

# Notes on Abstract Algebra<sup>1</sup>

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  $i$ th row and  $j$ th column, the entry is the sum of  $a_{ij}$  and  $b_{ij}$ .) Given a real number  $\alpha$ , we obtain the scalar product  $\alpha A = (\alpha \cdot a_{ij})$  by multiplying every entry in  $A$  by  $\alpha$ .

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

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

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:

$$\mathbf{R}^n \xrightarrow{S} \mathbf{R}^n \xrightarrow{T} \mathbf{R}^n$$

For matrices  $A$  and  $B$  the commutativity of addition

$$A + B = B + A \quad (2)$$

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

$$A \cdot (B + C) = A \cdot B + A \cdot C \quad (3)$$

and the associativity of multiplication

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \quad (4)$$

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

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

---

<sup>1</sup> Based on a series of lectures given at Harvard University in Fall 2003 by Prof. Benedict Gross.

The matrix

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

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  $1 \times 1$  matrix  $(a)$  contains only one real number, it is invertible if and only if  $a \neq 0$ . A  $2 \times 2$  matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is invertible if and only if  $ad - bc \neq 0$ , 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  $\det : M_n(\mathbf{R}) \rightarrow \mathbf{R}$  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:

- Multiplication must be associative: for all  $g, h, k \in G$ ,  $(gh)k = g(hk)$ .
- 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.
- 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 number of elements in  $G$  is called its *order* and this value, also denoted  $|G|$ , need not be finite.

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  $\text{Sym}(T)$  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,  $GL_n(\mathbf{R}) \subset \text{Sym}(\mathbf{R}^n)$ . If  $T = \{1, \dots, n\}$ , then  $\text{Sym}(T)$  is called the symmetric group on  $n$  letters and is denoted  $S_n$ .

## 2.2 Subgroups

Let  $G$  be a group. We call a nonempty subset  $H \subset G$  a *subgroup* and write  $H \leq G$  provided that

- a) The set  $H$  is closed under the multiplication operation of  $G$ .
- b) Whenever  $H$  contains an element  $a \in G$ ,  $H$  contains its inverse  $a^{-1}$  as well.

It is immediate from these requirements that a subgroup  $H$  contains the identity element. Since  $H$  is nonempty, it contains an element  $h$  as well as its inverse  $h^{-1}$ . Then from closure of multiplication we conclude that  $hh^{-1} = e \in H$ .

We turn our attention to  $S_3$ , the permutation group on three letters. Notice that this group is not commutative, since the elements

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

do not commute:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \text{but} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Note that for  $k \leq n$ ,  $S_k \leq S_n$  because we can simply fix the letters  $k+1, k+2, \dots, n$ . An easy corollary, then, is that  $S_n$  does not commute for  $n \geq 3$ . This is because  $S_3 \leq S_n$  and we can simply take  $\sigma$  and  $\tau$  as elements of the larger group  $S_n$  that do not commute.

Another example of a subgroup is the set of  $2 \times 2$  matrices that stabilise the line  $y = 0$  (vectors lying on this line remain on this line after transformation). In terms of matrices, this set looks like

$$S = \left\{ \begin{pmatrix} a & c \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}.$$

Showing that this set is closed is a simple matter of computing

$$\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & c' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ac' + cd' \\ 0 & dd' \end{pmatrix},$$

and observing that the determinant of this matrix is nonzero since all of  $a, a', d, d'$  were assumed to be nonzero. (Closure under inversion is also easily derived.)

It is not always easy to characterise all subgroups of a given group. For the additive group of integers, however, the following proposition does so nicely.

**Proposition S.** *The subgroups of  $\mathbf{Z}$  under addition are precisely given by  $b\mathbf{Z}$ , where  $b$  is a fixed integer.*

*Proof.* First, we fix an integer  $b$  and show that  $b\mathbf{Z}$  is a subgroup. Adding two integers  $bm + bn$  gives a third integer  $b(m+n)$ , which is also in  $b\mathbf{Z}$ , so the set is closed under the operation of addition; likewise  $-(bm) = b(-m)$ , so the set is closed under additive inverse.

Now we must show that these  $b\mathbf{Z}$  are all the possible subgroups. Let  $H \leq \mathbf{Z}$ . It is possible that  $H$  contains only the identity 0, in which case  $H = 0\mathbf{Z}$ . If not, let  $b$  be the smallest positive integer contained

in  $H$ . We know from closure that every multiple of  $b$  is in  $H$ , so  $b\mathbf{Z} \subset H$ . Now let  $h$  be any element in  $H$ . By the Euclidean division algorithm, we can divide  $h$  by  $b$  to get  $h = mb + r$ , where  $mb$  is some multiple of  $b$  and  $r$  is a remainder lying in the range  $0 \leq r < b$ . Since  $r = (-mb) + h$ , we have  $r \in H$ . But then necessarily we have  $r = 0$ , since  $b$  is the smallest positive integer in  $H$ . So  $h$  is an integer multiple of  $b$  and we have shown that  $H \subset b\mathbf{Z}$ . ■

Finally, we introduce a specific class of subgroup. If  $G$  is a group with an element  $g$ , the *cyclic subgroup* generated by  $g$  is the set

$$\langle g \rangle = \{g^m : m \in \mathbf{Z}\}.$$

This is a subgroup because  $g^m g^n = g^{m+n}$  and  $(g^m)^{-1} = g^{-m}$ . Note that not all powers are distinct! For example, in the group  $S_3$ , the cyclic subgroup generated by  $\tau$  contains only the identity element and  $\tau$  itself. If  $g^m = e$  and  $m$  is the smallest positive integer for which this holds, we say that the *order* of  $g$  is  $m$  and write  $|g| = m$ . If no such  $m$  exists, then we say  $g$  has infinite order.

