Math 250A Lecture 3 Notes

Daniel Raban

August 31, 2017

1 Non abelian groups of order 8

1.1 The dihedral group

Last time we found two nonabelian groups of order 8, the dihedral group D_8 (the symmetries of a square) and the quaternion group Q_8.

Problem: How many ways are there to arrange 8 non-attacking rooks on a chessboard? Here, non-attacking means that two rooks cannot be placed in the same row or column. There are 8 choices of where to put a rook in the first row, 7 places of where to put a rook in the second row, and so on. So the number of ways is 8!.

Consider a modification to this problem: how many ways are there to do the above up to symmetry? Well, D_8 acts on the configurations by acting on the chessboard. How many orbits are there?

Theorem 1.1 (Burnside[1]). *Suppose a group $G \circlearrowright S$. Then the number of orbits under this action is equal to the average number of fixed points of the action. That is,*

$$|\{\mathit{Orbits}\}| = \frac{1}{|G|} \sum_{g \in G} f(g),$$

where $f(g)$ is the number of elements of S fixed by g.

Proof. Look at the set of pair (g, s) with$g \cdot s = s$. Count the number of pairs in two ways:

Method 1: For each g, there are $f(g)$ choices for s. So we get $\sum_{g \in G} f(g)$.

Method 2: Look at one orbit of G of S. Say the orbit contains some $s \in S$. By Lagrange's theorem, the number of points in the orbit is $|G| / |G_s|$, where G_s is the stabilizer of s. So $|G| = |\text{Orbit}| \times |\text{number of elements in } G \text{ fixing a point of the orbit}|$. This means that the number of elements of G fixing a point in the orbit is the same for each point in the orbit. Then

$$|\text{pairs } (g, s)| = \sum_{\text{orbits}} |\{\text{pairs in orbit}\}|$$

[1] Many mathematicians have proved this independently of each other, so we could really put anyone's name here.

$$
\begin{aligned}
&= \sum_{\text{orbits}} |\text{Orbit}| \times |\text{number of elements in } G \text{ fixing a point of the orbit}| \\
&= \sum_{\text{orbits}} |G| \\
&= |G| \times |\{\text{Orbits}\}| \,.
\end{aligned}
$$

Dividing both our results by $|G|$ gives us the desired equality. $\square$

Definition 1.1. Two elements $s, b \in G$ are *conjugate* if there exists some $g \in G$ such that $a = gbg^{-1}$. Informally, elements are conjugate if they "sort of look the same."

The elements of D_8 that are conjugate will have the same number of fixed points. To calculate the number of configurations fixed by each conjugacy class, it is helpful to draw pictures and eliminate rows based on the symmetries.

Conjugacy classes of G	number of configurations fixed by element
identity	$8! = 40320$
reflections parallel to sides	$2 \times 0 = 0$
switch both diagonals	$8 \times 6 \times 4 \times 2 = 384$
rotation by $\pi/2$	$2 \times (6 \times 2) = 24$
reflection along a diagonal	$2 \times 764 = 1528$

The most tricky of these is the last one; let c_n be the desired number (not yet multiplied by 2, the size of the conjugacy class), where the chessboard is $n \times n$. then we have a few possibilities: if we place a rook in the top left corner, then there are c_{n-1} ways to arrange other rooks. If we place a rook elsewhere in row 1, we have c_{n-2} ways to arrange the other rooks. So we get a recurrence relation $c_n = c_{n-1} + (n-1)c_{n-2}$, and we can solve to get $c_8 = 764$.

These sum up to be 42256, so using the above theorem, we have our final answer as $42256/8 = 5282$ configurations.

1.2 Quaternions

We can represent quaternions using complex matrices:

$$
1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}
$$

Any nonzero quaternion has an inverse. Conjugate $\bar{z} = a - bI - cJ - dK$, so $z\bar{z} = a^2 + b^2 + c^2 + d^2$. Then $z^{-1} = 1/z = \bar{z}/(z\bar{z}) = \bar{z}/(a^2 + b^2 + c^2 + d^2)$, where the denominator is nonzero if $z \neq 0$. So nonzero quaternions form a group under multiplication. Call $|z| = a^2 + b^2 + c^2 + d^2$. Letting H^* be the nonzero quaternions, we have a homomorphism $H^* \to \mathbb{R}^*$ that takes $z \to |z|$. This homomorphism has kernel S^3. In fact, our quaternion group is a subgroup of S^3.

