Section 1.4: Matrix Groups

Juan Patricio Carrizales Torres

May 8, 2023

Before describing the matrix group, we must define what a *field* is. A field is a set F with two binary operations $+$ and $\cdot$ such that both $(F, +)$ and $(F/\{0\}, \cdot)$ are abelian groups. Also, the distributive law holds, namely, for any $a, b, c \in F$

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Then, the general linear group $GL_n(F)$ is the set of all $n \times n$ matrices with entries from the field F and nonzero determinant, where the associative matrix multiplication is the binary operation. Two useful results regarding general linear groups are the following:

(a) if F is a finite field, then $|F| = p^m$ for some prime p and integer m.

(b) if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$.

1 PROBLEMS

Let F be a field and let $n \in \mathbb{Z}^+$.

Problem 1. Prove that $|GL_2(F_2)| = 6$

Proof. This general linear group $GL_2(F_2)$ contains 2×2 matrices

$$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix},$$

where $b_1, b_2, b_3, b_4 \in F_2$ and $b_3 \cdot b_2 - b_4 \cdot b_1 \neq 0$ (nonzero determinant). Then, $b_3 \cdot b_2 \neq b_4 \cdot b_1$ (Recall that $\cdot$ is the binary operation in F_2 such that $(F_2/\{0\}, \cdot)$ is a group). Then, the statement $|GL_2(F_2)| = 6$ is equivalent to saying that there are 6 possible unique equations $b_3 \cdot b_2 \neq b_4 \cdot b_1$ for elements $b_1, b_2, b_3, b_4 \in F_2$. Let's call the instance $b \cdot a$ a *binary multiplication*. Because multiplication is closed, it follows that it is equal to some element inside F_2 and so we must find all ways to accomodate *binary multiplications* in the equation such that one side is 0 and the other is 1. Before doing that, we have to look at the 4 possible *binary* *multiplications*. We know that 0 is the *additive identity* and that the other element 1 is the *multiplicative identity* and its own additive and multiplicative inverse. Then, it follows that

$$\begin{aligned} 0 \cdot 1 &= (1+1) \cdot 1 = 1 \cdot 1 + 1 \cdot 1 \\ &= 0 + 0 = 0 \\ &= 0 \cdot 0 = 0 \cdot (1+1) \\ &= 0 \cdot 1 + 0 \cdot 1 = 0 + 0. \end{aligned}$$

and $1 \cdot 1 = 1$. Then, all binary multiplications, except for $1 \cdot 1$, are equal to 0.
Now, let one side of the equation be 1, which there is only one binary multiplication able to represent that, namely, $1 \cdot 1$. Then, we only have 3 binary multiplications out of the possible 4 that we can place at the other side such that two sides are not equal $(1 \cdot 0, 0 \cdot 1, 0 \cdot 0)$. Hence, per side there are 3 possible non equal equations and so there are 6 possible equations such that the binary multiplications at each side are not equal. □

Problem 2. Write out all the elements of $GL_2(F_2)$ and compute the order of each element.

Solution We have the following elements with their respective orders (n):

$$\begin{aligned} &\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, n = 2 \\ &\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, n = 2 \\ &\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, n = 1 (\text{identity matrix}) \\ &\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, n = 3 \\ &\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, n = 3 \\ &\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, n = 2 \end{aligned}$$

Problem 3. Show that $GL_2(F_2)$ is non-abelian.

Proof. Note that

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &\neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

□

Problem 4. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Proof. Suppose that n is not prime. Then, there is at least one integer $1 < k < n$ that is a factor. Hence, $n = kq_1q_2 \ldots q_m$ and so $l = q_1q_2 \ldots q_m$ is an integer (factor) such that $1 < l < n$ and $k \cdot l = n$. Therefore, $\overline{k}, \overline{l}$ are two elements in $\mathbb{Z}/n\mathbb{Z}$ such that $\overline{k} \cdot \overline{l} = \overline{k \cdot l} = \overline{n} = \overline{0}$, the additive identity. Hence, $\mathbb{Z}/n\mathbb{Z}^{\times}$ is not closed under multiplication, which implies that it is not a group. $\square$

Problem 5. Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

Proof. First assume that $|F| = n$ for some $n \in \mathbb{N}$. Then, there are n possible ways to accomodate the n elements in an entry. Therefore, there are $n^{n \times n}$ different ways to accomodate the elements of F in the entries of a $n \times n$ matrix. Then, $|GL_n(F)| \leq n^{n \times n}$ which is finite. Now, for the converse, assume that F has an infinity of elements. Note that the set of diagonal matrices

$$D = \{A = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix} |\det(A) \neq 0 \iff d_1, d_2, \ldots, d_n \neq 0\}$$

is a subgroup of $GL_n(F)$, namely the inverse of a diagonal matrix with nonzero determinant is a diagonal matrix with nonzero determinant, and the multiplication of two diagonal matrices with nonzero determinant results in a diagonal matrix with nonzero determinant. We show that one can construct an infinity ofdiagonal matrices with nonzero determinant. Note that, for some fixed $a \in F/\{0\}$ and every $b \in F/\{0\}$,

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & b \end{pmatrix}$$

is a diagonal matrix with nonzero determinant. Hence, D has an infinity of elements and so $GL_n(F)$ has an infinity of elements. $\square$

Problem 10. Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} |a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$.

(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.

