

# Math 126 Lectures 2&3

Shlomo Sternberg

Sept. 19 and 24, 2002

## Contents

<b>1</b>	<b>The homomorphism from <math>SU(2)</math> to <math>SO(3)</math>.</b>	<b>1</b>
<b>2</b>	<b>Group actions.</b>	<b>2</b>
2.1	Isotropy groups. . . . .	2
2.1.1	Proof of Euler's theorem. . . . .	3
2.2	Induced actions. . . . .	3
2.3	Orbits. . . . .	3
2.3.1	$\#G = \#(G \cdot m) \times \#G_m$ and some consequences. . . . .	3
<b>3</b>	<b>The Sylow theorems.</b>	<b>4</b>
3.1	Sylow subgroups exist. . . . .	4
3.2	$N_p \equiv 1 \pmod{p}$ . . . . .	5
3.3	$Q$ is contained in a conjugate of $P$ . . . . .	5
3.4	The number of $p$ -Sylow subgroups divides $\#G$ . . . . .	6

## 1 The homomorphism from $SU(2)$ to $SO(3)$ .

Write the real three vector  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$  as the two by two traceless self adjoint matrix

$$\begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix}.$$

This gives a 1-1 linear map between  $\mathbb{R}^3$  and the set of  $2 \times 2$  traceless s.a. matrices. Notice that

$$\det \begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix} = -(x^2 + y^2 + z^2).$$

If  $U$  is unitary and  $M$  is self adjoint then  $UMU^* = UMU^{-1}$  is self-adjoint and has the same determinant and trace as  $M$ . Also  $(UV)M(UV)^* = U(VMV^*)U^*$ .

This defines a homomorphism from  $U(2)$  to  $O(3)$ . Restrict this to  $SU(2)$ . We shall show that this is a 2-1 homomorphism  $\phi$  from  $SU(2) \rightarrow SO(3)$ : Let  $U_\theta := \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$ . Then

$$U_\theta \begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix} U_\theta^* = \begin{pmatrix} z & e^{-2i\theta}(x - iy) \\ e^{2i\theta}(x + iy) & -z \end{pmatrix}.$$

So  $\phi(U_\theta)$  is rotation through  $2\theta$  about the  $z$ -axis. Let

$$V_\phi := \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix}$$

Computation shows  $\phi(V_\phi)$  is rotation through  $2\phi$  about the  $y$ -axis. Since every element of  $SU(2)$  is conjugate to an element of the form  $U_\theta$  the image of the image of  $\phi$  lies in  $SO(3)$ .

If  $U$  is in the kernel of  $\phi$  then  $UMU^{-1} = M$  so  $UM = MU$  for every  $M$ . If we take  $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  then  $MU = UM$  implies that  $U$  is diagonal and hence of the form  $U_\theta$ . If we take  $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  we see that  $\theta = 0$  or  $\pi$ . So the kernel of  $\phi$  consists of  $I$  and  $-I$ .

To show that  $\phi$  is onto we call on a theorem of Euler which says that every element of  $SO(3)$  can be written as

$$R = R_\theta^z R_\phi^y R_\psi^z$$

i.e. a rotation about the  $z$ -axis followed by a rotation about the  $y$ -axis followed by another rotation about the  $z$ -axis. Since every rotation about the  $y$  or  $z$  axis is in the image of  $\phi$  this implies that all of  $SO(3)$  is in the image. We will prove Euler's theorem in the next section.

The fact that  $\phi$  is 2-1 has consequences for the topology of  $SO(3)$ .

## 2 Group actions.

The action of a group  $G$  on a set  $M$  is a homomorphism from  $G$  to  $S_M$ . Equivalently, it is a map  $G \times M \rightarrow M$  sending  $(a, m) \mapsto am$  such that

$$em = m \quad \forall m \in M \quad \text{and} \quad (ab)m = a(bm).$$

### 2.1 Isotropy groups.

Let  $m \in M$ . The set of all  $a \in G$  such that  $am = m$  is a subgroup of  $G$  called the **isotropy group** of  $m$  and denoted by  $G_m$ . The concept of an isotropy group gives a precise mathematical definition to the idea of the "symmetry" of an object.