If  $G$  is a group containing an element  $g$  such that  $\langle g \rangle = G$ , then  $G$  is called a *cyclic group*.

### 2.3 Isomorphisms and homomorphisms

Consider the group  $G_1 = \{\pm 1, \pm i\}$  under complex multiplication alongside the group  $G_2 = \langle \rho \rangle \leq S_4$ , where  $\rho$  is the permutation that takes  $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4$ , and  $4 \mapsto 1$ . The groups have the following multiplication tables:

		1	$i$	$-1$	$-i$			$e$	$\rho$	$\rho^2$	$\rho^3$
$G_1$ :	1	1	$i$	$-1$	$-i$	$G_2$ :	$e$	$e$	$\rho$	$\rho^2$	$\rho^3$
	$i$	$i$	$-1$	$-i$	1		$\rho$	$\rho$	$\rho^2$	$\rho^3$	$e$
	$-1$	$-1$	$-i$	1	$i$		$\rho^2$	$\rho^2$	$\rho^3$	$e$	$\rho$
	$-i$	$-i$	1	$i$	$-1$		$\rho^3$	$\rho^3$	$e$	$\rho$	$\rho^2$

It doesn't take long to realise that these two multiplication tables are the same, up to relabeling  $1 \equiv e, i \equiv \rho, -1 \equiv \rho^2$ , and  $-i \equiv \rho^3$ . This is an example of the concept of isomorphisms between groups.

Formally, an *isomorphism* is a bijection  $f : G \rightarrow G'$  from a group to another such that

$$f(x \cdot y) = f(x) \cdot f(y).$$

The multiplication on the left-hand side is taking place in  $G$  while the right-hand multiplication takes place in  $G'$ . In the above example, the function  $f : G_1 \rightarrow G_2$  that takes  $i^k \mapsto \rho^k$  for  $k = 0, 1, 2, 3$  gives an explicit isomorphism. If there exists an isomorphism between two groups, we say that they are *isomorphic*.

Any two cyclic groups of order  $n$  are isomorphic. We will not formally prove this, but it is clear that if  $G_1$  and  $G_2$  are cyclic groups of the same order generated by  $g_1$  and  $g_2$  respectively, then the function  $f : G_1 \rightarrow G_2$  given by  $f(g_1^k) = g_2^k$  for any integer  $k$  will be a well-defined isomorphism.

As a perhaps surprising example, the group of real numbers under addition and the group of positive real numbers under multiplication are isomorphic to one another. The function  $f(x) = e^x$  is a bijection from  $\mathbf{R}$  to  $\mathbf{R}^+$  and  $e^{x+y} = e^x e^y$  for real numbers  $x$  and  $y$ .

If two groups  $G_1$  and  $G_2$  are isomorphic, then

- The groups have the same order, i.e.  $|G_1| = |G_2|$ .
- Either  $G_1$  and  $G_2$  are both abelian or they are both non-abelian.
- Both groups have the same number of elements of every order.

These properties are useful in showing that two groups are not isomorphic. For example,  $S_3$  has no element of order 6, so it is not isomorphic to the cyclic group of order 6, which has two such elements: 1 and 5.

An isomorphism from a set to itself is called an *automorphism*. Given a group  $G$ , we can construct a set  $\text{Aut}(G)$  of all automorphisms of  $G$  and in fact, it is easily verifiable that  $\text{Aut}(G)$  is a group under function composition.

We may obtain a generalisation of an isomorphism by relaxing the requirement that the function be bijective. Any map  $f : G_1 \rightarrow G_2$  between groups that satisfies  $f(x \cdot y) = f(x) \cdot f(y)$  for all  $x, y \in G_1$  is called

a *homomorphism*, and an isomorphism is simply a bijective homomorphism. It follows from the definition that any homomorphism maps the identity of the first group to the identity of the second, and that inverses are mapped to inverses. The simplest example of a homomorphism is the trivial homomorphism that maps every element of  $G_1$  to the identity of  $G_2$ . Another homomorphism that is not an isomorphism is the map from  $\mathbf{Z}$  to  $S_2$  that takes all even integers to the identity and all odd integers to the permutation that switches 1 and 2.

The *kernel* of a homomorphism is the set of all elements in the domain that map to the identity in the target group. The *image* of a homomorphism  $f : G_1 \rightarrow G_2$  is the set of all elements in  $G_2$  that equal  $f(x)$  for some  $x \in G_1$ .