1. $A + B = B + A$
2. $A + (B + C) = (A + B) + C$
3. $A(BC) = (AB)C$
4. $A(B \pm C) = AB \pm AC$
5. $(B \pm C)A = BA + CA$
6. $\alpha(B \pm C) = \alpha B \pm \alpha C$
7. $(\alpha \pm \beta)A = \alpha A \pm \beta A$
8. $\alpha(\beta A) = (\alpha\beta)A$
9. $\alpha(BC) = (\alpha B)C = B(\alpha C)$

3.2 Matrix Transpose

If A is an $m \times n$ matrix then the transpose of A is the $n \times m$ matrix A^T such that the ith row of A is the ith column of A^T

3.3 Minors and Cofactors

If A is a square matrix of order n, then the minor of the entry a_{ij} denoted by M_{ij}, is the determinant of the matrix (of order n-1) obtaining from A by removing its ith row and jth column
The number $C_{ij} = (-1)^{i+j} M_{ij}$ is called the cofactor of a_{ij}

3.4 Determinants

If A is an $n \times n$ matrix then the determinant of A can be computed by any of the following cofactor expansions along the ith row and jth column respectively

$$\det(A) = a_{i1}C_{i1} + a_2C_2 + \ldots + a_{in}C_{in}$$
$$\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \ldots + a_{nj}C_{nj}$$

Let

$$A = \begin{pmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{pmatrix}$$

Compute $\det(A)$ by cofactor expansion along the first row

$$\begin{vmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{vmatrix} = 3 \cdot \begin{vmatrix} -4 & 3 \\ 4 & -2 \end{vmatrix} - 1 \cdot \begin{vmatrix} -2 & 3 \\ 5 & -2 \end{vmatrix} + 0 \cdot \begin{vmatrix} -2 & -4 \\ 5 & -4 \end{vmatrix} =$$

$$3 \cdot (-4) - 1 \cdot (-11) + 0 = -1$$

4 Linear Systems

4.1 Systems of linear systems

- A linear equation in n variables $x_1, \ldots, x_n$ is an equation of the form

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

Where the a_i's and b are constants and not all a_i's are equal to 0

- A finite set of linear equations is called a system of linear equations, or simply a linear system

4.2 Linear systems with different numbers of solutions

One solution - Can cancel down to x or y equalling 1 value
No solutions - Cancels down to a contradiction
Infinitely many solutions - Cancels down to a number equals a number

4.3 Matrix form of a linear system

A linear system

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots &= \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

can be written in a matrix form as $Ax = b$ where

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and } \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

The matrix A is called the coefficient matrix of the system
If A is (square and) invertible then the solution can be found as $x = A^{-1}b$

4.4 The augmented matrix and elementary row operations

The augmented matrix of a linear system is the matrix

$$(A|\mathbf{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right)$$

The basic method for solving a linear system is to perform algebraic operations on the system that:

(a) Do not alter the equation set

(b) Produce increasingly simpler systems

Typically the operations are

- Multiply an equation through by a non zero constant
- Interchange two equations
- Add a constant times one equation to another

What we want to do with this is to produce the identity matrix on the left, as then we can link variables and values

4.5 Homogeneous Linear Systems

A linear system $Ax = b$ is homogeneous if b is all 0s
Such a system has a trivial solution: x is all 0s. Any other solution is called non-trivial

If a homogeneous linear system has n variables and the reduced row echelon form of its augmented matrix has r non-0 rows then the system has n-r free variables
A homogenous linear system with more variables than equations has infinitely many solutions

5 Matrix Inversion

5.1 Elementary matrices

Every elementary matrix E is invertible, and the inverse is also elementary

5.2 Invertible matrices

If A is an $n \times n$ matrix, then the following are equivalent

1. A is invertible
2. The linear system $Ax = 0$ has only the trivial solution $x = 0$
3. The reduced row echelon form of A is I_n
4. A can be expressed as a product of elementary matrices
5. $\det(A) \neq 0$

5.3 Inversion algorithm

1. Write the matrix $[A|I_n]$
2. Apply elementary row operations to the whole matrix to transform its left half to reduced row echelon form
3. If this form is not in I_n, then the matrix is not invertible
4. Otherwise, the obtained matrix is $[I_n|A^{-1}]$