Solution Note that

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}.$$

Because $a_1, a_2, c_1, c_2 \neq 0$, it follows that $a_1a_2, c_1c_2 \neq 0$ and so G is closed under matrix multiplication.

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

Solution Consider some element $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ of G. Since $A \in G$ it follows that $a_1, c_1 \neq 0$. According to the result of the matrix multiplication showed in (a), for B to be an inverse of A it must be true that $a_1 a_2 = c_1 c_2 = 1$ and $a_1 b_2 + b_1 c_2 = 0 \iff a_1 b_2 = -b_1 c_2$.

Then, $a_2 = a_1^{-1} \neq 0, c_2 = c_1^{-1} \neq 0$ and $b_2 = (-b_1)c_1^{-1}a_1^{-1}$ which are elements of the field F. Hence, the inverse of A exists in G. Thus, G is closed under inverses.

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

Solution The set G over $\mathbb{R}$ is closed under matrix multiplication, closed under inverses and there is the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence, G is a group. Furthermore, note that for any $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ in G, $ac - 0 \neq 0$ (nonzero determinant). Thus, G is a subgroup of $GL_2(\mathbb{R})$.

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

Proof. Let the set in question be represented by B. From (a) we know that the matrix multiplication of two elements in B results in the matrix $\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}$, where $a_1 a_2 = c_1 c_2$ since $a_1 = c_1$ and $a_2 = c_2$. Hence, B is closed under matrix multiplication.

From (b), the inverse of any matrix in $B \subseteq G$ is represented by $\begin{pmatrix} a^{-1} & (-b)c^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix}$, where $a^{-1} = c^{-1}$ since $a = c$ (in the group $F^\times$ the inverses are unique). Therefore, B is closed under matrix multiplication.
Finally, the identity matrix is an element of B. Hence, B is a subgroup of $GL_2(\mathbb{R})$. $\square$

The next exercise introduces the *Heisenberg group* over the field F and develops some of its basic properties.

Problem 11. Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} | a, b, c \in F \right\}$ —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 $H(F)$ non-abelian).

Proof. First we show that $H(F)$ is closed under matrix multiplication. Note that

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

Since F is closed under addition and multiplication ($0a = 0$ for all $a \in F$) it follows that $d+a, e+fa+b, f+c \in F$. Thus, $H(F)$ is closed under matrix multiplication. Furthermore, note that $e+fa+b = b+cd+e$ (the left hand side comes from the entry $(1,3)$ of the matrix YX) is not true when $fa = 0$ and $cd = 1$, the additive and multiplicative identities, respectively. Hence, $H(F)$ is non-abelian. $\square$

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

Proof. Note that for $Y = X^{-1}$ to be true a necessary and sufficient condition is that $d = -a$, $f = -c$ and $e = ca - b$. Note that $-a, -c, ca - b \in F$ and so $H(F)$ is closed under inverses. $\square$

(c) Prove the associative law for $H(f)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

Proof. Consider the matrices $X, Y, Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned} (XY)Z &= \begin{pmatrix} 1 & d+a & e+fa+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & g+d+a & h+(d+a)i+e+fa+b \\ 0 & 1 & i+f+c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d+g & e+di+h \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= X(YZ). \end{aligned}$$

Hence, the matrix multiplication in $H(F)$ is associative. In order to calculate the order of $H(F)$, we consider how many matrices can be constructed using the given conditions as restrictions. Consider the matrix X. It is a "squeleton" for any matrix element of $H(G)$, where the only values that can be changed are a, b, c. Since $a, b, c \in F$, it follows, in the case that F is finite, that there are $|F| \cdot |F| \cdot |F|$ possible combinations of a, b, c and so the order of $H(F)$ is $|F|^3$. Clearly, if F is infinite then $H(F)$ is infinite. $\square$

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

Proof. □

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

Proof. **Lemma e.1.** Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(F)$ for some field F. Then,

$$X^n = \begin{pmatrix} 1 & n \cdot a & n \cdot b + m \\ 0 & 1 & n \cdot c \\ 0 & 0 & 1 \end{pmatrix},$$

where $m \in F$ and $n \in \mathbb{N}$.

Proof. We proceed by induction. By **(a)**, $X^2 = \begin{pmatrix} 1 & 2a & 2b + ca \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$. Hence, the result is true for $n = 2$. Now, assume that the result is true for X^k for some $k \in \mathbb{N}$. We show that it follows that the result is true for X^{k+1}. We know that,

$$\begin{aligned} X^{k+1} = X^k X &= \begin{pmatrix} 1 & k \cdot a & k \cdot b + m \\ 0 & 1 & k \cdot c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & k \cdot a + a & k \cdot b + m + b + k \cdot ac \\ 0 & 1 & c + k \cdot c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (k+1)a & (k+1)b + (m + k \cdot ac) \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Since $m + k \cdot ac \in F$ (closed under addition and multiplication) it follows that the result is true for X^{k+1}. By the Principle of Mathematical Induction, the result is true. □

Consider some nonidentity element $X \in H(F)$. Then, at least one of the variables a, b, c is nonzero. Then, for some $n \in \mathbb{N}$, at least one of the elements $n \cdot a, n \cdot b, n \cdot c$ is nonzero. By **Lemma e.1**, X^n is a nonidentity matrix for any $n \in \mathbb{N}$. Hence, every nonidentity element of $H(F)$ has infinite order. □