Math 126 Lecture 4

Shlomo Sternberg

Sept. 26, 2002

Contents

1 Morphisms.

Let the group G act on two sets M_1 and M_2. A map $f : M_1 \to M_2$ is called a **morphism** or is said to be **equivariant** if

$$f(am_1) = af(m_1) \quad \forall m_1 \in M_1 \quad \text{and } \forall\ a \in G.$$

Examples.

- If the action on M_2 is trivial (i.e. $am_2 = m_2\ \forall\ m_2 \in M_2$) then being equivariant means that f is **invariant**, i.e. $f(am_1) = f(m_1)\ \forall\ m_1 \in M_1$. This is an important special case, but the general notion will be important.

- Let M_2 be the set of all subgroups of G, and let G act on M_2 by the action induced from the conjugation action of G on itself. Let M_1 be any set on which G acts, and let $f : M_1 \to M_2$ be the map which assigns to each $m \in M_1$ its isotropy group:

$$f(m) := G_m.$$

The formula

$$G_{am} = aG_ma^{-1}$$

says that f is a morphism.

- Here is a closely related example: Let G act on a set M, and consider the action of G on $G \times M$ by

$$a(b, m) := (aba^{-1}, am).$$

Then the projection onto the second factor:

$$\theta : G \times M \to M, \qquad \theta(b, m) := m$$

is a morphism as is the projection onto the first factor

$$\tau : G \times M \to G, \qquad \tau(b, m) := b$$

where in this second equation we are considering the conjugation action of G on itself.

Let $Z \subset G \times M$ be the subset consisting of all pairs (b, m) such that $bm = m$. The set Z is carried into itself by the action of G on $G \times M$. In other words $aZ = Z$ for all $a \in G$. Indeed, if $(b, m) \in Z$ meaning $bm = m$, then $(aba^{-1})am = am$ which says that $(aba^{-1}, am) \in Z$.

Let $\rho : Z \to M$ denote the restriction of θ to Z and $\sigma : Z \to G$ denote the restriction of τ.

For an $m \in M$, its inverse image $\rho^{-1}(m)$ under ρ consists of all (a, m) such that $a \in G_m$. In symbols

$$\rho^{-1}(m) = G_m \times \{m\}.$$

For $a \in G$, we have

$$\sigma^{-1}(a) = \{a\} \times \mathrm{Fix}(a).$$

2 Counting fixed points.

In this last example, suppose that G is finite. But we do not assume that M is finite. For example, let G be a finite subgroup of $SO(3)$ and take M to be the unit sphere. Any rotation which is not the identity, has exactly two fixed points on the unit sphere, namely the two points where the axis of rotation meets the sphere. Of course every point of the unit sphere is fixed by the identity.

So in the last example of the preceding section, let us remove the set $\{e\} \times M$ from Z, and consider the set

$$Y := Z \setminus \{e\} \times M.$$

Let us also assume that every $a \neq e$ has only finitely many fixed points. This implies that Y is a finite set. Let $f : Y \to M$ denote the restriction of ρ to

Y, and let $g : Y \to G$ denote the restriction of σ to Y. Let $P \subset M$ denote the set of points of M which are left fixed by *some* $a \neq e$. So $P = f(Y)$, and $g(Y) \subset G \setminus \{e\}$.

We can now count the number of elements in Y in two ways: Using g we see that

$$\#Y = \sum_{a \neq e} \# \operatorname{Fix}(a).$$

Using P we see that

$$\#Y = \sum_{m \in P} (\#G_m - 1).$$

The -1 comes from the fact that we removed e. We can simplify this expression using the fact that $\#G_{ama^{-1}} = \#G_m$, so $\#G_m$ is constant on orbits of the G action on P. So if

$$P = P_1 \cup \cdots \cup P_r$$

is the decomposition of P into orbits, so that the number of points in each orbit is $\#G/\#G_m$ we have

$$\#Y = \sum_{orbits} \frac{\#G}{\#G_m} (\#G_m - 1)\,.$$

Equating the two ways of counting the numberr of points in Y gives

$$\sum_{a \neq e} \# \operatorname{Fix}(a) = \sum_{orbits} \frac{\#G}{\#G_m} (\#G_m - 1)\,.$$

3 The finite subgroups of $SO(3)$.

We will use this last formula to classify the finite subgroups of $SO(3)$ up to conjugacy. Since $\# \operatorname{Fix}(a) = 2$ for any non-trivial rotation acting on the sphere, the left hand side of the formula above is just $2(\#G-1)$. Introduce the notation

$$\begin{aligned} n &:= \#G \\ r &:= \#(\text{of orbits}) \\ n_i &:= \#G_m \text{ where } m \in \text{ } i\text{-th orbit }. \end{aligned}$$

