Notes on Abstract Algebra[1]

by

Marcel K. Goh

1. PRELIMINARY NOTIONS FROM LINEAR ALGEBRA

This set of notes assumes that the reader has had some exposure to linear algebra; the most crucial notions will be outlined in this section.

1.1. Basic properties of square matrices

We shall mainly concern ourselves with matrices of the form

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

where n is some positive integer and each entry $a_{ij} \in \mathbf{R}$. We call the set of all $n \times n$ matrices with real entries $M_n(\mathbf{R})$.

For two matrices A and B, we may form their *sum* $A + B = (a_{ij} + b_{ij})$. (This notation means that at the ith row and jth column, the entry is the sum of a_{ij} and b_{ij}.). Given a real number α, we obtain the scalar product $\alpha A = (\alpha \cdot a_{ij})$ by multiplying every entry in A by α.

We can also *multiply* $n \times n$ matrices A and B with the following formula:

$$A \cdot B = (c_{ij}) \quad \text{where } c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}. \tag{1}$$

Since a matrix represents a linear transformation, multiplying matrices is like composing functions. If S and T are the transformations represented by the matrices B and A, respectively, then the matrix product $A \cdot B$ can be thought of as the following composition of transformations:

$$\begin{tikzcd} \mathbf{R}^n \arrow[r, "S"] & \mathbf{R}^n \arrow[r, "T"] & \mathbf{R}^n \end{tikzcd}$$

For matrices A and B the commutativity of addition

$$A + B = B + A \tag{2}$$

is valid, and for three matrices A, B, and C, the distributive law

$$A \cdot (B + C) = A \cdot B + A \cdot C \tag{3}$$

and the associativity of multiplication

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \tag{4}$$

may be proven to hold as well. In particular, (4) is laborious to prove from the definition given in (1), but easy to derive when reasoning about matrices as transformations.

Unlike addition, multiplication is not commutative: $A \cdot B$ does not equal $B \cdot A$ in general. To prove this, we simply note that

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ but } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

[1] Based on a series of lectures given at Harvard University in Fall 2003 by Prof. Benedict Gross.

The matrix

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots\ddots & 0 & \\ 000 & \cdots & 1 & \end{pmatrix}$$

is called the *identity matrix* and has the property that $AI = IA = A$ for any matrix A. [When no ambiguity can arise, we often omit the $\cdot$ symbol when denoting a product.]

We say that a matrix A is *invertible* if and only if there exists a matrix B such that $AB = BA = I$; otherwise, it is called *singular.* Not all matrices are invertible. For example, the matrix $\mathbf{0}$, all of whose entries are 0, is not invertible in any dimension. The identity matrix is easily seen to be invertible (take $B = I$). Note that if an inverse matrix exists for a given matrix A, then it is unique, for if $AB = AB' = I$ and $B'A = BA = I$, then, multiplying the first identity by B on the left, we arrive at $BAB = BAB'$, i.e. $B = B'$.

Since a 1×1 matrix (a) contains only one real number, it is invertible if and only if $a \neq 0$. A 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible if and only if $ad - bc = 0$, since for any such matrix,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -c \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix},$$

and we can multiply both sides by $1/(ad - bc)$ to obtain the identity on the right, provided that $ad - bc$ is nonzero.

In general, there exists a function $\det : M_n(\mathbf{R}) \to \mathbf{R}$ such that a matrix $A \in M_n(\mathbf{R})$ is invertible if and only if $\det A \neq 0$. This determinant can be calculated as a sum over $n!$ terms; this formula will not be useful for our purposes.

1.2. The general linear group

Let us now restrict our attention to a certain subset of square matrices, namely those whose determinant is nonzero. This set is called the *general linear group of degree n* and is denoted $GL_n(\mathbf{R})$ when all matrix entries are real numbers. Remark that, since $(-1) + (1) = (0)$, this set is not closed under addition; scalar multiplication is also no longer a safe operation, since multiplying any matrix by 0 results in a singular matrix.

In return for these two forfeited closure properties, we get closure under matrix multiplication.

Proposition I. *Suppose that two matrices A and B are invertible. Then their product AB is also invertible.*

Proof. Consider $B^{-1}A^{-1}$ and the product $(B^{-1}A^{-1})(AB)$. By associativity of multiplication, this becomes $B^{-1}(A^{-1}A)B = B^{-1}IB = IB^{-1}B = II = I$. Alternatively, use the fact that $\det(AB) = \det(A)\det(B)$, which is nonzero because both $\det(A)$ and $\det(B)$ are nonzero. ▮

Thus the set $GL_n(\mathbf{R})$, under the operation of matrix multiplication, has a multiplicative inverse A^1 for every matrix A. It also contains an identity element I and the multiplication operation is associative. These are the properties of a group.

2. GROUPS

2.1. Properties and basic examples

A *group* G is a set on which is defined a rule of combination such that the product of two elements $g, h \in G$, denoted $g \cdot h$ or gh, is also in G. Furthermore, the following three properties must hold:

a) Multiplication must be associative: for all $g, h, k \in G$, $(gh)k = g(hk)$.

b) There exists an identity element $e \in G$ such that $ge = eg = g$ for all $g \in G$. This element is also often denoted 1.

c) For every element $g \in G$, there exists an inverse element g^{-1} such that $gg^{-1} = g^{-1}g = e$.

If $gh = hg$ for all $g, h \in G$, then we say the group G is *commutative* or *abelian*.

The most familiar abelian group is the set of all integers, denoted $\mathbf{Z}$, under the operation of addition. It has 1 as its identity, inverses $-a$ for every whole number a, and the commutative property; likewise, any vector space V is also an abelian group under vector addition.

Group theory is intimately connected to the study of symmetries of an object. Let T be a set and let $\mathrm{Sym}(T)$ denote the set of all bijections from T to itself. This is called the *symmetric group* on T as, under composition of functions, it obeys all the group axioms: It contains the identity transformation e and every bijection f has an inverse bijection f^{-1}. In some sense, the symmetric group is the most general group, because all other groups arise from adding restrictions to these bijections. For instance, $GL_n(\mathbf{R}) \subset \mathrm{Sym}(\mathbf{R}^n)$. If $T = \{1, \ldots, n\}$, then $\mathrm{Sym}(T)$ is called the symmetric group on n letters and is denoted S_n. This group has $n!$ elements and is non-abelian when $n \geq 3$.

2.2 Subgroups