

## §17 Groups of Matrices

In this paragraph, we examine some groups whose elements are matrices. The reader probably knows matrices (whose entries are real or complex numbers), but this is not a prerequisite for understanding this paragraph. We give an elementary account of the theory of matrices as far as needed here. Matrix theory will be taken systematically in Chapter 4, §43.

We allow the entries to be elements of any field. Fields will be formally introduced in Chapter 3, §29 (Definition 29.13). Until then, we shall be content with the following definition.

**17.1 Temporary Definition:** A *field* is one of the sets  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{Z}_p$ , where  $p$  is a prime number.

After having learned about fields in Chapter 3, the reader may check that the theory in this paragraph carries over to the more general situation where the term "field" is used in the sense of Definition 29.13.

We note that  $K$  is a commutative group under addition, whose identity element we shall denote by  $0$  (so that  $0$  is the number  $0$  in case  $K$  is one of  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , and it is the residue class  $\bar{0} = 0 + p\mathbb{Z}$  in case  $K$  is  $\mathbb{Z}_p$  for some prime number  $p$ ), and that  $K \setminus \{0\}$  is a group under multiplication. This will be used many times in this paragraph.

**17.2 Definition:** Let  $K$  be a field. A *matrix over  $K$*  is an array

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of four elements  $a, b, c, d$  of  $K$ , arranged in two rows and two columns, and enclosed within parentheses. (The plural of "matrix" is "matrices".)

Thus  $\begin{pmatrix} 1 & 2 \\ -4 & 0 \end{pmatrix}$  is a matrix over  $\mathbb{Q}$  (and also over  $\mathbb{R}$  and  $\mathbb{C}$ ),  $\begin{pmatrix} \pi & \sqrt{2} \\ 5 & -7 \end{pmatrix}$  is a matrix over  $\mathbb{R}$  (and also over  $\mathbb{C}$ ). In addition,  $\begin{pmatrix} \bar{2} & \bar{3} \\ \bar{5} & \bar{4} \end{pmatrix}$  is a matrix over  $\mathbb{Z}_7$ , when bars mean residue classes modulo 7.

The set of all matrices over a field  $K$  will be denoted by  $Mat_2(K)$ . The subscript 2 signifies that there are 2 rows and 2 columns in a matrix (in the sense of Definition 17.2).

If  $K$  is a field and  $A, B$  are matrices from  $Mat_2(K)$ , we say  $A$  is equal to  $B$  provided the corresponding entries in  $A$  and  $B$  are equal. More exactly,

$$A: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is equal to } B: \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

if and only if  $a = a', b = b', c = c', d = d'$ . In this case, we write  $A = B$ . A single matrix equation is equivalent to four equations between the elements of the underlying field. It is clear that matrix equality is an equivalence relation on  $Mat_2(K)$ . In particular, it is legitimate to say that  $A$  and  $B$  are equal when  $A$  is equal to  $B$ .

In this definition of matrix equality, the location of the entries are taken into account. Thus  $\begin{pmatrix} 5 & 1 \\ 0 & 2 \end{pmatrix}$  and  $\begin{pmatrix} 2 & 5 \\ 1 & 0 \end{pmatrix}$  are different matrices, although they are made up of the same numbers.

We introduce two binary operations on  $Mat_2(K)$ , addition and multiplication. Addition is defined in the most obvious way.

**17.3 Definition:** Let  $K$  be a field. For any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  in  $Mat_2(K)$ , we define the *sum of  $A$  and  $B$*  as the matrix

$$\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

The sum of  $A$  and  $B$  will be denoted by  $A + B$ . Taking sums in  $Mat_2(K)$  will be called *addition* (of matrices).

Addition of matrices is essentially the addition in the underlying field, carried out four times. Not surprisingly, many properties of addition in the field are reflected in matrix addition. For example, just like a field is a group under addition, matrices over a field form a group under addition, too.

**17.4 Theorem:** Let  $K$  be a field. Then  $Mat_2(K)$  is a commutative group under addition.

**Proof:** We check the group axioms

(i) For any matrices  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  in  $Mat_2(K)$ , we have  $a + e, b + f, c + g, d + h \in K$  since  $a, b, c, d, e, f, g, h \in K$  and  $K$  is closed under addition. Hence

$$A + B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \in K$$

and  $Mat_2(K)$  is closed under (matrix) addition.