5.4 Determinants and elementary row operations

Let A be a $n \times n$ matrix

- If B is obtained from A by multiplying a row by a constant k then $\det(B) = k \cdot \det(A)$
- If B is obtained from A by interchanging two rows then $\det(B) = -\det(A)$
- If B is obtained from A by adding a multiple of one row to another row then $\det(B) = \det(A)$

5.5 Properties of determinants

If A and B are square matrices of the same size then $\det(AB) = \det(A)\det(B)$
If A is invertible then $\det(A^{-1}) = 1/\det(A)$

5.6 Inverting a matrix via cofactors/adjoint

- $C_{ij} = (-1)^{i+j}M_{ij}$ is called the cofactor of a_{ij}
- The matrix where all cofactors are calculated is called the matrix of cofactors of a (cof(A))
- The transpose of cof(A) is the adjoint of A (adj(A))

$$\text{If A is an invertible matrix then } A^{-1} = \frac{1}{\det(A)} \cdot adj(A)$$

6 Vector spaces and linear independence

6.1 Norm and dot product in $\mathbb{R}^n$

- The length of a vector $v \in \mathbb{R}^n$ is defined by the formula

$$||\mathbf{v}|| = \sqrt{v_1^2 + v_2^2 + \ldots + v_n^2}$$

- For any vector v, the vector $\frac{1}{||v||}v$ is a unit vector in the same direction as v
- The dot product (aka inner product) of vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in $\mathbb{R}^n$ is defined as

$$u \cdot v = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n$$

6.2 Properties of dot product

If u,v and w are vectors in $\mathbb{R}^n$ then the following properties hold

- $u \cdot v = v \cdot u$ (symmetry)
- $u \cdot (v + w) = u \cdot v + u \cdot w$ (Distributivity)
- $k(u \cdot v) = (ku) \cdot v$ (Homogeneity)
- $v \cdot v \geqslant 0$ and $v \cdot v = 0$ iff $v = 0$ (Positivity)

If u and v are vectors in $\mathbb{R}^n$ then $u \cdot v \leqslant ||u|| \cdot ||v||$
If u and v are vectors in $\mathbb{R}^n$ then $||u + v|| \leqslant ||u|| + ||v||$

6.3 Orthogonality in $\mathbb{R}^n$

Two vectors u and v in $\mathbb{R}^n$ are orthogonal if $u \cdot v = 0$

If u and $a \neq 0$ are vectors in $\mathbb{R}^n$ then u can be uniquely expressed as $u = w_1 + w_2$ where $w_1 = ka$ and a and w_2 are orthogonal

If u and v are orthogonal vectors in $\mathbb{R}^n$ then $||u + v||^2 = ||u|| + ||v||^2$

6.4 General (real) vector spaces

V is a real vector space if the following axioms hold

1. $u + v = v + u$
2. $u + (v + w) = (u + v) + w$
3. There is an element $0 \in V$ such that $u + 0 = 0 + u = u$ for all u
4. For each $u \in V$, there is $-u \in V$ such that $u + (-u) = (-u) + u = 0$
5. $k(u + v) = ku = kv$
6. $(k + m)u = ku + mu$
7. $k(mu) = km(u)$
8. $1u = u$

6.5 Subspaces

A subset W of a vector space V is called a subspace of V if W is itself a vector space, with operations inherited from V

- To verify that W is a subspace of V, we don't need to check all 8 axioms
- We only need to check that W is closed under the operations of V

If $W_1, W_2, ..., W_r$ are subspaces of V then so is $W_1 \cap W_2 \cap \ldots \cap W_r$

6.6 Linear combinations

If $S = \{v_1, \ldots, v_r\}$ is a non-empty subset of a vector space V then

- The set $W = \{\sum_{i=1}^{r} k_i \mathbf{v}_i | k_i \in \mathbb{R}\}$ of all linear combinations in S is a subspace of V
- The set W is the (inclusion wise) smallest subspace of V that contains S

The set W is called the **span** of S, it is denoted by span(S) or span($v_1, \ldots, v_r$)

