Lecture Notes For

Mathematics 150B

Dr. Tyler J. Evans

Winter 2001

Contents

Chapter 1

Topics in Advanced Group Theory

1.1 Group actions

In this lecture, we begin our deeper investigation into the theory of groups with the notion of a group action. The notion of a group acting on a set is a fundamental tool in contemporary mathematics. Two of the main topics in this course are the mathematical notion of symmetry and representation theory of groups. Both of these notions involve the notion of group actions. Before we give the main definition, let us recall that a binary operation on a set S is a function $* : S \times S \to S$ and we usually write $*(s_1, s_2) = s_1 * s_2$. This notation is responsible for the terminology "multiplication" that is often used to describe binary operations on sets. In the same spirit, if A, B and C are any sets, we might call a function $\mu : A \times B \to C$ a "multiplication". We do not mean anything by this term, other than an ordered pair of elements (a, b) determines a unique element $\mu(a, b)$ of the set C. In the case of a group action, we are concerned with the case in which $A = G$ is a group and $B = C = S$ is a set and the mapping $G \times S \to S$ has two additional properties. Here is the main definition.

Definition 1.1.1 (Group action) *Let G be a group (written multiplicatively) and let S be a set. We say that G* **acts on** *S if we are given a function $G \times S \to S$ written $(g, s) \mapsto gs$ that satisfies*

G1. *$(gh)s = g(hs)$ for all $g, h \in G$ and all $s \in S$.*

G2. *$es = s$ for all $s \in S$ where $e \in G$ is the identity element.*

*In this case we also say that S is a G-***set** *and the function $G \times S \to S$ is called a* **group action**.

In other words, a set S is a G-set if for every $g \in G$ and $s \in S$, we have an element $gs \in S$. Note that this means that each $g \in G$ determines a function from $S \to S$. We will say a great deal more about this. We will now present some guiding examples of group actions on various different sets. The reader is advised to thoroughly master each of the following examples as their importance in the rest of our work can not be over estimated.

Example 1.1.2 1. If $n \in \mathbb{N}$ is a fixed positive integer, then the symmetric group S_n acts on the set $S = \{1, 2, \ldots, n\}$ under the assignment $(\sigma, j) \mapsto \sigma(j)$. That is, we define a function $S_n \times S \to S$ by $(\sigma, j) \mapsto \sigma(j)$. The axiom **G1** follows immediately from the law of composition in S_n and **G2** holds by the definition of the identity permutation (verify!).

2. More generally, if S is any set, then the permutation group $A(S)$ (i.e. the group of all bijective mappings $S \to S$ under function composition) acts on S via $\sigma s = \sigma(s)$.

3. In this example, the group G plays both the role of the group and the set. That is, every group G acts on itself via **left multiplication**. Specifically, the law of composition $G \times G \to G$ satisfies **G1** (associative law) and **G2** (identity) and hence defines an action of G on itself. That is, a group G is always a G-set.

4. Every group G is also a G-set via **conjugation**. To define this action, we declare that $(g, h) \mapsto ghg^{-1}$ for all $g \in G$ and $h \in G$. To avoid horrible confusion with our notations, we will **never** use the notation gh to denote an element g acting on $h \in G$ via conjugation. The verification that this is indeed an action of G on G is carried out by noting that $(g_1 g_2)h(g_1 g_2)^{-1} = g_1(g_2 h g_2^{-1})g_1^{-1}$ for all $g_1, g_2, h \in G$ so that **G1** holds and $ehe = h$ for all $h \in G$ so that **G2** holds as well. This is a particularly important action of a group on itself. In fact, we will devote an entire lecture to it!

5. More generally, if G is a group and S is the set of all subgroups H of G, then G acts on S by conjugation. Recall from MAT 150A that gHg^{-1} is a subgroup of G whenever H is a subgroup of G. The verification of **G1** and **G2** is the same as in example 4. Do it!

6. The next example is actually quite general. Let G be a group and let H be a (not necessarily normal) subgroup of G. Let G/H denote the set of left cosets of H in G. We want to emphasize at this point that G/H is not a group unless H is normal, but we can always consider the set of left cosets of H in G as a set. This coset space G/H is a G-set via the

action $(g, aH) \mapsto (ga)H$. We must show that this operation is well defined. Suppose then that $aH = bH$ so that $a^{-1}b \in H$. Then for any $g \in G$, we have

$$(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$$

so that $(ga)H = (gb)H$. We leave the careful verification that this map defines an action of G on G/H as an exercise.

We conclude this lecture by summarizing briefly and giving an equivalent definition of a group action. A set S is called a G-set if there is a mapping $G \times S \to S$ that satisfies **G1** and **G2**. In other words, each $g \in G$ defines a function $S \to S$ (we will see that the axioms **G1** and **G2** imply that each such function is a permutation of S) in such a way that a product of two elements in G is assigned to the composition of maps $S \to S$ and the identity element of G is assigned to the identity map $S \to S$. We state this more precisely in the following theorem.