We have

$$G_{bm} = bG_m b^{-1}$$

meaning that  $c \in G_{bm}$  if and only if  $c = bab^{-1}$  for some  $a \in G_m$ .

### 2.1.1 Proof of Euler's theorem.

Let  $M$  be the unit sphere and  $G = SO(3)$ . Let  $n$  denote the north pole. Any  $R \in SO(3)$  is determined by  $Rn$  and the image of any unit vector tangent to  $M$  at  $n$ . So if  $B$  is any other element of  $SO(3)$  with  $Bn = Rn$ , we can arrange that the unit vector is in the right direction by rotating about the axis through  $Bn$ . In other words,

$$R = CB, \quad C \in SO(3)_{Bn}.$$

Now we can get to any point on the unit sphere from the north pole by first rotating about the  $y$ -axis to achieve the correct latitude, and then rotating about the  $z$ -axis to achieve the correct longitude. In other words we can choose

$$B = R_\theta^z R_\phi^y.$$

So  $C = BR_\psi^z B^{-1}$  for some  $\psi$  and so

$$R = CB = BR_\psi^z B^{-1} B = BR_\psi^z = R_\theta^z R_\phi^y R_\psi^z$$

proving Euler's theorem.

## 2.2 Induced actions.

If  $G$  acts on  $M$ , it also acts on  $2^M$ , the set of all subsets of  $M$  by

$$aS := \{as \mid s \in S\}.$$

It also acts on the set of all functions on  $M$  by

$$(af)(m) := f(a^{-1}m).$$

If  $f$  is a function which takes on only two values, say 0 and 1, this action generalizes the action on  $2^M$ ,

## 2.3 Orbits.

Let  $G$  act on  $M$  and let  $m \in M$ . The **orbit through**  $m$  denoted by  $G \cdot m$  is the set of all points of the form  $am$ ,  $a \in G$ .

### 2.3.1 $\#G = \#(G \cdot m) \times \#G_m$ and some consequences.

If  $S$  is a finite set we let  $\#S$  denote the cardinality of  $S$ . Suppose  $G$  is finite and acts on  $M$ . If  $m \in M$  and  $n \in G \cdot m$ , then  $n = am$  for some  $a \in G$ . If also  $n = bm$ , then  $b^{-1}a \in G_m$ , and conversely. So there are exactly  $\#G_m$  elements  $a$  such that  $am = n$ , and so  $G \cdot m$  partitions  $G$  into  $\#(G \cdot m)$  cosets each having  $\#G_m$  elements, proving the formula in the title of this subsection. In particular both  $\#G \cdot m$  and  $\#G_m$  divide  $\#G$ .

## Applications.

- $G$  acts on itself by left multiplication, and hence acts on  $2^G$ , the set of all subsets of  $G$ . Under this action, if  $H$  is a subgroup, then the isotropy group of  $H$  is exactly  $H$ . hence we conclude that

$$\#H \text{ divides } \#G$$

for any subgroup of  $G$ .

- We can apply this to the subgroup  $H$  generated by single element  $a$ . Then  $\#H$  is the smallest positive integer  $n$  such that  $a^n = e$ . This is called the **order** of  $a$ . We see that the order of any element must divide  $\#G$ . This is a theorem of Lagrange.
- A group  $G$  is called a  $p$ -group (where  $p$  is a prime) if  $\#G$  is a power of  $p$ . This implies that every  $\#G \cdot m$  is a power of  $p$ . The set of **fixed points** of  $G$  (for any group action) is the set of all  $m \in M$  such that  $am = m$  for all  $a \in G$ . It is denoted by  $\text{Fix}(G, M)$  or  $\text{Fix}(G)$  if  $M$  is understood. The orbit through a point  $m$  of  $\text{Fix}(G)$  consists of the single point  $\{m\}$ . If  $G$  is a  $p$ -group, all other orbits  $O$  have the property that  $\#O$  is divisible by  $p$ . If  $M$  is finite, then we can decompose  $M$  into a finite disjoint union of orbits. Hence in this case

$$\# \text{Fix}(G) \equiv \#M \pmod{p}.$$

### 3 The Sylow theorems.

Let  $G$  be a finite group and write  $\#G = p^n k$  where  $k$  is not divisible by  $p$ . A subgroup of  $G$  of order  $p^n$  is called a  $p$ -**Sylow subgroup**. There are four statements (due to Sylow) concerning Sylow subgroups.