(ii) Associativity of addition in  $Mat_2(K)$  follows from associativity of addition in  $K$ . Indeed, for any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ ,  $C = \begin{pmatrix} k & m \\ n & p \end{pmatrix}$  in  $Mat_2(K)$ , we have

$$\begin{aligned} (A + B) + C &= \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] + \begin{pmatrix} k & m \\ n & p \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} + \begin{pmatrix} k & m \\ n & p \end{pmatrix} \\ &= \begin{pmatrix} (a+e)+k & (b+f)+m \\ (c+g)+n & (d+h)+p \end{pmatrix} \\ &= \begin{pmatrix} a+(e+k) & b+(f+m) \\ c+(g+n) & d+(h+p) \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e+k & f+m \\ g+n & h+p \end{pmatrix} \\ &= A + (B + C). \end{aligned}$$

(iii) What can be the identity element? Well, probably the matrix  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ , where 0 denotes the zero element of the field  $K$  (for instance, when  $K$  is  $\mathbb{Z}_p$  for some prime number  $p$ , 0 is the residue class  $\bar{0} = p\mathbb{Z}$ ). Indeed, we have, for any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ ,

$$A + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ c+0 & d+0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A$$

and  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  is a right identity of  $Mat_2(K)$ . The matrix  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  will be called the *zero matrix (over  $K$ )* and will be designated by the symbol 0. This should not be confused with the zero element of the underlying field  $K$ .

(iv) Any matrix  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$  has a right inverse (opposite)  $-A$  in  $Mat_2(K)$ , namely  $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$  (since  $-a, -b, -c, -d \in K$ ):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = \begin{pmatrix} a+(-a) & b+(-b) \\ c+(-c) & d+(-d) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

Thus  $Mat_2(K)$  is a group under addition. We finally check commutativity.

(v) Commutativity of addition in  $Mat_2(K)$  follows from commutativity of addition in  $K$ . Indeed, for any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  in  $Mat_2(K)$ , we have

$$A + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = B + A.$$

So  $Mat_2(K)$  is a commutative group under addition.  $\square$

The additive group  $Mat_2(K)$  is somewhat dull. It is just four copies of the additive group  $K$ . More interesting matrix groups arise when the operation is multiplication. We introduce this operation now.

**17.5 Definition:** Let  $K$  be a field. For any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  in  $Mat_2(K)$ , we define the *product of A and B* as the matrix

$$\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

The product of  $A$  and  $B$  will be denoted by  $A \cdot B$  or simply by  $AB$ . Taking products in  $Mat_2(K)$  will be called *multiplication* (of matrices).

This definition looks bizarre. One would expect the product of  $A$  and  $B$ , with the notation of Definition 17.5, to be  $\begin{pmatrix} ae & bf \\ cg & dh \end{pmatrix}$ . Some motivation for Definition 17.5 can be gained as follows. With each matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  (over  $\mathbb{R}$ , say), there is associated a coordinate transformation

$$\begin{aligned} x &= ax' + by' \\ y &= cx' + dy' \end{aligned}$$

of the Euclidean plane. Carrying out the transformations associated with  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$  successively, we obtain

$$\begin{aligned}x &= ax' + by' & x' &= ex'' + fy'' \\y &= cx' + dy' & y' &= gx'' + hy'',\end{aligned}$$

which gives

$$\begin{aligned}x &= a(ex'' + fy'') + b(gx'' + hy'') = (ae+bg)x'' + (af+bh)y'' \\y &= c(ex'' + fy'') + d(gx'' + hy'') = (ce+dg)x'' + (cf+dh)y'',\end{aligned}$$

so the product of the matrices is the one which is associated with the successive application of the transformation.

If matrix multiplication is new to you, you are urged to write down matrices over  $\mathbb{R}$  and multiply them in order to acquire dexterity in performing this operation.

We collect some basic properties of matrix multiplication in the next theorem. Let us recall that  $K \setminus \{0\}$  is a group under multiplication. The identity element of this group will be denoted by 1. Thus 1 is the number 1 when  $K$  is one of  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , and the residue class  $\bar{1} = 1 + p\mathbb{Z}$  when  $K = \mathbb{Z}_p$  for some prime number  $p$ .