Theorem 1.1.3 *Let G be a group and S be a set. Then S is a G-set if and only if there exists a homomorphism $\rho : G \to A(S)$ where $A(S)$ denotes the permutation group of S.*

Proof. ($\Longrightarrow$) If S is a G-set, then for each $g \in G$, the assignment $s \mapsto gs$ is a function $S \to S$. Moreover this function is a permutation of S since the function determined by g^{-1} is obviously an inverse to the function determined by g. This gives a map $\rho : G \to A(S)$ defined by $\rho(g)(s) = gs$. Now, the axiom **G1** shows that for all $g, h \in G$ and all $s \in S$, we have

$$\rho(gh)(s) = (gh)(s) = g(hs) = \rho(g)(hs) = \rho(g)(\rho(h)(s)) = \rho(g)\rho(h)(s)$$

so that ρ is a homomorphism.
($\Longleftarrow$) Now suppose that we are given $\rho : G \to A(S)$. We then define a map $G \times S \to S$ by $(g, s) \mapsto \rho(g)(s)$. Then the axioms **G1** and **G2** follow immediately from the fact that ρ is a homomorphism and the identity element of $A(S)$ is the identity map. ∎

1.2 Stabilizers and orbits

In this lecture, we introduce two important objects associated with a group action on a set S: isotropy subgroups and G-orbits. In general, if S is a G-set, $s \in S$ and $g \in G$, it will be important to know when $gs = s$. One can view this equation from two distinct points of view. Namely, we can

fix $g \in G$ and try to find all $s \in S$ such that $gs = s$, or one can fix $s \in S$ and find all $g \in G$ such that $gs = s$. We will want to be able to do both. For a given $s \in S$, the set

$$G_s = \{g \in G : gs = s\}$$

is called the **stabilizer of** s or the **isotropy subgroup of** s. To justify the latter terminology, we will need the following proposition. The reader is encouraged to write his or her own proof before reading the proof given here.

Proposition 1.2.1 *Let G be a group and let S be a G-set. Then for all $s \in S$, the stabilizer G_s of s is a subgroup of G.*

Proof. Let $s \in S$ be arbitrary. We show that G_s is closed under product and inversion. If $g, h \in G_s$, then we compute using **G1**:

$$(gh)(s) = g(hs) = gs = s$$

and hence $gh \in G_s$. Also, if $e \in G$ denotes the identity element, we have

$$s = es = (g^{-1}g)(s) = g^{-1}(gs) = g^{-1}s$$

so that $g^{-1} \in G_s$. The proposition follows. ∎

Let's return to the examples of the previous lecture and determine the stabilizers of a few elements.

Example 1.2.2

1. If S_n acts on $\{1, 2, \ldots, n\}$ and $1 \leq j \leq n$, then the stabilizer of j is the subset of S_n that leave j fixed. This stabilizer is naturally isomorphic to S_{n-1}. Proof?

2. If G acts on itself by left multiplication, then the stabilizer of any point is trivial. To see this, let $h \in G$ be arbitrary and note that $g \in G_h$ if and only if $gh = h$ which is true if and only if $g = e$ by the cancellation law in G.

3. If G acts on itself by conjugation, and $h \in G$, then $g \in G_h$ if and only if $ghg^{-1} = h$ if and only if $gh = hg$. Therefore we see that the stabilizer of $h \in G$ under conjugation is precisely the set of elements in G that commute with h. In this context, the stabilizer of an element under conjugation is often called the **centralizer of** h.

4. If G acts on the set S of subgroups of G, and $H \in S$, then $g \in G_H$ if and only if $gHg^{-1} = H$. For this example, the stabilizer of H is often called the **normalizer of** H **in** G. It is a nice exercise to show that the normalizer of H in G is the largest subgroup of G in which H is normal.

5. If $H \leq G$ is a subgroup of G, and G acts on $S = G/H$ by left translation, then $g \in G$ is in the stabilizer of aH if and only if $(ga)H = aH$ if and only if $a^{-1}ga \in H$.

We now turn our attention to the problem of determining those $s \in S$ that satisfy $gs = s$ for a given $g \in G$. It is useful to recast this problem in terms of an equivalence relation induced on S by the action of G. We state the result as a proposition. Once again, the reader is invited to furnish his or her own proof of this proposition. Also, please compare this proposition to the result in problem 2 of the MAT 150A midterm exam 1.

Proposition 1.2.3 *If S is a G-set, then the relation $\sim$ defined on S by $s_1 \sim s_2$ if and only if $gs_1 = s_2$ for some $g \in G$ is an equivalence relation.*

Proof. For reflexively, we note that $es = s$ for all $s \in S$ so that $s \sim s$ for all $s \in S$. For symmetry, we note that if $s_1 \sim s_2$, then $gs_1 = s_2$ for some $g \in G$ and hence $g^{-1}s_2 = s_1$ so that $s_2 \sim s_1$. Finally, if $s_1 \sim s_2$ and $s_2 \sim s_3$, then $gs_1 = s_2$ and $hs_2 = s_3$ for some $g, h \in G$. Then we easily have $(hg)s_1 = h(gs_1) = hs_2 = s_3$ so that $s_1 \sim s_3$ and the proof is complete. ■

Definition 1.2.4 (Orbit) *If S is a G-set, the equivalence classes of the equivalence relation induced on S are called the* **orbits of S under G.** *If $s \in S$, the class containing s is called the* **orbit of s.**

Most authors denote the orbit of s under G by Gs. Artin is an exception (he thinks it looks too much like G_s, the isotropy group). Since the purpose of these lecture notes is primarily to facilitate reading Artin, we will adopt his notation scheme completely and denote the orbit of s under G by $\mathcal{O}_s$. Therefore,

$$\mathcal{O}_s = \{gs : g \in G\}.$$

Note that, by definition, s and t are in the same orbit if and only if $gs = t$ for some $g \in G$. The orbit of $s \in S$ is the singleton $\{s\}$ if and only if $gs = s$ for all $g \in G$. Such an element is called a **fixed point**. Note that $s \in S$ is a fixed point if and only if $G_s = G$. This is actually a special case of the relationship between the orbits of S and the group structure of G. This relationship will be at the heart of our upcoming applications of G-sets.