Thus

$$2(n-1) = \sum_{i=1}^{r} \frac{n}{n_i}(n_i - 1)$$

or, dividing by n:

$$2 - \frac{2}{n} = r - \sum_{i=1}^{r} \frac{1}{n_i}. \tag{1}$$

We may exclude the trivial case where $G = \{e\}$, so that P is not empty. By definition, each element of P is fixed by at least one $a \neq e$ so $\#G_m \geq 2$ and so the right hand side of the above equation is $\geq \frac{r}{2}$. The left hand side is < 2. So $r < 4$. But $r = 1$ is impossible since $n_i \leq n$ and so

$$2 - \frac{2}{n} > 1 - \frac{1}{n_1}.$$

Thus the only possibilities are $r = 2$ and $r = 3$.

3.1 $r = 2$, the cyclic groups.

If $r = 2$ all non-trivial rotations are about a fixed axis. Equation (1) becomes

$$\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2}$$

and since $n_i \leq n$ this implies that $n_1 = n_2 = n$. So $G_m = G$, and the group consists of all rotations through angles $2\pi j/n$ about a fixed axis. For a given n, all such sugroups are conjugate, and the group is isomorphic to $C_n := \mathbb{Z}/n\mathbb{Z}$.

Now suppose that $r = 3$ so (1) becomes

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n}.$$

We choose notation so that $n_1 \leq n_2 \leq n_3$. Then $n_1 = 2$ for otherwise the left hand side of the above equation would be ≤ 1. Similarly, $n_2 \geq 4$ is impossible. If $n_2 = 3$ the above equation becomes

$$\frac{1}{n_3} = \frac{1}{6} + \frac{2}{n}$$

so $n_3 < 6$. The possibilities that we haven't excluded for (n_1, n_2, n_3) and n are:

$$(2,2,k) \quad k \geq 2 \text{ arbitrary}, \quad n_3 = k, \quad n = 2k,$$

and

$$\begin{aligned} (2,3,3) \quad n &= 12 \\ (2,3,4) \quad n &= 24 \\ (2,3,5) \quad n &= 60. \end{aligned}$$

Each of these possibilities actually occurs and represents exactly one subgroup up to conjucgacy. We proceed down the list:

3.2 (2,2,k), the dihedral groups.

Since $n_3 = k = n/2$ the orbit P_3 has two elements, and so the subgroup G_m corresponding to each of these two elements is the same, and is the cyclic group

C_k. For any q belonging to P_1 or P_2 the group $\#G_q = 2$ and so G_q consists of the identity and rotation through 180^o . The subgroup C_k acts on P_1 and no element of C_k other than the identity fixes any point of P_1. Since $\#P_1 = k$, we see that the points of P_1 all lie in a plane and form a regular k-gon. Similarly for P_2. The case $k = 2$ is a bit degenerate in that the group is (up to conjugacy) given by the identity together with 180^o rotations about each of the coordinate axes. If $k \geq 2$ is even, there are two types of 180^o axes, those which pass through the vertices and those which bisect the sides. The two orbits P_1 and P_2 are the intersections of each of these types of axis with the sphere. If $k \geq 2$ is odd, then all 180^o axes pass through a vertex and bisect the opposite side. The vertices form one orbit, say P_1, and the other intersection of each axis with the sphere form P_2.

3.3 (2,3,3), the tetrahedral group.

So $n = 12,\ \#P_1 = 6,\ \#P_2 = \#P_3 = 4$. The group of rotational symmetries of a tetrahedron has 12 elements since a given vertex can be moved to any other, and the isotropy group of a vertex is C_3. So (2,3,3) occurs as the symmetry group of the tetrahedron. To show that up to conjugacy this is the only possibility, it suffices to show that the points of P_2 form a regular tetrahedron. Let $m \in P_2$. Then $G_m = C_3$, so the other three point3 of P_3 form an equilateral triangle. In particular they are equidistant from one another. Doing the same for each of the points in P_2 shows that they are the vertices of a regular tetrahedron.

3.4 (2,3,4) the cubic group.

So $n = 24,\ \#P_1 = 12,\ \#P_2 = 8,\ \#P_3 = 6$. The group of rotational symmetries of a cube has 24 elements since a given vertex can be moved to any other, and the isotropy group of a vertex is C_3, as any adjacent vertex can be rotated into another. So (2,3,3) occurs as the symmetry group of the cube. Conversely, as above, the elements of P_3 form a regular octahedron (whose dual polytope is a cube).