**17.6 Theorem:** *Let  $K$  be a field, whose zero element is 0 and whose identity element is 1.*

- (1)  $Mat_2(K)$  is closed under matrix multiplication.
- (2)  $(AB)C = A(BC)$  for all  $A, B, C \in Mat_2(K)$ .
- (3) Let  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . Then  $AI = IA = A$  for all  $A \in Mat_2(K)$ .
- (4)  $A(B + C) = AB + AC$  and  $(B + C)A = (BA + CA)$  for all  $A, B, C \in Mat_2(K)$ .

**Proof:** Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ ,  $C = \begin{pmatrix} k & m \\ n & p \end{pmatrix}$  be arbitrary elements of  $Mat_2(K)$ .

(1) Since a field is closed under addition and multiplication,  $ae + bg$ ,  $af + bh$ ,  $ce + dg$ ,  $cf + dh \in K$  whenever  $a, b, c, d, e, f, g, h \in K$ . So  $AB \in Mat_2(K)$  for all  $A, B \in Mat_2(K)$  and  $Mat_2(K)$  is closed under multiplication.

(2) This is routine calculation. We evaluate  $(AB)C$  and  $A(BC)$ :

$$\begin{aligned}
(AB)C &= \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] \begin{pmatrix} k & m \\ n & p \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \begin{pmatrix} k & m \\ n & p \end{pmatrix} \\
&= \begin{pmatrix} (ae+bg)k + (af+bh)n & (ae+bg)m + (af+bh)p \\ (ce+dg)k + (cf+dh)n & (ce+dg)m + (cf+dh)p \end{pmatrix} \\
&= \begin{pmatrix} aek+bgk+afn+bhn & aem+bgm+afp+bhp \\ cek+dgk+cfn+dhn & cem+dgm+cfp+dhp \end{pmatrix}, \tag{i}
\end{aligned}$$

$$\begin{aligned}
A(BC) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[ \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} k & m \\ n & p \end{pmatrix} \right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} ek+fn & em+fp \\ gk+hn & gm+hp \end{pmatrix} \\
&= \begin{pmatrix} a(ek+fn)+b(gk+hn) & a(em+fp)+b(gm+hp) \\ c(ek+fn)+d(gk+hn) & c(em+fp)+d(gm+hp) \end{pmatrix} \\
&= \begin{pmatrix} aek+afn+bgk+bhn & aem+afp+bgm+bhp \\ cek+cfn+dgk+dhn & cem+cfp+dgm+dhp \end{pmatrix}. \tag{ii}
\end{aligned}$$

Since addition is commutative in  $K$ , the matrices (i) and (ii) are equal. Hence  $(AB)C = A(BC)$  for all  $A, B, C \in Mat_2(K)$ .

$$\begin{aligned}
(3) \text{ We compute } AI &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a1+b0 & a0+b1 \\ c1+d0 & c0+d1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A, \\
IA &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1a+0c & 1b+0d \\ 0a+1c & 0b+1d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A,
\end{aligned}$$

as claimed.

$$\begin{aligned}
(4) \text{ We have } A(B+C) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[ \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} k & m \\ n & p \end{pmatrix} \right] \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e+k & f+m \\ g+n & h+p \end{pmatrix} \\
&= \begin{pmatrix} a(e+k)+b(g+n) & a(f+m)+b(h+p) \\ c(e+k)+d(g+n) & c(f+m)+d(h+p) \end{pmatrix} \\
&= \begin{pmatrix} ae+ak+bg+bn & af+am+bh+bp \\ ce+ck+dg+dn & cf+cm+dh+dp \end{pmatrix} \\
&= \begin{pmatrix} ae+bg+ak+bn & af+bh+am+bp \\ ce+dg+ck+dn & cf+dh+cm+dp \end{pmatrix} \\
&= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} + \begin{pmatrix} ak+bn & am+bp \\ ck+dn & cm+dp \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} k & m \\ n & p \end{pmatrix} \\
&= AB + AC.
\end{aligned}$$

The proof of  $(B+C)A = (BA+CA)$  follows similar lines and is left to the reader.  $\square$

Theorem 17.6 seems promising. Three of the group axioms are satisfied, with  $I$  as the identity. It remains to investigate whether every matrix over a field has a right inverse.