#### 3.1 Sylow subgroups exist.

That is, the set of Sylow subgroups is not empty. To prove this we first need a lemma from combinatorics:

**Lemma 3.1** *Let  $p$  be a prime and  $k$  an integer not divisible by  $p$ . The number of ways of selecting a subset with  $p^n$  elements from a set with  $p^n k$  elements is congruent to  $k \pmod{p}$ .*

**Proof of lemma.** The number in question is the coefficient of  $x^{p^n}$  in

$$(1+x)^{p^n k} = \left( (1+x)^{p^n} \right)^k.$$

But  $(1+x)^{p^n} \cong 1+x^{p^n} \pmod{p}$ . And the coefficient of  $x^{p^n}$  in  $(1+x^{p^n})^k$  is  $k$ .  
□

**Proof of the existence of Sylow subgroups.** Let  $M$  consist of the set of all subsets of  $G$  of cardinality  $p^n$ .  $G$  acts on  $M$  by virtue of its left multiplication

action on itself. Decompose  $M$  into orbits. Not every orbit  $O$  has the property that  $\#O$  is divisible by  $p$  for then  $\#M$  would be divisible by  $p$  contrary to the lemma. Let  $O$  be an orbit for which  $\#O$  is not divisible by  $p$ . So  $O = G \cdot S$  where  $S$  is a subset of  $G$  such that

$$\#S = p^n \quad \text{and} \quad \#G_S = \#G/\#G \cdot S = tp^n$$

where  $t$  is some integer not divisible by  $p$ . Let  $a \in G_S$ . Then  $as \in S$  for any  $s \in S$  so the coset  $G_S s \subset S$ . But multiplication on the right by  $s$  is a one to one map on  $G$ , and hence

$$\#G_S = \#(G_S s) \leq \#S = p^n.$$

So  $t = 1$  in the above expression and  $\#G_S = p^n$  and hence  $G_S$  is a  $p$ -Sylow subgroup.  $\square$

Notice that the above proof shows that the  $S$  we have chosen has the property that  $G_S s = S$  for any  $s \in S$ , and hence  $s^{-1}G_S s$  is a Sylow subgroup in the orbit  $O = G \cdot S$  and so  $s^{-1}G_S s = s^{-1}S$ . So  $S$  is the orbit of the Sylow subgroup  $s^{-1}G_S s$ , and the isotropy subgroup of  $s^{-1}G_S s$  is just itself. So  $\#O = k$ , and every orbit whose cardinality is not divisible by  $p$  has exactly  $k$  elements and exactly one point of this orbit is a Sylow subgroup. No orbits whose cardinality is divisible by  $p$  can contain a Sylow subgroup. So the number  $N_p$  of Sylow subgroups is the same as the number of orbits whose cardinality is not divisible by  $p$  and each such orbit has cardinality  $k$ . In particular, since we can partition  $M$  into orbits,

$$\#M \equiv kN_p \pmod{p}.$$

### 3.2 $N_p \equiv 1 \pmod{p}$ .

We have proved that  $\#M \equiv kN_p \pmod{p}$ . On the other hand, the lemma says that  $\#M \equiv k \pmod{p}$ . So  $N_p \equiv 1 \pmod{p}$ .  $\square$

Let  $P$  be a  $p$ -Sylow subgroup of  $G$  and let  $Q$  be a  $p$ -subgroup of  $G$  (which means that  $\#Q = p^m$  for some  $m \leq n$ ). The third Sylow theorem says that

### 3.3 $Q$ is contained in a conjugate of $P$ .

For this we will need two lemmas. The first is a general lemma about two subgroups of a group. Let  $A$  and  $B$  be subgroups of a group  $G$ . We let  $AB$  denote the set of all elements of  $G$  which can be written as  $ab$  with  $a \in A$  and  $b \in B$ . So  $AB$  is a subset of  $G$ , but need not be a subgroup. But  $A \cap B$  is a subgroup.

