



MAT240: Algebra I

Review Notes

Author: Joseph Siu

Email: joseph.siu@mail.utoronto.ca

Date: April 18, 2024



Contents

1	Fields	2
2	Modular Arithmetic	2
3	Complex Number	2
4	Polynomial	2
5	Matrix	3
5.1	How matrices are linear transformations	3
5.2	Matrix multiplications in general	3
5.3	Check linearly independency of columns	3
5.4	From the row perspective	3
5.5	Purpose of row reductions	4
5.6	Other properties of similar matrices	4
5.7	Determinants	4
5.8	Eigenvectors, eigenvalues, and eigenspaces	5
6	Vector Spaces	5
7	Subspaces	5
8	System of equations	5
9	Independence and spanning sets	6
10	Basis	6
11	Dimension	6
12	Linear transformations	6
13	Coordinates	6
14	Change of coordinates	6
15	Rank	6
16	Determinants	6
17	Diagonalization	6

1 Fields

Commutativity, Associativity, Distributivity, Identity, Inverse.

2 Modular Arithmetic

$$[a] + [b] = [a + b], [a] \cdot [b] = [a \cdot b].$$

Claim 1

All elements in \mathbb{Z}_n are invertible if and only if n is a prime.



Proof. Assume $n = ab$, then assume for contradiction $ac = 1 \pmod{n}$ for some c , then $ac - ny = 1$ for some y , and $ac - aby = 1$ so $a(c - by) = 1$ so a divides 1, contradiction.

QUOD
ERAT
DEMON■

Claim 2

a is invertible in \mathbb{Z}_n if and only if $\gcd(a, n) = 1$.



Proof. Assume a invertible where $ac = 1 \pmod{n}$, and assume $\gcd(a, n) = b > 1$, then $ac - nx = 1$ for some x , however right side not divisible by b so contradiction.

Assume $\gcd(a, n) = 1$, then $ax + ny = 1$ for some x, y , so $ax = 1 \pmod{n}$.

QUOD
ERAT
DEMON■

3 Complex Number

Modulus is just the length of the line, which by pathagorean theorem is $\sqrt{x^2 + y^2}$.

To find multiplicative inverse, we first multiply the conjugate, then divide by modulus squared so that it is projected to the real line then scaled to 1. That is, $\left(\frac{1}{x^2 + y^2}\right)(x - yi)(x + yi) = 1$.

Polar form is a scaled radius of the unit circle, that is, first rotate the line from 0 to 1 by θ , then scale by the modulus. Here $\tan \theta = \frac{y}{x}$. To calculate we can also consider sin and cos separately, that is, modulus $x = r \cos \theta$ and $y = r \sin \theta$.

4 Polynomial

Definition 1 – Polynomial Division


$$f(x) = q(x)g(x) + r(x), \text{ where } \begin{cases} \deg r < \deg g & \text{if } g \neq 0 \\ r = 0 & \text{if } g = 0 \end{cases}$$

g divides f if $r \equiv 0$.



To find the irreducible polynomials, we can first eliminate the combination of coefficients that guarantee an integer root.

Theorem 1 – FTA

Every non-constant polynomial has a root over \mathbb{C} (every non-constant polynomial can be factored into products of linear factors over \mathbb{C}). 

5 Matrix

(This section assumed that the reader is already familiar with most of the definitions of MAT240 regarding matrices. This section will reinforce the connections between the ideas of matrices and linear transformations.)

5.1 How matrices are linear transformations

Since every matrix represents a linear transformation and vice versa, to understand matrix, it is equivalent to understand the linear transformation that corresponds to the matrix.

First consider a linear transformation and its matrix. The set that contains the columns of the matrix spans the image of the linear transformation. That is, consider a vector in the domain, then the output of the linear transformation given this vector is the summation of the i^{th} entry of the vector times the i^{th} column of the matrix. What this means is that the matrix stores some vectors (columns) that can be scaled and added (using the given vector) to form any vector in the image.

5.2 Matrix multiplications in general

What we have discussed was the case that a matrix is multiplied with a vector at the right, if a matrix is multiplied with another matrix at the right instead, we can treat the right matrix as a set of vectors (columns), then we perform the same operation as before, then put all the results together and form another matrix (set of column vectors). Furthermore, If two matrices are multiplied together, this can be treated as a composition of linear transformations from right to left.