Suppose  $K$  is a field and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(K)$ . Then  $A$  has a right inverse

$X = \begin{pmatrix} x & y \\ z & u \end{pmatrix}$  in  $\text{Mat}_2(K)$  if and only if  $AX = I$ , which is equivalent to

$$\begin{array}{ll} (1) & ax + bz = 1, & (2) & ay + bu = 0, \\ (3) & cx + dz = 0, & (4) & cy + du = 1. \end{array}$$

We multiply the equation (1) by  $d$ , (3) by  $-b$  and add them side by side. Using associativity of addition in  $K$ , distributivity of multiplication over addition, and *commutativity* of multiplication in  $K$ , we get

$$(ad - bc)x = d.$$

We multiply (2) by  $d$ , (4) by  $-b$  and add them. We multiply (1) by  $-c$ , (3) by  $a$  and add them. We multiply (2) by  $-c$ , (4) by  $a$  and add them. We get

$$(ad - bc)y = -b, \quad (ad - bc)z = -c, \quad (ad - bc)u = a.$$

We emphasize again that commutativity of multiplication in  $K$  is used crucially to derive these equations.

The element  $ad - bc$  appears in each one of these equations. In view of its importance, we give it a name.

**17.7 Definition:** Let  $K$  be a field and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(K)$ . Then the element  $ad - bc$  in  $K$  is called the *determinant of A*, written as  $\det(A)$  or as  $\det A$ .

We have shown: if  $K$  is a field and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(K)$ , and if  $X = \begin{pmatrix} x & y \\ z & u \end{pmatrix}$  in  $\text{Mat}_2(K)$  is a right inverse of  $A$ , then

$$\begin{array}{ll} (\det A)x = d & (\det A)y = -b \\ (\det A)z = -c & (\det A)u = a. \end{array} \tag{D}$$

These equations impose certain conditions on a matrix having a right inverse. We cannot expect that every matrix has a right inverse. Those having a right inverse are characterized very simply as the matrices with a nonzero determinant.

**17.8 Theorem:** *Let  $K$  be a field and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(K)$ . Then  $A$  has a right inverse if and only if  $\det A \neq 0$ . If this is the case, then there is a unique right inverse of  $A$ , namely the matrix*

$$\begin{pmatrix} (\det A)^{-1}d & -(\det A)^{-1}b \\ -(\det A)^{-1}c & (\det A)^{-1}a \end{pmatrix}$$

where  $(\det A)^{-1}$  is the inverse of  $\det A \in K \setminus \{0\}$  in the multiplicative group  $K \setminus \{0\}$ .

**Proof:** First we assume  $\det A = 0$  and show that  $A$  has no right inverse. Indeed, if  $\det A = 0$  and  $A$  had a right inverse, then the equations (D) would become

$$\begin{array}{ll} d = 0 & b = 0 \\ c = 0 & a = 0, \end{array}$$

and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  would be the zero matrix  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . The existence of a right inverse  $X = \begin{pmatrix} x & y \\ z & u \end{pmatrix}$  would yield

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I = AX = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} 0x+0z & 0y+0u \\ 0x+0z & 0y+0u \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

hence  $1 = 0$  in  $K$ , a contradiction. Thus  $A$  has no right inverse if  $\det A = 0$ .

Now let us assume  $\det A \neq 0$  and show that  $A$  has a unique right inverse. Since  $\det A \in K \setminus \{0\}$  and  $K \setminus \{0\}$  is a group under multiplication,  $\det A$  has an inverse in  $K \setminus \{0\}$ , which we denote by  $(\det A)^{-1}$ . This is the nonzero element of the field  $K$  such that  $(\det A)^{-1}(\det A) = (\det A)(\det A)^{-1} = 1 =$  the identity element of  $K \setminus \{0\}$ . So we can solve for  $x, y, z, u$  in (D) by multiplying the equations in (D) by  $(\det A)^{-1}$ . We get

$$\begin{array}{ll} x = (\det A)^{-1}d, & y = -(\det A)^{-1}b, \\ z = -(\det A)^{-1}c, & u = (\det A)^{-1}a. \end{array}$$