Theorem 1.2.5 (Counting formula) *If S is a G-set and $s \in S$, then $|\mathcal{O}_s| = [G : G_s]$. That is, the order of the orbit of s under G is the index of the stabilizer of s in G.*

Proof. The theorem states that two sets have the same number of elements. Our proof will be completely typical for such a result; we will establish a bijective function from $\mathcal{O}_s$ to G/G_s, the space of left cosets of G_s in G. The obvious choice for the map $\varphi : \mathcal{O}_s \to G/G_s$ is given by the rule $\varphi(gs) = gG_s$. We must show that this map is well defined and bijective. First, if $gs = hs$, then $h^{-1}gs = s$ so that $h^{-1}g \in G_s$ and hence $gG_s = hG_s$. This shows φ is well defined. Moreover, each of these implications are necessary as well as sufficient so that φ is injective. Finally, φ is trivially onto since if we are given $gG_s \in G/G_s$, then the element $gs \in \mathcal{O}_s$ and of course $\varphi(gs) = gG_s$. ∎

We conclude this lecture with a look at some orbits in our family of examples.

Example 1.2.6

1. If S_n acts on $\{1, 2, \ldots, n\}$ and $1 \leq j \leq n$, then the orbit of j is $\{1, 2, \ldots, n\}$ since you can send j to any position with all permutations. Note that in this case the counting formula states that $n!/(n-1)! = n$.

2. If G acts on itself by left multiplication, we have seen that the stabilizer of any point is trivial. It follows from the counting formula that the orbit of any element has order $|G|$ and hence is equal to G.

3. If G acts on itself by conjugation, the orbit of $h \in G$ is the set

$$\mathcal{O}_h = \{ghg^{-1} : g \in G\}.$$

   This orbit is always called the **conjugacy class of** h. Note that the counting formula for this example states that the size of a conjugacy class of h is the index of the centralizer of h in G.

4. If G acts on the set S of subgroups of G, then an element $H \in S$ is a fixed point if and only if H is normal in G.

Note that in examples 1 and 2, there is only one orbit (i.e. all elements are in the same orbit). We say that G **acts transitively on** S if there is exactly one orbit. We conclude this lecture by remarking that the counting formula can be combined with Lagrange's theorem to yield the following corollary. We leave the proof as an exercise for the reader.

Corollary 1.2.7 *If S is a G-set and $s \in S$, then $|G| = |G_s||\mathcal{O}_s|$.* ∎

1.3 The class equation of an action

We saw in the last lecture that if G is a group and S is a G-set, then the action of G on S partitions S into orbits $\mathcal{O}_s$. If S is a finite set, there are necessarily a finite number of orbits in this partition. Recall that $s \in S$ is a fixed point if the action if $\mathcal{O}_s = \{s\}$. Let S^G denote the set of fixed points so that

$$S^G = \{s \in S : gs = s \text{ for all } g \in G\}.$$

Since the orbits form a partition of S, it follows that $|S|$, the number of elements in S, is the sum over the disjoint orbits of the sizes of these orbits. Since each fixed point is in an orbit by itself, the sum over these singleton orbits is precisely the number of fixed points. All of this fits together into the following theorem.

Theorem 1.3.1 *If G is a group and S is a finite G-set, then*

$$|S| = |S^G| + \sum_{\substack{\text{disjoint non-} \\ \text{trivial orbits}}} |\mathcal{O}_s|.$$

Proof. The proof has essentially been given above. Namely, since the orbits from a partition of S, it follows immediately that the sum over all disjoint orbits $\sum |\mathcal{O}_s|$ is equal to $|S|$. By definition, an orbit $\mathcal{O}_s$ is non-trivial if $|\mathcal{O}_s| > 1$ so that $s \in S$ is a fixed point if and only if $\mathcal{O}_s$ is a trivial orbit. Therefore the sum over the trivial orbits is precisely the number of fixed points. ∎

This innocent looking formula is called the **class equation of the action (G-set)**. It has a surprising number of useful applications. We remark that for simplicity, we will only speak of the class equation of finite G-sets, although the notion can be defined for infinite G-sets as well. If G is a finite group, then the counting formula from the previous lecture implies that the number of elements in each orbit is a divisor of G. This puts a severe restriction on the positive integers that may occur in the class equation of a G-set. Before we can state our first application of the class equation we need to make a definition.

Definition 1.3.2 (p-Group) *A finite group G is a* **p-group** *if $|G| = p^n$ for some prime $p \in \mathbb{Z}$ and some positive integer $n \in \mathbb{N}$.*

We remark that a p-group is necessarily finite.