**Lemma 3.2**  $\#(AB) = (\#A)(\#B)/\#(A \cap B)$ .

**Proof.** We know that  $A \cap B$  is a subgroup of  $A$ . Let

$$x_1(A \cap B), x_2(A \cap B), \dots, x_r(A \cap B)$$

be the distinct cosets of  $A \cap B$  in  $A$ . So every element of  $A$  is in one of these cosets. Also, if  $i \neq j$  then  $x_j x_i^{-1} \notin A \cap B$ . Let  $ab \in AB$ . Write  $a = x_i g$  for some  $i$  with  $g \in A \cap B$ . So  $ab = x_i g b \in x_i B$ . Also, the cosets  $x_i B$  are disjoint, for if not  $x_i B = x_j B$  for some  $i \neq j$  implying that  $x_i^{-1} x_j \in A \cap B$  which is not the case. So

$$\#(A)/\#(A \cap B) = \#(AB)/\#B$$

which is equivalent to the statement of the lemma.  $\square$

For the second lemma we need some notation. If  $B$  is a subgroup of any group  $G$ , then  $N_G(B)$  denotes the isotropy subgroup of  $B$  under the conjugation action, i.e. the set of all  $a \in G$  such that  $aBa^{-1} = B$ . If  $A$  is a subgroup of  $N_G(B)$  then  $AB$  is a subgroup.

**Lemma 3.3** *Let  $P$  be a  $p$ -Sylow subgroup of a group  $G$ . Then any  $p$ -subgroup  $Q$  of  $N_G(P)$  is contained in  $P$ . In particular,  $P$  is the unique  $p$ -subgroup of  $N_G(P)$ .*

**Proof.** Suppose that  $\#Q = p^m$ . Then  $QP$  is a subgroup of order  $p^{n+m-s}$  where  $\#P = p^n$  and  $\#(Q \cap P) = p^s$  by the preceding lemma. Since  $p^n$  is the largest  $p$ -th power dividing  $\#G$ , we must have  $m \leq s$ . On the other hand,  $P \cap Q$  is a subgroup of  $Q$ , and hence  $s \leq m$ . So  $s = m$  and hence  $P \cap Q = Q$  which says that  $Q \subset P$ .  $\square$

**Proof of the assertion.** Let  $M$  denote the set of distinct  $G$ -conjugates of  $P$ . Let  $P$  act on  $M$  by conjugation. So  $P \in \text{Fix}(P, M)$ . We claim that  $P$  is the only element of  $\text{Fix}(P, M)$ . Suppose that  $gPg^{-1} \in \text{Fix}(P, M)$ . This says that

$$x(gPg^{-1})x^{-1} = gPg^{-1}, \quad \forall x \in P$$

or

$$(g^{-1}xg)P(g^{-1}xg)^{-1} = P$$

so  $(g^{-1}xg) \in N_G(P)$ . This is true for all  $x \in P$  so  $g^{-1}Pg \subset N_G(P)$  and since  $\#((g^{-1}Pg)) = \#P$  the preceding lemma implies that  $g^{-1}Pg = P$ . So there is only one fixed point and hence  $\#M \equiv 1 \pmod{p}$ .

Now consider the conjugation action of  $Q$  on  $M$ . Since  $\#M \equiv \#\text{Fix}(Q, M) \pmod{p}$  we conclude that  $\text{Fix}(Q, M) \neq \emptyset$ . So there is a  $g \in G$  such that

$$x(gPg^{-1})x^{-1} = gPg^{-1} \quad \forall x \in Q$$

so  $g^{-1}Qg \subset N_G(P)$  and hence  $g^{-1}Qg \subset P$ , again by the last lemma, so  $Q \subset gPg^{-1}$ .  $\square$

In particular, any two  $p$ -Sylow subgroups are conjugate. This implies

### 3.4 The number of $p$ -Sylow subgroups divides $\#G$ .

Indeed, the number of  $p$ -Sylow subgroups is the number of elements in the single orbit of the conjugacy action of  $G$  on the set of  $p$ -Sylow subgroups since we know that all such are conjugate. But we know that the number of elements in an orbit of any  $G$  action divides  $\#G$ .  $\square$