

# Dummit & Foote Ch. 1.4: Matrix Groups

Scott Donaldson

Mar. 2023

## 1. (3/16/23)

Prove that  $|GL_2(\mathbb{F}_2)| = 6$ .

*Proof.* Matrices in  $GL_2(\mathbb{F}_2)$  have the form  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , where  $a, b, c, d \in \{0, 1\}$ . There are 16 possible matrices of this form (2 options for each entry over 4 entries,  $2^4 = 16$ ).

From the definition of  $GL_2$ , we discount matrices with determinant 0. A  $2 \times 2$  matrix has determinant 0 when  $ad - bc = 0$ , that is,  $ad = bc$ . This happens only when  $ad = bc = 1$  or  $ad = bc = 0$ . There is only one matrix where  $ad = bc = 1$ ,  $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ . Matrices with determinant 0 have one of  $a, d$  and  $b, c$  equal to 0. They are the matrices with all zero entries (1), with three zero entries (4), and with two zero entries ( $a$  and  $b$ , or  $a$  and  $c$ , or  $b$  and  $d$ , or  $c$  and  $d$ ) (4).

This leaves us with  $16 - 1 - 1 - 4 - 4 = 6$  matrices with nonzero determinants, so the order of  $GL_2(\mathbb{F}_2) = 6$ .  $\square$

## 2. (3/16/23)

Write out all the elements of  $GL_2(\mathbb{F}_2)$  and compute the order of each element.

- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ : 1 (identity)
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ : 2
- $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ : 2
- $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ : 3

- $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ : 3
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ : 2

### 3. (3/16/23)

Show that  $GL_2(\mathbb{F}_2)$  is non-abelian.

*Proof.* To prove that  $GL_2(\mathbb{F}_2)$  is non-abelian, we need only show that it contains two non-commuting elements. We have:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \text{ while} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Since these products are not equal,  $GL_2(\mathbb{F}_2)$  is non-abelian.  $\square$

### 4. (3/18/23)

Show that if  $n$  is not prime then  $\mathbb{Z}/n\mathbb{Z}$  is not a field.

*Proof.* Let  $n$  be a composite positive integer and let  $a$  divide  $n$  with  $a > 1$ . We will show that  $a$  does not have a multiplicative inverse in  $\mathbb{Z}/n\mathbb{Z}$ , and therefore  $\mathbb{Z}/n\mathbb{Z}$  is not a field.

We will show that there is no integer  $c$  such that  $ac = 1 \pmod{n}$ . Since  $a$  divides  $n$ , let  $ab = n = 0 \pmod{n}$ . So  $a(b+1) = ab + a = n + a = a \pmod{n}$ . That is, for the pair of consecutive integers  $b$  and  $b+1$ , we have  $ab = 0 < 1$  and  $a(b+1) = a > 1$ . Then there is no integer  $c$  strictly between  $b$  and  $b+1$  such that  $ac = 1 \pmod{n}$ . For any larger integers, we note that  $abk = nk = 0 \pmod{n}$ , and  $a(bk+1) = abk + a = nk + a = a \pmod{n}$ , and therefore there is no integer  $c$  among all of  $\mathbb{Z}^+$  with  $ac = 1$ . Therefore, since  $a$  has no multiplicative inverse,  $\mathbb{Z}/n\mathbb{Z}$  is not a field.  $\square$

### 5. (3/18/23)

Show that  $GL_n(F)$  is a finite group if and only if  $F$  has a finite number of elements.

*Proof.* Let  $F$  be a field with  $m < \infty$  elements and, for some  $n > 1$ , let  $GL_n(F)$  be the general linear group of degree  $n$  on  $F$ . The total possible number of  $n \times n$  matrices with entries from  $F$  is  $m^{n^2}$ . Since the number of elements in  $GL_n(F)$  is at most this value, it is a finite group (in 6. we will show that it is strictly less than).

To prove the converse, we will show that, if  $F$  is an infinite field, then  $GL_n(F)$  must not be a finite group. Let  $F$  be an infinite field. For every  $x \in F$  (excluding  $x = 0$ ), we can construct an  $n \times n$  matrix whose diagonal entries are  $x$  and all other entries are 0. By definition, the determinant of such a matrix is the product of the diagonal entries,  $x^n \neq 0$ . Therefore such a matrix belongs to  $GL_n(F)$ . This is a bijection between  $F$  and  $GL_n(F)$ , and so they have the same cardinality, that is,  $GL_n(F)$  must not be a finite group.

Thus,  $GL_n(F)$  is a finite group if and only if  $F$  has a finite number of elements.  $\square$

## 6. (3/19/23)

If  $|F| = q$  is finite prove that  $|GL_n(F)| < q^{n^2}$ .