Proposition 1.3.3 *If G is a p-group and S is a finite G-set, then $|S| \equiv |S^G| \pmod{p}$.*

Proof. If $s \in S$ is in a non-trivial orbit, then $1 < |\mathcal{O}_s|$ and $|\mathcal{O}_s|$ is a divisor of $|G| = p^n$. It follows that $|\mathcal{O}_s| \equiv 0 \pmod{p}$. Therefore the class equation reduces modulo p to $|S| \equiv |S^G| \pmod{p}$. ■

1.4 Applications of G-set to counting

Suppose we wish to determine the number of distinguishable ways the faces of a cube can be marked with one to six dots to form a die. For example, a standard die is marked so that when it is placed on a table with the 1 on the bottom and the 2 facing front, the 6 is on top, the 3 on the left, the 4 on the right and the 5 to the back. There are other (distinguishable) ways to mark the die. If we temporarily distinguish between the faces of an unmarked cube calling them bottom, front, top, left, right and back, then there are 6 choices for how to mark the bottom, 5 choices for the front and so on so that there are $6! = 720$ ways to mark the die. We will say that two markings of the die are **indistinguishable** if one marking can be carried to the other by a rotation of the marked cube. For example, if the standard die described above is rotated 90° counter-clockwise (viewed from above), the 3 will be in front and so on, but it is the same die. The rotations of the die form a group G, with the law of composition being composition of rotations. If you like, you can think if G as a certain subgroup of S_8, since each rotation of the cube determines a permutation of the 8 vertices.

Now, each of the 6 faces of the cube can be placed down, and then any 1 of the 4 faces perpendicular to the table can be put in the front. Therefore there are 24 possible positions for the cube. Moreover, each one of these positions can be obtained from any other one by a rotation of the cube. It follows that $|G| = 24$.

Let S be the set of 720 possible markings of the cube. We note that G acts on S by rotating the cube. Two markings of the cube are indistinguishable if and only if they are in the same orbit. Therefore the problem of counting the distinguishable markings of the cube is equivalent to counting the number of distinct orbits in the G-set S.

The following theorem, due to Burnside, is a tool for determining the number of orbits of a finite G-set S in the case that G is a finite group. For notation, for each $g \in G$ we let

$$S_g = \{s \in S : gs = s\}$$

and recall that for each $s \in S$, $G_s = \{g \in G : gs = s\}$. Finally, recall that $\mathcal{O}_s = \{gs : g \in G\}$ is the orbit of s.

Theorem 1.4.1 (Burnside) *Let G be a finite group and S a finite G-set. If r is the number of orbits in S under G, then*

$$r \cdot |G| = \sum_{g \in G} |S_g|.$$

Proof. Let N be the number of elements $(g, s) \in G \times S$ such that $gs = s$. For each $g \in G$, there are exactly $|S_g|$ such pairs so that

$$N = \sum_{g \in G} |S_g|. \tag{1.1}$$

On the other hand, for each $s \in S$, there are exactly $|G_s|$ such pairs so that

$$N = \sum_{s \in S} |G_s|.$$

The counting formula together with Lagrange's theorem implies that for each $s \in S$ we have $|G_s| = |G|/|\mathcal{O}_s|$ so that

$$N = \sum_{s \in S} \frac{|G|}{|\mathcal{O}_s|} = |G| \left(\sum_{s \in S} \frac{1}{|\mathcal{O}_s|} \right).$$

Now, $1/|\mathcal{O}_s|$ has the same value for all s in the same orbit. Therefore of $\mathcal{O}$ is any orbit, then

$$\sum_{s \in \mathcal{O}} \frac{1}{|\mathcal{O}_s|} = 1.$$

Therefore we have

$$N = |G| \cdot (\text{the number distinct orbits}) = |G| \cdot r. \tag{1.2}$$

Equating the expressions for N in equations (1.2) and (1.1) gives the result. ■

Corollary 1.4.2 *If G is a finite group and S is a finite G-set, then*

$$(\text{the number of orbits of } S \text{ under } G) = \frac{1}{|G|} \cdot \sum_{g \in G} |S_g|.$$

■

Example 1.4.3 We can now easily answer our question regarding the markings of the die. Letting G denote the group of rotations of the cube, we note that if $g \in G$ and $g \neq e$, then $|S_g| = 0$ since every non-identity element of G takes any marking to a distinct marking. However, $|S_e| = 720$ since the identity element fixes every marking. Therefore if we let r denote the number of orbits of S under G (the number of distinguishable markings), the corollary to Burnside's theorem gives

$$r = \frac{1}{24} \cdot 720 = 30.$$

Example 1.4.4 How many distinguishable ways can seven people be seated at a round table, where there is no distinguishable "head" of the table? Of course there are 7! ways to assign people to different chairs. We let S be the set of the 7! possible assignments. A rotation of people achieved by asking each person to move to the place to the right results in the same arrangement. Such a rotation generates a cyclic group G of order 7, which we consider to act on S in the obvious way. Just as in the previous example, only the identity element $e \in G$ leaves any arrangement fixed, and it leaves all 7! arrangements fixed. It follows from the corollary to Burnside's theorem that if r is the number of orbits in S under G, then

$$r = \frac{1}{7} \cdot 7! = 6! = 720.$$

Therefore there are 720 different arrangements of people.

Example 1.4.5 How many distinguishable necklaces (with no clasp) can be made using seven different colored beads of the same size? Unlike the table in the previous example, a necklace can be turned over as well as rotated. Therefore we should consider the full dihedral group D_7 as acting on the set S of 7! possible arrangements of the beads. Since the order of D_7 is $|D_7| = 14$, the number r of distinguishable necklaces is

$$r = \frac{1}{14} \cdot 7! = 360.$$

In using the corollary to Burnside's theorem, you have to be able to compute $|G|$ and $|S_g|$ for all $g \in G$. in practice, computing $|G|$ will not present any difficulties. The next example shows that the computation of $|S_g|$ is not always as trivial as in the previous examples. We continue to assume that the reader is familiar with elementary combinatorics.

Example 1.4.6 We want to find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paint are available, assuming only one color is used on a single edge, and the same color may be used on different edges.