5.3 Check linearly independency of columns

Now, we can see the columns of the matrix span the image of the linear transformation, but how do we know if the columns form a basis¹ of the image (column space)²? We need to check if they are linearly independent or not, the easiest way would be change the matrix to RREF, and see if one column can be expressed as a linear combination of the others or not (if it is full rank then the columns are dependent thus form a basis). Here note that when performing row reductions, the column space (image) has changed, however since we only care whether they are independent or not, so row operations won't affect the result.

5.4 From the row perspective

To now, we have discussed matrices from a column perspective as combinations / sets of column vectors. However, when solving solution like $Ax = B$, we can think this as a system of linear equations, where row operations won't affect the solution since all operations are reversible, for example:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{array} \right) : \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 1 & 1 & 0 & b \rightarrow b + a \\ 0 & 0 & 1 & c \end{array} \right) \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 0 & 1 & b \rightarrow c \\ 0 & 1 & 0 & c \rightarrow b \end{array} \right) \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 1 & \frac{1}{2} & 0 & b \rightarrow \frac{b}{2} \\ 0 & 0 & 1 & c \end{array} \right)$$

are the transformations that add the first row to the second row; swap the last 2 rows; and multiply the second row by $\frac{1}{2}$ respectively. We can see that the vectors that satisfy the later equations must also satisfy

¹An ordered linearly independent set that spans the space.

²Space, or vector space, is a set of vectors that are closed under addition and scalar multiplication.

the original equations since we can reverse the operations without changing the equalities:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ -1 & 1 & 0 & b \rightarrow b + a \rightarrow b + a - a = b \\ 0 & 0 & 1 & c \end{array} \right) \quad \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 0 & 1 & b \rightarrow c \rightarrow b \\ 0 & 1 & 0 & c \rightarrow b \rightarrow c \end{array} \right) \quad \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 1 & 2 & 0 & b \rightarrow \frac{b}{2} \rightarrow 2\frac{b}{2} = b \\ 0 & 0 & 1 & c \end{array} \right)$$

From here, we can also see why when finding the null space³ of the image (column space), our row operations won't affect the result, and performing row operations is very helpful not only because we can decrease the numbers of values to look at, but also it is easier to see *how* the columns are depending on others if there are any.

5.5 Purpose of row reductions

Relating to this discussion, we can see the purpose of row reductions is to transform the given matrix to a diagonalized (or mostly diagonalized) form, so that *some* solutions of the diagonalized matrix remain the same as the original matrix⁴, for example the null space is preserved.

5.6 Other properties of similar matrices

However just knowing the points that do not change after “diagonalization”⁵ is probably not that interesting enough, in fact, similar matrices also preserve another important property: the eigenvalues. Geometrically the eigenspace contains vectors that are only being stretched by some factor λ after the linear transformation. Before we begin, the idea of determinant needs to be introduced.

5.7 Determinants

As commonly known, the determinant of a transformation is simply the “area / volume / hyper-volume” determined by the column vectors (the vectors that span the image). We first define the identity matrix (that is, transformation that its image is spanned by the standard basis) to have determinant 1. Then we define swapping rows or columns as negating the original determinant. What this does intuitively is that the order of “axis / dimension” we used to calculate the “hyper-volume” of the transformation got changed, which results in flipping the entire “hyper-volume” from an external perspective. Lastly, as we can see intuitively, scaling or adding determinants on one “axis / dimension” will scale or add the entire “hyper-volume” by the same factor or value.

To summarize, we define determinant using the following three definitions:

1. $\det I = 1$.
2. $\det A' = -\det A$ if A' is obtained by swapping 2 rows or 2 columns of A .
3. $\begin{vmatrix} ta+x & tb+y \\ c & d \end{vmatrix} = t \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} x & y \\ c & d \end{vmatrix}$.

Moreover, by [Leibniz formula](#), we can calculate the determinant for any square $n \times n$ matrix A as:

$$\det A = \sum_{j=1}^n (-1)^{i+j} A_{ij} \det(\tilde{A}_{ij}) \quad \forall i \in \{1, \dots, n\},$$

where \tilde{A}_{ij} is defined by removing the i^{th} row and j^{th} column of A .

Using these definitions, we can come up with useful properties such as $\det AB = \det A \det B$ and $\det A^T = \det A$, that is, linear transformation through column vectors has the same determinant as linear transformation

³Null space contains vectors that are being sent to 0 by the linear transformation / matrix.

⁴We say that the matrices that can diagonalize to the same diagonal matrix are *similar*.