*Proof.* An element of  $GL_n(F)$  is an invertible  $n \times n$  matrix whose entries come from  $F$ . For each entry, there are  $q$  possibilities, and there are  $n^2$  total entries, so there are  $q^{n^2}$  possible such matrices (before discounting those with determinant = 0). It is guaranteed that some number of  $n \times n$  matrices have determinant 0; for example, the matrix whose entries are all 0 obviously has determinant 0. So the number of elements of  $GL_n(F)$  is always strictly less than  $q^{n^2}$ .  $\square$

## 7. (3/19/23)

Let  $p$  be a prime. Prove that the order of  $GL_2(\mathbb{F}_p)$  is  $p^4 - p^3 - p^2 + p$ .

*Proof.* From 5. and 6., there are  $p^{2^2} = p^4$  possible  $2 \times 2$  matrices, and the order of  $GL_2(\mathbb{F}_p)$  is strictly less than this number. Let us count the ways in which an element of  $GL_2(\mathbb{F}_p)$  might have a determinant equal to 0.

A  $2 \times 2$  matrix in  $GL_2(\mathbb{F}_p)$  has the form  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , with  $a, b, c, d \in \mathbb{F}_p$ . The determinant of a  $2 \times 2$  matrix is  $ad - bc$ . First, consider the cases in which  $a, b, c, d \neq 0$ . Setting the determinant equal to 0, we can see that  $d$  must equal  $bc/a$ . So there are  $p - 1$  choices for  $a, b, c$ , and  $d$  is fixed based on the other entries. Then there are  $(p-1)^3$  matrices with 4 nonzero entries with determinant equal to 0.

Next, consider  $2 \times 2$  matrices with one entry equal to 0, for example,  $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ . The determinant of this matrix is  $a \cdot 0 - bc = -bc$ . In order for this to equal 0, at least one of either  $b$  or  $c$  must equal zero. Then there are no matrices with exactly 1 zero entry with determinant equal to 0.

Now consider  $2 \times 2$  matrices with two entries equal to 0. Such matrices have the form  $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$ , or  $\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}$ . There are  $p - 1$  possible choices for both of the nonzero entries, so there are  $4(p - 1)^2$  matrices with exactly 2 nonzero entries with determinant equal to 0.

Matrices with three entries equal to 0 have the form  $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix},$  or  $\begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}.$  There are  $4(p-1)$  such matrices.

Finally, there is the single matrix with all 0 entries,  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$

So, the total number of elements of  $GL_2(\mathbb{F}_p)$  is:

$$\begin{aligned} p^4 - (p-1)^3 - 4(p-1)^2 - 4(p-1) - 1 &= \\ p^4 - (p^3 - 3p^2 + 3p - 1) - (4p^2 - 8p + 4) - (4p - 4) - 1 &= \\ p^4 - p^3 + 3p^2 - 3p + 1 - 4p^2 + 8p - 4 - 4p + 4 - 1 &= \\ p^4 - p^3 + (3-4)p^2 + (-3+8-4)p + (1-4+4-1) &= \\ p^4 - p^3 - p^2 + p & \end{aligned}$$

as desired.  $\square$

## 8. (3/21/23)

Show that  $GL_n(F)$  is non-abelian for any  $n \geq 2$  and  $F$ .

*Proof.* To show that  $GL_n(F)$  is non-abelian, we need to show that it contains two elements that are noncommutative. By definition of general linear groups,  $GL_n(F)$  consists of invertible  $n \times n$  matrices whose entries come from the field  $F$ . Further, by definition of fields,  $F$  contains an additive identity 0 and a multiplicative identity 1. Therefore, if we consider only matrices in  $GL_n(F)$  whose entries are 0 or 1 and whose product's entries are 0 or 1 (in  $\mathbb{Z}$ ), these are elements of every  $GL_n(F)$  regardless of which  $F$  we choose.

Let  $A$  be the transpose of the identity matrix and let  $B$  be equal to the identity matrix with the final two columns swapped:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

The upper-right entry of  $AB$  is the dot product of the first row of  $A$  with the last column of  $B$ :  $0 \cdot 0 + 0 \cdot 0 + \dots + 0 \cdot 1 + 1 \cdot 0 = 0$ .

The upper-right entry of  $BA$  is the dot product of the first row of  $B$  with the last column of  $A$ :  $1 \cdot 1 + 0 \cdot 0 + \dots + 0 \cdot 0 + 0 \cdot 0 = 1$ .

Because  $AB$  and  $BA$  do not contain exactly the same entries, they are not equal matrices. Therefore,  $A$  and  $B$  do not commute. Further, because for every  $n \geq 2$  and every field  $F$ ,  $GL_n(F)$  contains the elements  $A$  and  $B$ ,  $GL_n(F)$  is non-abelian.  $\square$

## 9. (3/21/23)

Prove that the binary operation of multiplication of  $2 \times 2$  matrices is associative.

