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 2×2 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.

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

However, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. These products are not equal, so $GL_2(\mathbb{F}_2)$ 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 $ac = 1 \bmod n$. Since a divides n, let $ab = n = 0 \bmod n$. So $a(b+1) = ab + a = n + a = a \bmod n$. 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 $ac = 1 \bmod n$. For any larger integers, we note that $abk = nk = 0 \bmod n$, and $a(bk+1) = abk + a = nk + a = a \bmod n$, 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. □

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}. □

7. (3/19/23)

Let p be a prime. Prove that the order of $GL_2(F_p)$ is $p^4 - p^3 - p^2 + p$.

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

A 2×2 matrix in $GL_2(F_p)$ has the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $a, b, c, d \in F_p$. The determinant of a 2×2 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 2×2 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 2×2 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 $GL_2(F_p)$ is:

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

as desired. □