6.7 Linear (in)dependence

Vectors $v_1, \ldots, v_r$ are called linearly independent if

$$k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \ldots + k_r\mathbf{v}_r = \mathbf{0} \Rightarrow k_1 = k_2 = \ldots = k_r = 0$$

Otherwise they are **linearly dependent**
A set S of two or more vectors is linearly dependent iff at least one of the vectors is expressible as a linear combination of the other vectors in S

Let $S = \{v_1, \ldots, v_r\}$ be a subset of $\mathbb{R}^n$. If $r > n$ then S is linearly dependent

7 Basis and Dimension of a vector space

7.1 Basis

If V is a vector space and $S\{v_1, \ldots, v_r\}$ is a set of vectors in V then S is a basis for V if

1. S is linearly independent
2. S spans V

- The standard unit vectors form a basis for $\mathbb{R}^n$, called the standard basis
- The $m \times n$ matrices M_{ij} whose entries are all 0 except $a_{ij} = 1$ form the standard basis for the space $\mathbb{M}_{nm}$ of all $m \times n$ matrices

7.2 Basis representation is unique

If $S = \{v_1, ..., v_n\}$ is a basis for a vector space V then each vector $v \in V$ can be expressed as $\mathbf{v} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \ldots + k_n\mathbf{v}_n$ in exactly one way

7.3 Coordinates

If $S = \{v_1, \ldots, v_n\}$ is a basis for the vector space V then the coordinates of a vector $v \in V$ relative to the basis S are the (unique) numbers $k_1, k_2, \ldots, k_n$ such that $\mathbf{v} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \ldots + k_n\mathbf{v}_n$
The vector $(v)_s = (k_1, k_2, \ldots, k_n) \in \mathbb{R}^n$ is the coordinate vector of v relative to S

7.4 Dimension

A vector space V is finite-dimensional if it can be spanned by a finite set of vectors. Otherwise, V is infinite-dimensional.

Let V be a finite-dimensional vector space and let $\{v_1, ..., v_n\}$ be any basis in V

1. Any subset of V with more than n vectors is linearly dependent
2. Any subset of V with fewer than n vectors does not span V

All bases of a finite dimensional vector space have the same number of vectors

The dimension of a finite-dimensional vector space V, denoted by dim(V), is the number of vectors in any of its basis, by convection, dim($\{0\}$) = 0

7.5 Plus/Minus Theorem

Let S be a non-empty set of vectors in a vector space V

1. If S is linearly independent and $v \in V$ is not in span(S) then $S \cup \{v\}$ is also linearly independent
2. If some $v \in S$ can be expressed as a linear combination of other vectors in S then span(S) = span(S $\{V\}$)

Let V be a n-dimensional vector space and let S be a subset of V with exactly n vectors. If S is linearly independent or S spans V then S is a basis for V

7.6 Dimension of a subspace

Let W be a subspace of a finite-dimensional vector space V. Then

1. W is finite-dimensional and dim(W) $\leqslant$ dim(V)
2. $W = V$ iff dim(W) = dim(V)

7.7 Row space, column space and null space

Let A be an $m \times n$ matrix
The **row space** of A is the subspace of $\mathbb{R}^n$ spanned by the row vectors of A
The **column space** of A is the subspace of $\mathbb{R}^m$ spanned by the column vectors of A
The **null space** of A is the solution set of the linear system $Ax = 0$

7.8 Elementary row operations and the column space

Elementary row operations change neither the row space nor the null space of a matrix, but they can change the column space

7.9 Finding basis for the row, column and null spaces

To find the basis for the column space

- Transform A (by elementary row operations) to row echelon form R
- Select all columns in R that have leading 1s
- The corresponding columns in A form a basis

To find a basis for the row space of a matrix A

- Transform A (by elementary row operations) to row echelon form R
- The rows in R with the leading 1s form a basis for the row space of A

To find a basis for the null space

- Find the general solution to the system $Ax = 0$
- For each free variable, x, take the solution (vector v_x) in which $x = 1$ and the other free variables are set to 0
- These vectors v_x together form a basis for the null space

To find a basis for span(S)

- Form a matrix whose row vectors are the vectors in S and then do as above

7.10 Rank and nullity

The row space and column space of a matrix have the same dimension.