Identify $\mathbb{R}^3 = \{bI + cJ + dK \in H\}$. The map $v \mapsto g^{-1}vg$ (for g a nonzero quaternion) maps $\mathbb{R}^3 \to \mathbb{R}^3$. It is a rotation of $\mathbb{R}^3$.[2] So we get a homomorphism $S^3 \to \underbrace{\mathrm{SO}_3(\mathbb{R})}_{\text{rotations of } \mathbb{R}^3}$.
This is not an isomorphism because the kernel has order 2 (exercise). We get a short exact sequence

$$1\ to\, \{\pm 1\} \to S^3 \to \mathrm{SO}_3(\mathbb{R}) \to 1.$$

Pick any finite group of rotations, a subset of $\mathrm{SO}_3(\mathbb{R})$. For example, pick rotations of a rectangle in $\mathbb{R}^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or rotations of an icosahedron (has 60 elements). The inverse image of the previous homomorphism is a subgroup of S^3 of twice the order. In our examples, we get the quaternions and the "binary icosahedral group."

2 Groups of order 9, 10, and 12

2.1 Groups of order 9

There are two natural examples for the abelian cases:

- Groups of order 9
  - $\mathbb{Z}/9\mathbb{Z}$
  - $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

These are the only abelian groups: if we have an element of order 9, then we have $\mathbb{Z}/9\mathbb{Z}$, and if all elements are of order 3 an G is abelian, then it is a product of vector spaces over 3 elements, $\mathbb{F}_3 \times \mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

In fact, these two are the only groups of order 9 due to the following theorem:

Theorem 2.1. *Let p be prime. All groups of order p^2 are abelian.*

We require a lemma:

Lemma 2.1. *Any group of order p^n has nontrivial center.*

Proof. Sum over the conjugacy classes of G, picking some g in each C_g. Denote the center of G as Z. If g is in the center of G, then its conjugacy class has only 1 element: g itself. Then

$$|G| = \sum_g |C_g| = \sum_g \frac{|G|}{|G_g|} = \sum_{g \notin Z} \frac{|G|}{|G_g|} + |Z|$$

Since p divides the order of G and the summation term, p divides the order of the center. In particular, the center contains at least p elements and is nontrivial. □

[2] In computer graphics, such as in video games, quaternions are used to compute rotations of $\mathbb{R}^3$. They are quicker to multiply than 3×3 matrices.

Proof. Suppose G has order p^2. By our lemma, the center is nontrivial, so the center has order p or p^2.

However, the center cannot have order p. Suppose it does, and pick some g not in the center. If $g^2 \in Z$, then g has order p^2, so the group is cyclic and hence abelian. Then $g^2 \notin Z$, so $\langle g \rangle \cap Z = \{e\}$. Then $G = \langle g \rangle\, Z$, so every element can be written as $g^n a$ for some n and a in the center of G. Then all elements commute with each other, so the center is all of G, which is a contradiction.

So the center has order p^2 and is hence all of G. So G is abelian. $\square$

2.2 Nilpotent groups

Suppose G_0 has order p^n. Take its center Z_0, and let $G_1 = G_0/Z_0$. Keep quotienting out by the center. One might think that the center would be trivial after quotienting out by the center, but this is actually not true. Take $G = \{\pm 1, \pm i, \pm j, \pm k\}$ and $Z = \{\pm 1\}$; then $G/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has nontrivial center.

Definition 2.1. A group is *nilpotent* if it can be reduced to 1 element by repeatedly taking the quotient of its center at each step.

All products of groups of prime power order are nilpotent. Later, we will prove a converse: any finite nilpotent group is the product of group of order p^n.

2.3 Groups of order $2p$

For groups of order 10, and more generally order $2p$ for some prime p, we can generalize the methods we used for groups of order 6:

1. Pick subgroup H of order p
2. H has index 2 so is normal
3. Pick subgroup S of order 2

As in the case of order 6, $G \cong H \rtimes \mathbb{Z}/2\mathbb{Z}$. This is classified by the ways $\mathbb{Z}/2\mathbb{Z}$ can act on $\mathbb{Z}/p\mathbb{Z}$. Later, we will show that the automorphisms are isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, so we get two groups:

- Groups of order $2p$
  - the abelian group $\mathbb{Z}/2p\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
  - the dihedral group D_{2p}, the symmetries of the regular $2p$-gon (nonabelian)

2.4 Groups of order 12

Our list will be:

- Groups of order 12
  - the abelian group $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
  - the abelian group $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  - the nonabelian group D_{12}, the dihedral group of order 12 ($\cong D_6 \times \mathbb{Z}/2\mathbb{Z}$)[3]
  - rotations of a tetrahedron (nonabelian)
  - binary dihedral group (nonabelian)

[3] D_{8n+4} splits as a product for any $n \in \mathbb{N}$.