Thus, if  $A$  has a right inverse at all, this right inverse must be the matrix written in the enunciation of the theorem (in particular,  $A$  has a unique

right inverse). It is easy to check that this matrix is indeed a right inverse of  $A$ :

$$\begin{aligned} & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} (\det A)^{-1}d & -(\det A)^{-1}b \\ -(\det A)^{-1}c & (\det A)^{-1}a \end{pmatrix} \\ &= \begin{pmatrix} (\det A)^{-1}(ad-bc) & (\det A)^{-1}(-ab+ba) \\ -(\det A)^{-1}(cd-dc) & (\det A)^{-1}(-cb+da) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I. \end{aligned}$$

Hence  $A$  does have a unique right inverse and it is the matrix given in this theorem.  $\square$

We will prove presently that the matrices with right inverses form a group under multiplication. From Lemma 7.3, it will then follow that the unique right inverse of a matrix with a nonzero determinant is also the unique left inverse of the same matrix. We shall refer to it as its inverse.

The rule for finding the inverse of  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is simple: interchange  $a$  and  $d$ , then put a minus sign in front of  $b$  and  $c$ , and multiply each entry by  $(\det A)^{-1}$  [i.e., divide each entry by  $\det A$ ]. For example, the inverse of

$$\begin{pmatrix} 5 & 2 \\ 1 & 2 \end{pmatrix} \in \text{Mat}_2(\mathbb{Q}) \text{ is } \begin{pmatrix} \frac{1}{8} & 2 & -\frac{1}{8} & 2 \\ -\frac{1}{8} & 1 & \frac{1}{8} & 5 \end{pmatrix} = \begin{pmatrix} 1/4 & -1/4 \\ -1/8 & 5/8 \end{pmatrix} \text{ and that of}$$

$$\begin{pmatrix} \bar{5} & \bar{2} \\ \bar{1} & \bar{4} \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}_7) \text{ is } \begin{pmatrix} \bar{2} & \bar{4} & -\bar{2} & \bar{2} \\ -\bar{2} & \bar{1} & \bar{2} & \bar{5} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{3} \\ \bar{5} & \bar{3} \end{pmatrix} \text{ since the determinant is equal to } \bar{1}\bar{8} = \bar{4} \text{ and } \bar{4}^{-1} = \bar{2}.$$

**17.9 Theorem:** *Let  $K$  be a field.*

(1)  $\det(AB) = (\det A)(\det B)$  for all  $A, B \in \text{Mat}_2(K)$ .

(2)  $\det I = 1$  ( $\in K$ ).

(3) If  $AX = I$ , then  $\det X = (\det A)^{-1}$ .

**Proof:** (1) We use the notation of Definition 17.5. We get

$$\begin{aligned} \det(AB) &= (ae + bg)(cf + dh) - (af + bh)(ce + dg) \\ &= aecf + aedh + bgcf + bgdh - afce - afdg - bhce - bhdg \\ &= aedh - afdg + bgcf - bhce \\ &= ad(eh - fg) - bc(eh - fg) \end{aligned}$$

$$\begin{aligned}
&= (ad - bc)(eh - fg) \\
&= (\det A)(\det B).
\end{aligned}$$

(2)  $\det I = 1 \cdot 1 - 0 \cdot 0 = 1 - 0 = 1$ .

(3) This follows from (1) and (2): if  $AX = I$ , then  $1 = \det I = \det(AX) = (\det A)(\det X)$ , so  $\det X = (\det A)^{-1}$ .

□

The formula  $\det AB = (\det A)(\det B)$  is known as the multiplication rule of determinants. Loosely speaking, the determinant of a product is the product of the determinants. By induction on  $n$ , it is extended to  $n$  factors:  $\det(A_1 A_2 \dots A_n) = (\det A_1)(\det A_2) \dots (\det A_n)$ .

We finally have a group of matrices under multiplication.

**17.10 Theorem:** *Let  $K$  be a field. Then*

$$\{A \in \text{Mat}_2(K) : \det A \neq 0\}$$

*is a group under matrix multiplication.*

**Proof:** We check the group axioms. Let us call our set  $G$  for brevity.

(i) For  $A, B \in G$ , we have  $\det A \neq 0 \neq \det B$ . In the field  $K$ , product of nonzero elements is nonzero ( $K \setminus \{0\}$  is a group, and closed under multiplication). So  $\det AB = (\det A)(\det B) \neq 0$  by Theorem 17.9(1) and consequently  $AB \in G$ . Thus  $G$  is closed under multiplication.

(ii) Associativity of multiplication in  $G$  follows from Theorem 17.6(2).