The **rank** of a matrix A, denoted by $\text{rank}(A)$ is the dimension of its row space
The **nullity** of A, denoted by $\text{nullity}(A)$ is the dimension of the null space of A

For any $m \times n$ matrix A, $\text{rank}(A)$ and $\text{nullity}(A)$ are the numbers of leading and free variables, respectively, in the general solution to $ax = 0$

For any matrix A with n columns, $\text{rank}(A) + \text{nullity}(A) = n$

8 Linear Maps

8.1 Linear Maps

Let V and W be vector spaces. A function $f : V \to W$ is called a linear map, or a linear transformation from V to W if, for all $u, v \in V$, $k \in \mathbb{R}$
If $V = W$ then f is called a linear operator

8.2 Bases and linear maps

Let $f : V \to W$ be a linear map where V is finite-dimensional. If $S = \{v_1, ..., v_n\}$ is a basis for V then the image of any vector $v \in V$ can be expressed as

$$f(\mathbf{v}) = c_1 f(\mathbf{v}_1) + c_2 f(\mathbf{v}_2) + \ldots + c_n f(\mathbf{v}_n)$$

where $c_1, \ldots, c_n$ are the coordinates of v relative to S

8.3 The kernel and range of a linear map

Let $f : V \to W$ be a linear map
The **kernel** of f, denoted by $\ker(f)$ is defined by $\ker(f) = \{x \in V | f(x) = 0\}$
The **range** of f is defined as $\text{range}(f) = \{\mathbf{u} \in W | \mathbf{u} = f(\mathbf{x}) \text{ for some } \mathbf{x} \in V\}$

8.4 Dimension theorems for matrices and linear maps

The **rank** of a linear map f, denoted by $\text{rank}(f)$ is the dimension of $\text{range}(f)$
The **nullity** of f, denoted by $\text{nullity}(f)$, is the dimension of $\ker(f)$

If f is a linear map from R^n to R^m then $\text{rank}(f) + \text{nullity}(f) = n$

9 Eigenvalues and Eigenvectors

Let S be an $n \times n$ matrix. A non-zero vector $x \in \mathbb{R}^n$ is called an eigenvector of A, if, for some scalar λ

$$Ax = \lambda x$$

In this case, λ is called an eigenvalue of A and x is an eigenvector corresponding to λ

9.1 Characteristic equation of a matrix

If A is an $n \times n$ matrix then λ is an eigenvalue of A iff it satisfies $\det(\lambda I - A) = 0$

The equation $\det(\lambda I - A) = 0$ is called the characteristic equation of A

9.2 Characteristic polynomial of a matrix

In general, the expression $\det(\lambda I - A)$ is a polynomial

$$p(\lambda) = \lambda^n + c_1 \lambda^{n-1} + \ldots + c_{n-1} \lambda + c_n$$

where n is the order of A. It is called the characteristic polynomial of A

9.3 Eigenspaces and their bases

- Let λ_0 be an eigenvalue of A and consider the equation $(\lambda_0 I - A)x = 0$
- The solution set of the equation is a subspace of $\mathbb{R}^n$, it is the null space of the matrix $\lambda_0 I - A$
- It is called the eigenspace of A corresponding to λ_0 because the non-zero vectors in this subspace are the eigenvectors of A corresponding to λ_0
- To find the basis in this subspace, use the algorithm for finding basis in null space of a matrix

Find (a basis of) the eigenspace of $A = \begin{pmatrix} 2 & -1 \\ 10 & -9 \end{pmatrix}$ corresponding to $\lambda = 8$

Form the equation $(-8I - A)x = 0$, or

$$\begin{pmatrix} -10 & 1 \\ -10 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{or} \quad \begin{array}{l} -10x_1 + x_2 = 0 \\ -10x_1 + x_2 = 0 \end{array}$$

The subspace consists of all vectors of the form $(x, 10x)$. One basis is $\{(1, 10)\}$

9.4 Similarity of matrices

Square matrices A and B are called similar if $A = P^{-1}BP$ for some invertible P

If A and B are similar then $\det(A) = \det(B)$

A square matrix is called **diagonalisable** if it is similar to a diagonal matrix

9.5 Diagonalization

An $n \times n$ matrix is diagonalisable iff it has n linearly independent eigenvectors