There are $4^3 = 64$ ways of painting the edges in all since each of the 3 edges can be painted any one of the 4 colors. Let S be the set of these 64 painted triangles. The group G acting on S is the symmetry group of the triangle and hence $G = D_3 = S_3$. We will use the notations for S_3 established in MAT 150A so that $x, y \in S_3$ satisfy $x^3 = 1$, $y^2 = 1$ and $yx = x^2y$. We must compute

$|S_g|$ for each of the six elements $g \in S_3$.

$\|S_1\| = 64$	each painted triangle is left fixed by $1 \in S_3$.
$\|S_x\| = 4$	to be invariant under $x \in S_3$, all edges must be the same color, and there are 4 colors.
$\|S_{x^2}\| = 4$	same reason as for x.
$\|S_y\| = 16$	the edges that are interchanged must be the same color (4 choices) and the remaining edge can be any color (times 4 choices).
$\|S_{xy}\| = 16$	same reason as for y.
$\|S_{x^2y}\| = 16$	same reason as for y.

Now we can compute

$$\sum_{g \in S_3} |S_g| = 64 + 4 + 4 + 16 + 16 + 16 = 120.$$

It follows that if r denotes the total number of distinguishable triangles, then

$$r = \frac{1}{6} \cdot 120 = 20.$$

1.5 Conjugation

The purpose of this lecture is to thoroughly investigate the notions of isotropy subgroups, orbits, fixed points and the class equation for the action of conjugation. Recall that a group G may act on itself in a number of ways, and by conjugation, we always mean the action defined by the mapping $G \times G \to G$ given by $(g, h) \mapsto ghg^{-1}$. The results we will find here are of interest by themselves. They will also play an important role in the subsequent lecture on the Sylow theorems.

The stabilizer of $h \in G$ under conjugation is called the **centralizer of h in G**. It is denoted by $Z(h)$ so that

$$Z(h) = \{g \in G : ghg^{-1} = h\} = \{g \in G : gh = hg\}.$$

Therefore we see that the centralizer of $h \in G$ is the set of those elements in G that commute with h. Note that $h \in Z(h)$ for all $h \in G$ since every element commutes with itself.

The orbit of $h \in G$ under conjugation is called the **conjugacy class of h** and is usually denoted by C_h. Therefore

$$C_h = \{h' \in G : h' = ghg^{-1} \text{ for some } g \in G.\}$$

In this notation, the counting formula for group actions reads

$$|G| = |C_h||Z(h)|$$

for all $h \in H$.

If S is any G-set, then an element $s \in S$ is a fixed point of the action if and only if its stabilizer $G_s = G$. Therefore in the case of conjugation, and element $h \in G$ is a fixed point if and only if the centralizer $Z(h) = G$. Recall that the center of a group G is the subgroup

$$Z = Z(G) = \{h \in G : gh = hg \text{ for all } g \in G\}.$$

Our remarks imply that $h \in G$ is a fixed point under the action of conjugation if and only if $h \in Z$ so that $|G^G| = |Z|$. We note that if $h \in Z$, then the counting formula implies that the conjugacy class of h consists of h alone. If we put all of this together, we see that the class equation for the action of a group G on itself by conjugation becomes

$$|G| = |Z| + \sum_{\substack{\text{non-trivial} \\ \text{conj.classes}}} |C_h|. \tag{1.3}$$

Note that for each $h \in G$, $|C_h| = [G : Z(h)]$ so that the size of any conjugacy class is a positive divisor of $|G|$. Moreover, if we denote the identity element of G by $1 \in G$, then $C_1 = \{1\}$ so that one of the numbers in (1.3) is always a 1. If the action of G is conjugation, the equation (1.3) is usually referred to as the **class equation of** G. That is, if no other action is specified, the term "class equation" always means the class equation of the action of G on itself by conjugation.

Example 1.5.1 The reader can check that the conjugacy classes for the group S_3 are the following three subsets:

$$\{1\}, \{x, x^2\}, \{y, xy, x^2y\}.$$

Therefore the class equation for S_3 is

$$6 = 1 + 2 + 3.$$

Among other things, this equation tells us that the center of S_3 is the trivial subgroup $\{1\}$.

If G is a p-group, the class equation can often be an effective tool in learning about the structure of G. The following two propositions illustrate this idea.

Proposition 1.5.2 *If G is a p-group, then $Z = Z(G) \neq \{1\}$. That is, the center of a p-group is always non-trivial.*

Proof. Using our previous result on p-group actions, we know that $0 \equiv |G| \equiv |Z| \pmod{p}$. Since $1 \in Z$, $|Z| \geq 1$ and hence $|Z| \geq p$ since $|Z| \equiv 0 \pmod{p}$. ∎

The next result is an interesting example of an application of G-sets to the classification of finite groups. If you like a good challenge, see if you can discover a proof that does not use group actions.

Proposition 1.5.3 *If $p \in \mathbb{Z}$ is a prime, then every group of order p^2 is abelian.*

Proof. Let $g \in G$ be an arbitrary element. It suffices to show that $Z(g) = G$ (why?). If $g \in Z$, then of course $Z(g) = G$ and we are done. Otherwise $Z(g)$ properly contains the center Z since $Z \subseteq Z(g)$ and $g \notin Z$. By the previous proposition, $|Z| \geq p$ so that $|Z(g)| > p$. But $|Z(g)|$ is a divisor of $|G| = p^2$ so that we must have $|Z(g)| = p^2$ and hence $Z(g) = G$. ∎

We conclude this lecture by remarking that the last result fails for higher powers of the prime p. For example, the dihedral group D_4 is a non-abelian group of order $8 = 2^3$.