3.5 (2,3,5) the icosahedral group.

So $n = 60,\ \#P_1 = 30,\ \#P_2 = 20,\ \#P_3 = 12$. The group of rotational symmetries of a regular icosahedron has 60 elements, since each vertex can be moved to any other and the isotropy subgroup of a vertex is C_5. Conversely, consider the orbit P_3. By a rotation (i.e. a conjugacy in $SO(3)$) we may assume that two of the twelve points of P_3 lie on the z-axis. The remaining ten points can not lie on the equator, for then there would be a rotation through $2\pi/5$ about an axis x, y-plane, which would have to take the eight remaining points off the equator. So five of the remaining ten points lie in the upper hemisphere, and half in the lower hemisphere. Each ot the five points in the upper hemisphere lie on a regular pentagon, since rotation through $2\pi/5$ about the z-axis belongs to our group. So these five points, and hence all twelve points are equidistant and so the points of P_3 form a regular icosahedron.

4 The dihedral groups, revsited.

Let V be a vector space endowed with a scalar product, denoted by $(\ , \ )$. For any non-zero vector $\gamma \in V$, the reflection in the hyperplane orthogonal to γ is denoted by s_γ and is given explicitly by

$$s_\gamma : \ v \mapsto v - \frac{2(v,\gamma)}{(\gamma,\gamma)}\gamma.$$

If $w \in O(V)$ is an orthogonal transformation, we have

$$ws_\gamma w^{-1} = s_{w\gamma}. \tag{2}$$

In the plane, reflection in the x-axis is given by

$$s_\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

where β is any non-zero vector on the $y-$axis say the unit vector

$$\beta = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Conjugating by (counterclockwise) rotation, R_θ, through angle θ,

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

shows that the reflection about the line making angle θ with the $x-$ axis is given by

$$s_\alpha = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

where α is any vector perpendicular to this line, for example

$$\alpha := \begin{pmatrix} \sin\alpha \\ -\cos\alpha \end{pmatrix}. \tag{3}$$

Multiplying the matrices shows that

$$s_\alpha s_\beta = R_{2\theta}, \quad s_\beta s_\alpha = R_{-2\theta}. \tag{4}$$

Also

$$sR_\theta s = R_{-\theta} \tag{5}$$

for any reflection, s. This is a direct computation for reflection in the $x-$axis, and then folows by conjugation for any reflection.

From this it follows that the dihedral group D_m of symmetries of the regular $m-$sided polygon is generated by two "adjacent" reflections, and can be written abstractly as the semi-direct product of the multaplicative group $\{1, -1\}$ with the cyclic group $C_m = \mathbf{Z}/m\mathbf{Z}$ so, if $\epsilon, \epsilon' = \pm 1, \quad x, x' \in \mathbf{Z}/m\mathbf{Z}$ the multiplication law is given by

$$(\epsilon, x)(\epsilon', x') = (\epsilon\epsilon', \epsilon x' + x).$$

Explicitly the isomorpism of D_m with this semi-direct product can be realized by

$$s_\alpha \mapsto (-1, 1), \quad s_\beta \mapsto (-1, 0)$$

so that

$$R_{2\theta} \mapsto (1, 1), \quad \theta = \pi/m.$$

If, instead of the finite cyclic group $\mathbf{Z}/\mathbf{Z}_m$ we consider the semi-direct product of $\{1, -1\}$ with the infinite cyclic group, $\mathbf{Z}$, (so the same multiplication law as above), we obtain an infinite group called the infinite diheral group and denoted by D_∞. Let us describe the dihedral groups, D_3, D_4, D_5, D_6. The general pattern will the emerge. We will take

$$\beta = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \alpha = \begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix}, \quad \theta = \pi/m$$

where $m = 3, 4, 5, 6 \cdots$ so that s_β is a reflection about the $x-$axis and s_α is reflection about the line through $(\cos\theta, \sin\theta)$. So

$$R_{2\theta} = s_\alpha s_\beta, \quad R_{-2\theta} = s_\beta s_\alpha$$

in all cases. Also, we have equations of the form

$$s_\beta s_\alpha s_\beta = s_{s_\beta \alpha}$$

etc. We have

$$D_3, \quad \theta = \pi/3$$

$$
\begin{array}{ccc}
 & 1 & \\
s_\alpha & & s_\beta \\
R_{2\theta} = s_\alpha s_\beta & & s_\beta s_\alpha = R_{-2\theta} \\
 & s_\beta s_\alpha s_\beta = s_\alpha s_\beta s_\alpha &
\end{array}
$$