(iii)  $I$  is a right identity element of  $G$ , for  $\det I = 1 \neq 0$  by Theorem 17.9(2), so  $I \in G$ ; and  $AI = A$  for all  $A \in G$  by Theorem 17.6(3).

(iv) Any  $A \in G$  has a right inverse in  $G$ . Indeed, if  $A \in G$ , then  $\det A \neq 0$ , so  $A$  has a right inverse  $X$  in  $\text{Mat}_2(K)$ . As  $\det X = (\det A)^{-1} \neq 0$  (Theorem 17.9(3)), we see  $X \in G$ . Thus  $A$  has a right inverse in  $G$ .

Therefore,  $G$  is a group. □

**17.11 Definition:** Let  $K$  be a field. The group of Theorem 17.10 is called the *general linear group (of degree 2) over  $K$* , and is written as  $GL(2,K)$ .

Since  $GL(2,K)$  is a group, the unique right inverse of any matrix  $A$  in  $GL(2,K)$  is also the unique left inverse of that matrix (Lemma 7.3). It will be called the *inverse of  $A$* , and will be written as  $A^{-1}$ , in conformity with the usual terminology and notation. The matrix  $I$  will be called the *identity matrix*. Elements of  $GL(2,K)$  are called *invertible matrices* or *regular matrices*. Matrices whose determinants are zero are called *singular*.

The next theorem furnishes another matrix group.

**17.12 Theorem:** Let  $K$  be a field. Then

$$\{A \in Mat_2(K) : \det A = 1\}$$

is a group under matrix multiplication.

**Proof:** Let us call this set  $S$  for brevity. As  $1 \neq 0$  in  $K$ , we get  $S \subseteq GL(2,K)$ . We use the subgroup criterion (Lemma 9.2) to check that  $S$  is a subgroup of  $GL(2,K)$ .

(i) For  $A, B \in S$ , we have  $\det A = 1 = \det B$ , therefore  $\det AB = (\det A)(\det B) = 1 \cdot 1 = 1$  by Theorem 17.9(1) and consequently  $AB \in S$ . Thus  $S$  is closed under multiplication.

(ii) For any  $A \in S$ , we have  $\det A = 1$ , so  $\det (A^{-1}) = (\det A)^{-1} = 1^{-1} = 1$  by Theorem 17.9(3) and  $A^{-1} \in S$ . Thus  $S$  is closed under the forming of inverses.

Therefore,  $S$  is a subgroup of  $GL(2,K)$ . □

**17.13 Definition:** Let  $K$  be a field. The group of Theorem 17.12 is called the *special linear group (of degree 2) over  $K$* , and is written as  $SL(2,K)$ .

We close this paragraph with a group that plays an important role in number theory and in complex analysis.

**17.14 Theorem:** *The set*

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Q}) : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

*is a group under matrix multiplication.*

**Proof:** Let us call this set  $H$  for brevity. Clearly  $\emptyset \neq H \subseteq SL(2, \mathbb{Q})$ . We check that  $H$  is a subgroup of  $SL(2, \mathbb{Q})$ .

(i) Suppose  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  are elements of  $H$ . Then  $AB = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$ . Here the entries of  $AB$ , namely  $ae+bg$ ,  $ce+dg$ ,  $af+bh$ ,  $cf+dh$  are integers, because  $a, b, c, d, e, f, g, h$  are integers. Also,  $\det A = 1 = \det B$ , therefore  $\det AB = (\det A)(\det B) = 1 \cdot 1 = 1$  by Theorem 17.9(1) and  $AB \in H$ . Thus  $H$  is closed under multiplication.

(ii) Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$ . Then  $\det A = 1$  and so  $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$  by Theorem 17.8. The entries  $d$ ,  $-b$ ,  $-c$ ,  $a$  of  $A^{-1}$  are integers, because  $a$ ,  $b$ ,  $c$ ,  $d$  are integers. Also, we have  $\det A = 1$ , so  $\det(A^{-1}) = (\det A)^{-1} = 1^{-1} = 1$  by Theorem 17.9(3) (or  $\det(A^{-1}) = da - (-b)(-c) = ad - bc = 1$ ). So  $A^{-1} \in H$  and  $H$  is closed under the forming of inverses.