*Proof.* Let  $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ ,  $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ ,  $C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$ .

$$\begin{aligned}
 A(BC) &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \left( \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right) \\
 &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix} \\
 &= \begin{pmatrix} a_1(b_1c_1 + b_2c_3) + a_2(b_3c_1 + b_4c_3) & a_1(b_1c_2 + b_2c_4) + a_2(b_3c_2 + b_4c_4) \\ a_3(b_1c_1 + b_2c_3) + a_4(b_3c_1 + b_4c_3) & a_3(b_1c_2 + b_2c_4) + a_4(b_3c_2 + b_4c_4) \end{pmatrix} \\
 &= \begin{pmatrix} (a_1b_1 + a_2b_3)c_1 + (a_1b_2 + a_2b_4)c_3 & (a_1b_1 + a_2b_3)c_2 + (a_1b_2 + a_2b_4)c_4 \\ (a_3b_1 + a_4b_3)c_1 + (a_3b_2 + a_4b_4)c_3 & (a_3b_1 + a_4b_3)c_2 + (a_3b_2 + a_4b_4)c_4 \end{pmatrix} \\
 &= \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \\
 &= \left( \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \right) \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \\
 &= (AB)C.
 \end{aligned}$$

□

## 10. (3/22/23)

Let  $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$ .

- (a) Compute the product of  $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$  and  $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$  to show that  $G$  is closed under matrix multiplication.

$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$ .  $\mathbb{R}$  is closed under addition and multiplication, so the entries of the matrix product are all in  $\mathbb{R}$ , and so the product is an element of  $G$ .

- (b) Find the matrix inverse of  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  and deduce that  $G$  is closed under inverses.

The inverse of  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  is the  $2 \times 2$  matrix  $\begin{pmatrix} d & e \\ f & g \end{pmatrix}$  such that

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ f & g \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Looking at lower-left entry first, we have  $0 \cdot d + cf = 0$ . We know that  $c$  is nonzero, so  $f = 0$ .

Next, looking at the upper-left entry, we have  $ad + b \cdot 0 = 1 \Rightarrow ad = 1$ . So  $d = 1/a$ . Similarly for the lower-right entry,  $cg = 1 \Rightarrow g = 1/c$ .

Finally, looking at the upper-right entry, we have  $ae + bg = ae + b/c = 0$ .

So  $e = -b/ac$ . Therefore the inverse matrix is  $\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$ .

- (c) Deduce that  $G$  is a subgroup of  $GL_2(\mathbb{R})$ .

From 9., matrix multiplication is associative for  $2 \times 2$  matrices. As shown in a),  $G$  is closed under the operation of matrix multiplication, and in b), inverses of elements in  $G$  are also in  $G$ . Thus  $G$  is a subgroup of  $GL_2(\mathbb{R})$ .

- (d) Prove that the set of elements of  $G$  whose diagonal entries are equal (i.e.  $a = c$ ) is also a subgroup of  $GL_2(\mathbb{R})$ .

Now let  $H$  be the set of elements of  $G$  whose diagonal entries are equal; that is, matrices of the form  $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a \neq 0$ .

$H$  is closed under matrix multiplication:

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix}.$$

From b), the inverse of  $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$  is  $\begin{pmatrix} 1/a & -b/a^2 \\ 0 & 1/a \end{pmatrix}$ , which is also in  $H$ .

Thus this set is also a subgroup of  $GL_2(\mathbb{R})$ .

## 11. (3/23/23)

Let  $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$  — called the *Heisenberg group* over  $F$ .

Let  $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$  and  $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$  be elements of  $H(F)$ .

- (a) Compute the matrix product  $XY$  and deduce that  $H(F)$  is closed under matrix multiplication. Exhibit explicit matrices such that  $XY \neq YX$  (so that  $H(F)$  is always non-abelian).

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+e+af \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}.$$

Given this product, the only entry that has a different value when the order of multiplication is reversed is the upper-right, which is  $b + e + af$

for  $XY$  and  $b+e+cd$  for  $YX$ . So we need to find  $af \neq cd$ . Let  $a = f = 1$  and  $c = d = 0$ .

Then:

$$XY = \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & e \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & b+e+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and}$$

$$YX = \begin{pmatrix} 1 & 0 & e \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & b+e \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

For no  $b, e \in F$  is it possible for  $b+e$  to equal  $b+e+1$ . Thus  $H(F)$  is non-abelian.

- (b) Find an explicit formula for the matrix inverse  $X^{-1}$  and deduce that  $H(F)$  is closed under inverses.