$$D_4 \quad \theta = \pi/4$$

$$
\begin{array}{ccc}
 & 1 & \\
s_\alpha & & s_\beta \\
R_{2\theta} = s_\alpha s_\beta & & s_\beta s_\alpha = R_{-2\theta} \\
s_{s_\beta \alpha} = s_\beta s_\alpha s_\beta & & s_\alpha s_\beta s_\alpha = s_{s_\alpha \beta} \\
 & R_\pi = s_\alpha s_\beta s_\alpha s_\beta = s_\beta s_\alpha s_\beta s_\alpha &
\end{array}
$$

$$D_5, \quad \theta = \pi/5$$

$$
\begin{array}{ccc}
 & 1 & \\
s_\alpha & & s_\beta \\
R_{2\theta} = s_\alpha s_\beta & & s_\beta s_\alpha = R_{-2\theta} \\
s_{s_\beta \alpha} = s_\beta s_\alpha s_\beta & & s_\alpha s_\beta s_\alpha = s_{s_\alpha \beta} \\
R_{4\theta} = s_\alpha s_\beta s_\alpha s_\beta & & s_\beta s_\alpha s_\beta s_\alpha = R_{-4\theta} \\
 & s_\alpha s_\beta s_\alpha s_\beta s_\alpha = s_\beta s_\alpha s_\beta s_\alpha s_\beta &
\end{array}
$$

$$D_6, \quad \theta = \pi/6$$

$$
\begin{array}{ccc}
 & 1 & \\
s_\alpha & & s_\beta \\
R_{2\theta} = s_\alpha s_\beta & & s_\beta s_\alpha = R_{-2\theta} \\
s_{s_\beta \alpha} = s_\beta s_\alpha s_\beta & & s_\alpha s_\beta s_\alpha = s_{s_\alpha \beta} \\
R_{4\theta} = s_\alpha s_\beta s_\alpha s_\beta & & s_\beta s_\alpha s_\beta s_\alpha = R_{-4\theta} \\
s_\alpha s_\beta s_\alpha s_\beta s_\alpha & & s_\beta s_\alpha s_\beta s_\alpha s_\beta \\
 & R_\pi = s_\alpha s_\beta s_\alpha s_\beta s_\alpha s_\beta & \\
 & = s_\beta s_\alpha s_\beta s_\alpha s_\beta s_\alpha &
\end{array}
$$

In fact, the dihedral groups can be characterized abstractly as groups generated by two distincct elements of order two. Here is a precise statement.

Theorem 4.1 *Let W be a group generated by two distinct elements, s and s' both of order two. Let*

$$p := ss'.$$

The subgroup P generated by p is a normal subgroup of index two, and W is the semi-direct product of the two element subgroup $T = \{1, s\}$ and P.

Let m be the order of p. Then $m \geq 2$ and there is a unique isomorphism, ϕ, of D_m onto W such that

$$\phi((-1,1)) = s, \quad \phi((-1,0)) = s'.$$

Proof. We have

$$\begin{aligned} sps^{-1} &= sss's \\ &= s's \\ &= p^{-1} \quad \text{so} \\ sp^n s &= p^{-n} \end{aligned}$$

for all integers, n. Since s and s' generate W, so do s and p. So the last equation shows that P is a normal subgroup. Since TP contains s and s', this shows that $TP = W$. So either $W = P$ or P has index two, and $s \notin P$ so W is the semi-direct product of T and W. So we must show that $W \neq P$. Suppse that $W = P$. Then W would be commutative, hence $p^2 = s^2 {s'}^2 = 1$, hence W contains only two elements, namely 1 and p. This contradicts the hypothesis that s and s' are two distinct elements of order two, implying that W has at least three elements. In particular, $m \geq 2$.

Let $q = (1,1)$ be the generator of the cyclic subgroup of D_m (so that for m finite, the element q corresponds to $R_{2\theta}$). Then there is a unique isomorphism of the cyclic subgroup of D_m onto P with $q \mapsto p$. Also there is a unique homomorphism of $\{1, -1\}$ onto T which sends $-1 \mapsto s$. These piece together to give the desired isomorphism on account of the equation

$$sp^n s^{-1} = p^{-n}.$$

This isomorphism maps $(-1,1) \mapsto s$, $(-1,0) = (-1,1)(1,1) \mapsto sp = s'$ proving the existence of the ϕ given in the theorem. The uniqueness follows from the fact that $(-1,1)$ and $(-1,0)$ generate D_m. $\square$