1.6 Application: The Sylow Theorems

The purpose of this lecture is to illustrate the usefulness of group actions by proving a partial converse to the theorem of Lagrange. In particular, thanks to Lagrange, we know that if G is a finite group and H is any subgroup of G, then the order of H must divide $|G|$. We want to turn this question around: given a finite group G and a positive divisor d of $|G|$, can we find a subgroup H of G such that $|H| = d$? The answer to this question is **no** in general. For example, it can be shown that the alternating group A_4 (which has order 12) has no subgroup of order 6, even though 6 is a divisor of 12. The Sylow theorems assert that for a prime power divisor of $|G|$, there is a subgroup of that prime-power order. They also give information about the number of such subgroups.

These theorems are of vital importance by themselves, but we wish to emphasize again that we include them here mainly as an example of the power of the notion of group actions. As we will see, the set S that the group will act on will sometimes be the group itself, a collection of cosets of a subgroup or even the collection of all subgroups.

We begin by establishing some notation. Let S be a finite G-set with, say, r orbits and let $\{s_1, \ldots, s_r\}$ contain exactly one element from each orbit. Suppose that $\mathcal{O}_{s_i} = \{s_i\}$ for $0 \leq i \leq t$ so that $\{\mathcal{O}_{s_{t+1}}, \ldots, \mathcal{O}_{s_r}\}$ is the collection of non-trivial orbits. In this notation, the class equation of the

action on S becomes

$$|S| = |S^G| + \sum_{i=t+1}^{r} |\mathcal{O}_{s_i}|. \tag{1.4}$$

Most of the results in this lecture will follow from equation (1.4) once we choose the right set S and the right group action on S. We have already given a proof of the following theorem. We state it again for convenience as well as to emphasize its importance. This theorem seems to be amazingly powerful! In the rest of the lecture, if we choose the correct set, the correct group action on it and apply this theorem, what we want will seem to drop in our lap with no effort at all. Recall that a group G is a p-group of $|G| = p^n$ for some prime p and some positive integer $n \in \mathbb{N}$.

Theorem 1.6.1 *If G is a p-group and S is a finite G-set, then $|S| \equiv |S^G| \pmod{p}$.* ∎

Our goal in this lecture is to show that a finite group G has a subgroup of every prime power order dividing $|G|$. We begin with the special case known as Cauchy's theorem. For the rest of this lecture, p is always a prime integer.

Theorem 1.6.2 (Cauchy) *If G is a finite group and p divides $|G|$, then G has an element of order p and, consequently, a subgroup of order p.*

Proof. Let S be the set of all p-tuples $(g_1, \ldots, g_p)$ of elements of G such that $g_1 g_2 \cdots g_p = e$. That is,

$$S = \{(g_1, \ldots, g_p) : g_i \in G \text{ and } g_1 g_2 \cdots g_p = e\}.$$

We claim that p divides $|S|$. To see this, note that when forming a p-tuple in S, we may choose $g_1, \ldots, g_{p-1}$ arbitrarily and then g_p is uniquely determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$. Therefore $|S| = |G|^{p-1}$ and since p divides $|G|$ by hypothesis, we see that p divides $|S|$ as claimed.
Now define $\sigma \in S_p$ to be the cycle

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & p-1 & p \\ 2 & 3 & \cdots & p & 1 \end{pmatrix}$$

and let σ act on S by

$$\sigma(g_1, g_2, \ldots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_p, g_1).$$

Note that $(g_2, g_3, \ldots, g_p, g_1) \in S$ since $g_1(g_2 \cdots g_p) = e$ implies that $g_1 = (g_2 \cdots g_p)^{-1}$ so that $(g_2 \cdots g_p)g_1 = e$ as well. Therefore we see that σ does indeed act on S and we define an action of the cyclic subgroup $\langle \sigma \rangle$ of S_p on S by iteration in the obvious way.

Now, $|\langle\sigma\rangle| = p$ so that we may apply theorem (1.6.1), and hence we have $|S| \equiv |S^{\langle\sigma\rangle}| \pmod{p}$. Since p divides $|S|$, this congruence shows that p divides $|S^{\langle\sigma\rangle}|$ as well. Now, an element $(g_1, \ldots, g_p) \in S$ is left fixed by $\langle\sigma\rangle$ if and only if $g_1 = g_2 = \cdots = g_p$. We know that $(e, \ldots, e) \in S$ is one such element so that $|S^{\langle\sigma\rangle}| \geq 1$. But p divides this number and hence $|S^{\langle\sigma\rangle}| \geq p$. Therefore the exists at least one element $a \in G$, $a \neq e$, with $(a, \ldots, a) \in S$ so that $a^p = e$. Therefore G has an element of order p and $\langle a\rangle$ is a subgroup of order p. ■

Cauchy's theorem is a special case of the first Sylow theorem (there are three) which states that a group of order $p^n k, (p, k) = 1$, has a subgroup of order p^j for all $1 \leq j \leq n$. Before we can give the proof, we will need two technical lemmas.

If G is a group, let $\mathcal{S}$ denote the set of all subgroups of G and recall that G acts on $\mathcal{S}$ by conjugation. That is, the mapping $G \times \mathcal{S} \to \mathcal{S}$ given by $(g, H) \mapsto gHg^{-1}$ makes $\mathcal{S}$ a G-set. If $H \in \mathcal{S}$, the stabilizer G_H is the subgroup

$$G_H = \{g \in G : gHg^{-1} = H\}$$

and is called the **normalizer of H in G**. We will denote the normalizer of H in G by $N(H)$. Note that $N(H)$ is the largest subgroup of G in which H is normal, and H is normal in G if and only if $N(H) = G$ (nice exercises!). Here is the first lemma.