⁵The process of changing a matrix into a diagonalized form, but as we all know what some matrices (not full rank) cannot be fully diagonalized, here comes the Jordan Normal Form which will be discussed in MAT247.

through row vectors. Last but not least, we can see that similar matrices have the same determinant as their diagonal matrix

$$\det A = \det Q^{-1} \det A \det Q = \det Q^{-1} A Q = \det B,$$

and

$$\det A = \det P^{-1} \det D \det P = \det P^{-1} D P = \det D,$$

for some similar matrices $B = Q^{-1} A Q$ and diagonal matrix D where $A = P^{-1} D P$. Notice here that the determinant of all corresponding diagonal matrices are the same which the reason will be explained in the next paragraph.

5.8 Eigenvectors, eigenvalues, and eigenspaces

Finally, we can discuss what eigenvalues, eigenvectors, and eigenspaces are. To start, eigenvectors are vectors that are only stretched after applying matrix A (or linear transformation T_A), namely $Av = \lambda v$ for some vector v and some constant λ . By distributivity we may rearrange this equation to $(A - \lambda I)v = 0$, here λ is a constant to be determined. Since v is non-zero, and is being transformed to the 0-vector through matrix $A - \lambda I$ (and thus it's linear transformation $T_{A-\lambda I}$), so v exists if and only if $T_{A-\lambda I}$ is *not* full rank, or in other words, its columns are linearly dependent. Which we also know that if there exists a column that is dependent from the others, then we may perform column operations to make the row to be 0, which by Leibniz formula gives the determinant is equal to 0. Thus, we may conclude that as long as $\det(A - \lambda I) = 0$, there exists a non-zero vector v that satisfies $Av = \lambda v$, and we will also call such vector an eigenvector with eigenvalue λ .

Since the entries of A are constants, and λI is a diagonal matrix where all diagonal entries are λ , to find all possible λ , we will treat it as a variable, and apply the Leibniz formula to get a polynomial from $\det(A - \lambda I) = 0$, which is called the *characteristic* polynomial. Then we can see that the roots of such polynomial gives all possible λ that satisfies the equation $Av = \lambda v$ for some vector v in the domain.

So, the eigenvalues of a linear transformation / matrix are the roots of the characteristic polynomial determined using $\det(A - \lambda I) = 0$, the eigenvectors are the vectors that satisfy $Av = \lambda v$ for some eigenvalue λ , and the eigenspace is the space that contains all eigenvectors that correspond to the *same* eigenvalue.

6 Vector Spaces

$$T(ax + y) = aT(x) + T(y), T(0) = 0.$$

The dimension of a vector space is the size (cardinality) of the basis of the vector space. By replacement theorem, all bases of a vector space have the same size.

7 Subspaces

$\{0\}$ and the space itself are trivial subspaces, others are called non-trivial subspaces. Subspace is just a subset of another vector space that is also a vector space.

Common subspaces include the null space (kernel) and the column space (image) of a matrix⁶.

If $V = W_1 + W_2$ and $W_1 \cap W_2 = \{0\}$, then $V = W_1 \oplus W_2$. That is, if V is the sum of two “disjoint” subspaces (only intersect at 0), then V is called the direct sum of W_1 and W_2 .

8 System of equations

To solve $Ax = B$, we augment the matrix A to $A | B$, then perform row operations to make the left side to be in its RREF form, then set the free (non-leading) variables and express the pivot (leading) variables in terms of the free variables, then we can get a basis of the solutions.

⁶By dimension theorem we have that $\dim V = \dim \text{im} T + \dim N(T)$ for all linear transformation $T : V \rightarrow W$.

We call the solutions that are not the 0-vector the non-trivial solutions, and 0 the trivial solution.

9 Independence and spanning sets

We used the word linearly independent throughout this notes, but we haven't formally defined what is linearly independent. We say vectors v_1, \dots, v_n are linearly independent if the only solution to $c_1v_1 + \dots + c_nv_n = 0$ is $c_1 = \dots = c_n = 0$. Otherwise, we say they are linearly dependent. In other words, if one vector can be expressed by the other ones, then they are linearly dependent.

10 Basis

The span of a set of vectors is the set of all linear combinations of the vectors. We will call this set a basis of the span if its vectors are linearly independent.

That is, a basis of a vector space is a set of vectors that are linearly independent and span the vector space.

11 Dimension

The dimension of a vector space is the size of its basis.

$\dim T_A = \text{rank } A$, where A is the corresponding matrix of linear transformation T_A .

For finite dimensional vector space V , if W is a subspace, then $\dim W \leq \dim V$.

12 Linear transformations

13 Coordinates

14 Change of coordinates

15 Rank

16 Determinants

17 Diagonalization