18 Matrix groups (11/03)

Definition 18.1. Let k be a field (such as $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{F}_p = \mathbf{Z}/p$ for some prime number p) or even a commutative ring (such as $\mathbf{Z}$). Let $n \geqslant 0$ and let $\mathrm{M}_n(k)$ be the set of all $n \times n$-matrices with coefficients in k. We make $\mathrm{M}_n(k)$ into a magma via the binary operation of matrix multiplication. If M and N are $n \times n$-matrices, then the ijth entry of MN is

$$\sum_{k=1}^{n} M_{ik} N_{kj}.$$

It easy to see that this is a unital magma with identity element I_n, the diagonal matrix with 1s on the diagonal. It is less pleasant to see directly from the definition that matrix multiplication is associative.

Lemma 18.2. *Matrix multiplication makes* $\mathrm{M}_n(k)$ *into a monoid.*

Proof. We have already observed that there is a two-sided identity element I_n. To prove associativity we argue as follows. We can identify $\mathrm{M}_n(k)$ as the set of linear transformations $F\colon k^n \to k^n$, where k^n is the n-dimensional vector space over k equipped with the standard basis $e_1, \ldots, e_n$. Then, recall that M corresponds to the linear transformation $F(e_j) = \sum_{i=1}^{n} m_{ij} e_j$. Linear transformations are certain functions from k^n to itself. Thus, we have an inclusion of sets $\mathrm{M}_n(k) \to \mathrm{Fun}(k^n, k^n)$, where the right-hand side is the set of *all* functions $k^n \to k^n$. The right-hand side has a natural magma structure given by composition of functions. This magma is in fact a monoid. The identity element is the identity function; associativity follows from the fact that function composition is associative. Now, the inclusion $\mathrm{M}_n(k) \to \mathrm{Fun}(k^n, k^n)$ is a magma homomorphism that sends I_n to the identity element. As this homomorphism of magmas is injective and as $\mathrm{Fun}(k^n, k^n)$ is associative, it follows that $\mathrm{M}_n(k)$ is associative too. □

Remark 18.3. For commutative rings k a similar argument works, but one replaces the phrase "vector space" with k-module. Alternatively, for a ring like $\mathbf{Z}$, one can use the inclusion $\mathrm{M}_n(\mathbf{Z}) \subseteq \mathrm{M}_n(\mathbf{Q})$.

Lemma 18.4. *If M is a monoid and $U \subseteq M$ is the subset of elements of M with a two-sided inverse, then U is a group, called the maximal subgroup of M.*

Proof. As U contains the identity element and every element of U has an inverse, it is enough to show that U is closed under multiplication in M (as then associativity follows from that of M). But, if $u, v \in U$ with two-sided inverses u^{-1} and v^{-1}, then uv has two sided inverse $v^{-1}u^{-1}$ by associativity. □

Definition 18.5. If k is a field (or a ring), then $\mathbf{GL}_n(k) \subseteq \mathrm{M}_n(k)$ is the maximal subgroup of $\mathrm{M}_n(k)$. I.e., $\mathbf{GL}_n(k)$ consists of those matrices with a two-sided inverse.

Remark 18.6. Recall the determinant function $\det\colon \mathrm{M}_n(k) \to k$. It satisfies $\det(MN) = \det(M)\det(N)$ and is thus a monoid homomorphism (where k is equipped with the multiplicative monoid structure). The invertible matrices are precisely those M such that $\det(M)$ is a unit in k. The restriction of det to $\mathbf{GL}_n(k)$ induces a surjective group homomorphism $\det\colon \mathbf{GL}_n(k) \to k^\times$.

Definition 18.7. We let $\mathbf{SL}_n(k) = \ker(\det)$. It is the subgroup of invertible matrices whose determinant is 1.