Lemma 1.6.3 *If G is a finite group and $H \leq G$ is a p-group, then*

$$[N(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. We let H act on G/H, the space of left cosets of H in G, by left translation so that $(h, xH) \mapsto (hx)H$. The crux of the proof is to determine the fixed points of this action and apply theorem (1.6.1). We compute

$$(hx)H = xH \iff x^{-1}hxH = H \iff x^{-1}hx \in H.$$

Therefore $h(xH) = xH$ for all $h \in H$ if and only if $x^{-1}hx \in H$ for all $h \in H$ if and only if $x \in N(H)$. It follows that the number of fixed points of G/H under H is the number of H cosets in $N(H)$, and this number is precisely $[N(H) : H]$. If we note that $|G/H| = [G : H]$, then an application of theorem (1.6.1) finishes the proof. ■

The second lemma is really just a corollary of the the previous one. Namely, we have the following.

Lemma 1.6.4 *Let H be a p-subgroup of a finite group G. If p divides $[G : H]$, then $N(H) \neq H$.*

Proof. If p divides $[G : H]$, then lemma (1.6.3) implies that p divides $[N(H) : H]$. Therefore $[N(H) : H] \neq 1$ and hence $N(H) \neq H$. ∎

We can now state and prove the first Sylow theorem; the main goal of this lecture.

Theorem 1.6.5 (First Sylow Theorem) *Let G be a finite group with $|G| = p^n k$, $n \geq 1$ and $(p, k) = 1$. Then for each $1 \leq j \leq n$, G has a subgroup P_j of order p^j. Moreover, P_j is normal in P_{j+1} for $1 \leq j < n$.*

Proof. By Cauchy's theorem (1.6.2), G has a subgroup P_1 of order p. We proceed by induction. Namely, we will show that if $1 \leq j < n$ and G has a subgroup P_j of order p^j, then G has a subgroup P_{j+1} of order p^{j+1}. Suppose then that $P_j \leq G$ has order p^j for some $j < n$. It follows that p divides $[G : P_j]$ (why?) and hence p divides $[N(P_j) : P_j]$ by lemma (1.6.3). Now, P_j is normal in $N(P_j)$ so that $N(P_j)/P_j$ is a group and our previous remark implies that p divides the order $|N(P_j)/P_j|$. Now we apply Cauchy's theorem (1.6.2) to the group $N(P_j)/P_j$ to find a subgroup K of order p in $N(P_j)/P_j$. If $\eta : N(P_j) \to N(P_j)/P_j$ is the quotient map, then $\eta^{-1}(K) \leq G$ is a subgroup of G such that $P_j \leq \eta^{-1}(K) \leq N(P_j)$. It follows that P_j is normal in $\eta^{-1}(K)$, and moreover, the first isomorphism theorem implies that $|\eta^{-1}(K)| = p^{j+1}$. ∎

One consequence of the first Sylow theorem is that every finite group G has a maximal prime-power order subgroup for every prime that divides $|G|$. That is, if $|G| = p^n k, n \geq 1, (p, k) = 1$, then G has a subgroup of order p^n.

Definition 1.6.6 (Sylow p-subgroup) *If G is a finite group with order $|G| = p^n k, n \geq 1, (p, k) = 1$, then a subgroup of order p^n is called a* **Sylow p-subgroup**.

Recall that conjugation by a fixed $g \in G$ is an automorphism of the group G so that, in particular, if P is a Sylow p-subgroup of G, then every conjugate subgroup gPg^{-1} is also a Sylow p-subgroup. The next theorem says that we get all Sylow p-subgroups in this way. The proof is an absolutely beautiful application of group actions!

Theorem 1.6.7 (Second Sylow Theorem) *If P and Q are any two Sylow p-subgroups of a finite group G, then $P = gQg^{-1}$ for some $g \in G$. That is, any two Sylow p-subgroups of a finite group G are conjugate.*

Proof. Let $\mathcal{S} = G/P$ be the set of left cosets of P in G and let Q act on $\mathcal{S}$ by left translation so that $a(bP) = (ab)P$ for $a \in Q$ and $b \in G$. Now Q is a p-group so that theorem (1.6.1)implies that

$|\mathcal{S}| \equiv |\mathcal{S}^Q| \pmod{p}$. But $|\mathcal{S}| = [G : P] = k$ is not divisible by p so that $|\mathcal{S}^Q| \neq 0$. If $bP \in \mathcal{S}^Q$, then $abP = bP$ for all $a \in Q$ iff. $b^{-1}abP = P$ for all $a \in Q$ iff. $b^{-1}ab \in P$ for all $a \in Q$ iff. $b^{-1}Qb \leq P$. But $|b^{-1}Qb| = |P|$ so that $b^{-1}Qb = P$ and P and Q are conjugate as desired. ■

The third (and final!) Sylow theorem provides a method for counting how many Sylow p-subgroups a finite group G has. You will show in your homework that a Sylow p-subgroup is normal iff. it is unique. Therefore the following theorem can also be used to find normal subgroups of a group G. Once again, note how elegant the proof is with the notion of group actions.