Therefore,  $H$  is a subgroup of  $SL(2, \mathbb{Q})$ . □

**17.15 Definition:** The group of Theorem 17.14 is called the *special linear group (of degree 2) over  $\mathbb{Z}$* , or the *modular group*, and is written as  $SL(2, \mathbb{Z})$  or as  $\Gamma$ .

### Exercises

1. Let  $K$  be a field. Show that  $GL(2, K)$  is not an abelian group.
2. Find all elements of  $GL(2, \mathbb{Z}_2)$ . What is the order of  $GL(2, \mathbb{Z}_2)$ ?
3. Write down the multiplication table of  $GL(2, \mathbb{Z}_2)$ . Compare it (eventually after reordering the rows and columns) with the multiplication table of  $S_3$ .

4. Find all elements of  $SL(2, \mathbb{Z}_3)$ . What is the order of  $SL(2, \mathbb{Z}_3)$ ?
5. Write down the multiplication table of  $SL(2, \mathbb{Z}_3)$
6. Let  $K$  be a field and let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ . When  $a = 0 = b$ , we have  $\det A = 0$ . In case  $(a, b) \neq (0, 0)$ , prove that  $\det A = 0$  if and only if there is an element  $k$  in  $K$  such that  $c = ka$ ,  $d = kb$ . Use this result and show that  $|GL(2, \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$ .
7. Determine how many elements in  $GL(2, \mathbb{Z}_p)$  have the same determinant. Find the order of  $SL(2, \mathbb{Z}_p)$ .
8. Show that  $\left\{ \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \in Mat_2(K) : b \neq 0 \right\}$  is a subgroup of  $GL(2, K)$ .
9. Prove that  $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in Mat_2(K) : ad \neq 0 \right\}$  is a group under multiplication. Its elements are called *triangular matrices*.
10. Let  $K$  be a field. For any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ , we define the *trace of A* to be the element  $a + d$  of  $K$  (sum of the entries in the upper-left lower-right diagonal). Show that the trace of  $AB$  is equal to the trace of  $BA$  for all  $A, B \in Mat_2(K)$ .
11. Let  $K$  be a field. For any  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ , we define the *transpose of A* to be the matrix  $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in Mat_2(K)$ , which is written  $A^t$ . Show that  $\det A^t = \det A$  and  $(AB)^t = B^t A^t$  for all  $A, B \in Mat_2(K)$ .
12. Let  $m \geq 2$  and put  $Mat_2(\mathbb{Z}_m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_m \right\}$ . Show that the theory in the text, until Theorem 17.8, remains valid for the elements of  $Mat_2(\mathbb{Z}_m)$ , which are called *matrices over  $\mathbb{Z}_m$* .
- In place of Theorem 17.8, prove that  $A \in Mat_2(\mathbb{Z}_m)$  has a unique right inverse if and only if  $\det A \in \mathbb{Z}_m^\times$ .
- Put  $GL(2, \mathbb{Z}_m) = \{A \in Mat_2(\mathbb{Z}_m) : \det A \in \mathbb{Z}_m^\times\}$ . Show that  $GL(2, \mathbb{Z}_m)$  is a group under multiplication.
- Prove that Theorem 17.12 remains true if " $K$ " is replaced by " $\mathbb{Z}_m$ ".

13. Develop a theory of matrices over  $\bar{\mathbb{Z}}$  by modifying the theory of matrices over  $\mathbb{Z}$ . How do you define  $GL(2, \bar{\mathbb{Z}})$ ?

14. Let  $H = \left\{ \begin{pmatrix} a & \bar{b} \\ -b & a \end{pmatrix} : a, b \in \mathbb{C} \right\} \subseteq Mat_2(\mathbb{C})$ , where  $\bar{x}$  is the complex conjugate of  $x \in \mathbb{C}$ . Prove that  $H$  is closed under addition and multiplication. Show that  $H \setminus \{0\}$  is a group under multiplication.

15. If  $K$  is a field and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ , we write  $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ . Let

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in Mat_2(\mathbb{C}).$$

Thus 1 is the identity matrix over  $\mathbb{C}$ . Show that  $ij = k, jk = i, ki = j$ . Prove that  $\{1, -1, i, -i, j, -j, k, -k\}$  is a group under multiplication, called a *quaternion* group of order 8 and is denoted as  $Q_8$ . Show that  $Q_8$  has exactly one element of order 2. Find all subgroups of  $Q_8$ .