Lemma 18.8. *The center of $\mathbf{GL}_n(k)$ consists of the matrices uI_n where $u \in k^\times$.*

Example 18.9 (Order of $\mathbf{GL}_2(\mathbf{F}_p)$)**.** Consider a prime p and the finite group $\mathbf{GL}_2(\mathbf{F}_p)$. First, what is its order? Well, $\mathbf{GL}_2(\mathbf{F}_p)$ is also the set of group homomorphisms $\mathbf{Z}/p \times \mathbf{Z}/p \to \mathbf{Z}/p \times \mathbf{Z}/p$ and so it acts on the non-zero elements of $\mathbf{Z}/p \times \mathbf{Z}/p$ of which there are $p^2 - 1$. What is the stabilizer of $(1, 0)$? Solving

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

we see that the stabilizer consists of those invertible matrices such that $a = 1$ and $c = 0$. Thus, since such a matrix has $\det(M) = d$, we have that $d \in k^\times$ and b can be anything. Thus, there are $p(p-1)$ elements in the stabilizer. It follows that

$$|\mathbf{GL}_2(\mathbf{F}_p)| = p(p-1)^2(p+1).$$

Note that $\mathbf{GL}_n(\mathbf{F}_p)$ is non-abelian for $n \geqslant 2$. In particular, we have $|\mathbf{GL}_2(\mathbf{F}_2)| = 6$ and thus it must be isomorphic to S_3. This corresponds to the permutations of the 3 non-zero elements of $\mathbf{Z}/2 \times \mathbf{Z}/2$.

Example 18.10 (p-Sylow subgroups of $\mathbf{GL}_2(\mathbf{F}_p)$)**.** Fix a prime p and let P be a p-Sylow subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$. We see from the computation of the order that $P \cong \mathbf{Z}/p$. How many p-Sylows are there? We can write down one as

$$P = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\},$$

where $*$ can be any element of $\mathbf{F}_p$. This is *not* normal. What's the easiest way to see this? Well,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

is another order p element not in P! So, $n_p > 1$. Let's see the stabilizer of $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ under conjugation. We solve

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

subject to the constraint that $ad - bc \neq 0$. We get

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

which implies $c = 0$, $a = d$, and $a^2 \neq 0$, or $a \neq 0$. So, these are the matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a \neq 0$. There are $(p-1)p$ of these. Thus, it follows that there are $(p-1)(p+1) = \frac{|\mathbf{GL}_2(\mathbf{F}_p)|}{(p-1)p}$ conjugates of u. What happens if instead we solve for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

for $1 \leqslant k \leqslant p-1$? We get

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix},$$

which implies $kc = 0$, which implies $c = 0$ and $a = kd$, with $d \neq 0$. These are the matrices of the form

$$\begin{pmatrix} kd & b \\ 0 & d \end{pmatrix}.$$

In particular, the powers u^k of u are indeed conjugate to u. It follows finally that there are $p+1$ subgroups obtained by conjugating P and hence $n_p = p+1$. (This matches up out with our knowledge that $S_3 \cong \mathbf{GL}_2(\mathbf{F}_2)$ has 3 2-Sylow subgroups.)

18.1 Exercises

Exercise 18.1. Let k be a field. Show that the center of $\mathbf{GL}_n(k)$ consists of the matrices uI_n where $u \in k^\times$.

Exercise 18.2. Let p be a prime. Determine the center of $\mathbf{SL}_2(\mathbf{F}_p)$.

Exercise 18.3. Fix a prime number p. Let $\mathbf{PGL}_n(\mathbf{F}_p)$ be the quotient of $\mathbf{SL}_n(\mathbf{F}_p)$ by its center. Compute the order of $\mathbf{PGL}_2(\mathbf{F}_p)$.[1]

Exercise 18.4. Find the number of p-Sylow subgroups in $\mathbf{SL}_2(\mathbf{F}_p)$.

Exercise 18.5. Find the number of p-Sylow subgroups in $\mathbf{PGL}_2(\mathbf{F}_p)$.

[1] Arguably a better definition of $\mathbf{PGL}_n(\mathbf{F}_p)$ is as the quotient of $\mathbf{GL}_n(\mathbf{F}_p)$ by *its* center, but this is the standard definition in the field of group theory. Are these two groups isomorphic?