Suppose  $D = \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{pmatrix}$  such that  $XD = I_3$ . Carrying out the multiplication, we obtain the following set of equations:

- $d_{11} + ad_{21} + bd_{31} = 1$
- $d_{12} + ad_{22} + bd_{32} = 0$
- $d_{13} + ad_{23} + bd_{33} = 0$
- $d_{21} + cd_{31} = 0$
- $d_{22} + cd_{32} = 1$
- $d_{23} + cd_{33} = 1$
- $d_{31} = 0$
- $d_{32} = 0$
- $d_{33} = 1$

Substituting  $d_{31} = d_{32} = 0, d_{33} = 1$  into the first equations, we obtain the following:

- $d_{11} + ad_{21} = 1$
- $d_{12} + ad_{22} = 0$
- $d_{13} + ad_{23} + b = 0$
- $d_{21} = 0$
- $d_{22} = 1$
- $d_{23} + c = 1$

So we have  $d_{23} = -c$ , and substituting that, as well as  $d_{21} = 0, d_{22} = 1$  into the above, we obtain:

- $d_{11} = 1$

- $d_{12} + a = 0$
- $d_{13} - ac + b = 0$

Then  $D = \begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ . Since  $XD = I_3$ ,  $D = X^{-1}$ , and we see that  $H(F)$  is closed under inverses.

- (c) Prove the associative law for  $H(F)$  and deduce that  $H(F)$  is a group of order  $|F|^3$ .

Since  $H(F)$  is closed under matrix multiplication, we can ignore all but the upper-triangular entries (upper-middle, upper-right, and middle-right), since they will always be either 0 or 1.

From a), the upper-middle and middle-right entries of  $XY$  are  $a + d$  and  $c + f$ , respectively. If we multiply their product by a third matrix, these entries will be the sum of the respective entries of the three entries, which is associative.

The upper-right entry of  $XY$  is  $b + e + af$ . Let  $Z$  be a matrix with upper-triangular entries  $g, h, i$ . Then  $(XY)Z$  has the upper-right entry  $(b + e + af) + h + (a + d)i = b + e + h + af + ai + di$ . The upper-right entry of  $X(YZ)$  is  $(e + h + di) + b + a(f + i) = b + e + h + af + ai + di$ . Thus,  $(XY)Z = X(YZ)$ , and so  $H(F)$  is associative.

Since  $H(F)$  is closed under matrix multiplication, inverses, and is associative, it is a group. In choosing elements of  $H(F)$ , we can freely choose from three elements  $a, b, c \in F$ . Therefore  $|H(F)| = |F|^3$ .

- (d) Find the order of each element of the finite group  $H(\mathbb{Z}/2\mathbb{Z})$ .

- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : 1$
- $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : 2$
- $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : 2$
- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} : 2$
- $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : 2$



- $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} : 3$
- $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} : 2$
- $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} : 3$

(e) Prove that every nonidentity element of the group  $H(\mathbb{R})$  has infinite order.

*Proof.* Let  $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R})$ . We will show by induction that the upper-middle, upper-right, and middle-right entries of  $X^n$  are  $na$ ,  $(n(n-1)/2)ac + nb$ , and  $nc$ , respectively.

For the base case,  $X^1 = X$  has the upper-middle, upper-right, and middle-right entries  $a = 1 \cdot a$ ,  $b = 0 \cdot ac + 1 \cdot b$ ,  $c = 1 \cdot c$ .

For the induction step, suppose for  $X^n$ , the relevant entries are  $na$ ,  $(n(n-1)/2)ac + nb$ , and  $nc$ . Then

$$X^{n+1} = X^n X = \begin{pmatrix} 1 & na & (n(n-1)/2)ac + nb \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & (n+1)a & b + nac + (n(n-1)/2)ac + nb \\ 0 & 1 & (n+1)c \\ 0 & 0 & 1 \end{pmatrix}. \text{ The upper-middle and middle-right entries satisfy the induction hypothesis, and the upper-right entry is:}$$

$$\begin{aligned} b + nac + (n(n-1)/2)ac + nb &= (n + n(n-1)/2)ac + (n+1)b = \\ ((2n + n^2 - n)/2)ac + (n+1)b &= ((n^2 + n)/2)ac + (n+1)b = \\ &= (n(n+1)/2)ac + (n+1)b. \end{aligned}$$

Thus,  $X^{n+1}$  satisfies the induction hypothesis.

Now if  $|X| < \infty$ , then for some  $n$ ,  $X^n = I_3$ . So we need:

$na = (n(n-1)/2)ac + nb = nc = 0$ . For  $na$  and  $nc$ , since  $n > 0$ , we need  $a = c = 0$ . Then  $nb = 0$ , so  $b = 0$ . Therefore the identity matrix is the only element of  $H(\mathbb{R})$  with finite order.  $\square$