



MAT240: Algebra I

Review Notes

Author: Joseph Siu

Email: joseph.siu@mail.utoronto.ca

Date: April 18, 2024



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.)

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.

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.

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.

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

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

From here, you can also see why when finding the null space 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.

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.

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 matrix ³, for example the null space is preserved.

However just knowing the points that do not change after “diagonalization” ⁴ is probably not that interesting enough, in fact, similar matrices also preserve another important property: the eigenspace (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.

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. $\begin{vmatrix} ta+x & tb+y \\ c & d \end{vmatrix} = t \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} x & y \\ c & d \end{vmatrix}$.

³We say that the matrices that can diagonalize to the same diagonal matrix are *similar*.

⁴The 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.