Theorem 1.6.8 (Third Sylow Theorem) *If G is a finite group such that $|G| = p^n k, n \geq 1$, $(p, k) = 1$, then the number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.*

Proof. Let P be a Sylow p-subgroup of G and let $\mathcal{S}$ be the set of all Sylow p-subgroups of G. Then P acts on $\mathcal{S}$ by conjugation and theorem (1.6.1) implies that $|\mathcal{S}^P| \equiv |\mathcal{S}| \pmod{p}$. Now, $Q \in \mathcal{S}^P$ iff. $aQa^{-1} = Q$ for all $a \in P$ iff. $P \leq N(Q)$. Of course $Q \leq N(Q)$ so that Q and P are two Sylow p-subgroups of $N(Q)$. The second Sylow theorem (1.6.7) implies they are conjugate in $N(Q)$. But since Q is normal in $N(Q)$, it is only conjugate to itself so that $Q = P$. It follows that $\mathcal{S}^P = \{P\}$ so that $|\mathcal{S}| \equiv 1 \pmod{p}$ as claimed.

Now let G act on $\mathcal{S}$ by conjugation. Again, the second Sylow theorem (1.6.7) implies that there is only one orbit in $\mathcal{S}$ under this action so that $|\mathcal{S}| = [G : N(P)]$ where $P \in \mathcal{S}$. Therefore $|\mathcal{S}|$ (the number of Sylow p-subgroups of G) is a divisor of $|G|$. ■

Example 1.6.9 We will show that no group of order 15 is simple. Recall that a group is simple if it has no non-trivial normal subgroups. Suppose that $|G| = 15$ and let P be a Sylow 5-group. We know P exists by the first Sylow theorem (1.6.5). Moreover, the third Sylow theorem (1.6.8) implies that the number of such P is of the form $5k + 1$ and is a divisor of 15. The only possibility is to take $k = 0$ so that there is exactly 1 Sylow 5-group which is necessarily normal in G by the second Sylow theorem (1.6.7).

Chapter 2

Symmetry

2.1 The orthogonal group O_n

The applications of group theory to symmetry are arguably the most exciting and most important parts of the theory. Indeed, symmetry and symmetrical structures arise in all branches of science and mathematics so that one can find numerous interesting applications of the work we are about to undertake. We will focus primarily on symmetry of figures in the Euclidean plane $\mathbb{R}^2$, but we will also partially study some symmetries of 3-dimensional figures in $\mathbb{R}^3$ as well. It will turn out that understanding the mathematics of rotations in $\mathbb{R}^2$ and $\mathbb{R}^3$ is crucial. We therefore begin our investigation with a careful treatment of this matter.

The reader is most likely aware that a rotation of the Euclidean plane $\mathbb{R}^2$ about the origin through an angle θ is a linear operator on $\mathbb{R}^2$ whose matrix with respect to the standard basis $\{e_1, e_2\}$ for $\mathbb{R}^2$ is given by

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

A rotation of $\mathbb{R}^3$ is slightly more difficult to describe. Usually, a rotation in 3-space is given by a pair (v, θ) where $v \in \mathbb{R}^3$ is a unit vector (the axis of rotation), and θ is a real number that gives the amount of the rotation through the line spanned by v. Note that there are some subtleties to this definition. Namely, the distinct pairs (v, θ) and $(-v, -\theta)$ represent the same rotation of $\mathbb{R}^3$. The primary goal of this lecture is to give a definition of a rotation in 3-space, and then to show that all such rotations are linear operators on $\mathbb{R}^3$. In fact, they are all special orthogonal operators.

Recall that a real $n \times n$ matrix A is called **orthogonal** if $AA^t = I_n$, where A^t is the transpose of A and I_n is the $n \times n$ identity matrix. The reader has no doubt proved in an elementary linear algebra class that if A is an orthogonal matrix over $\mathbb{R}$, then $\det A = \pm 1$. The set of all orthogonal $n \times n$ matrices forms a subgroup of $\mathrm{GL}_n(\mathbb{R})$ denoted by $\mathrm{O}_n(\mathbb{R})$ or sometimes just O_n. This group is called the **orthogonal group**. The reader can check that the subset of those $A \in \mathrm{O}_n$ satisfying $\det A = +1$ forms a subgroup called the **special orthogonal group**. It is denoted by $\mathrm{SO}_n(\mathbb{R})$ or just SO_n so that

$$\mathrm{SO}_n = \{A \in \mathrm{O}_n : \det A = 1\}.$$

We leave it as an exercise for the reader to show that $[\mathrm{O}_n : \mathrm{SO}_n] = 2$ and hence SO_n is a normal subgroup of O_n. Before we can prove that any rotation of $\mathbb{R}^3$ is given by multiplication by an element $A \in \mathrm{SO}_3$, we will need some facts about the Euclidean inner product (dot product) and isometries (distance preserving maps). For convenience, we write all vectors $X \in \mathbb{R}^n$ as column vectors with respect to the standard basis.

Definition 2.1.1 (Dot product) *If $X, Y \in \mathbb{R}^n$, then the* **dot product** *or* **Euclidean inner product** *of X and Y is the real number*

$$X \cdot Y = X^t Y = x_1 y_1 + \cdots + x_n y_n.$$

Surprising as it may seem, the dot product is the link between the geometry of the set $\mathbb{R}^n$ and the algebra of the vector space $\mathbb{R}^n$. Specifically, the reader can easily check that for a vector $X \in \mathbb{R}^2$, we have

$$X \cdot X = x_1^2 + x_2^2$$

so that $\sqrt{X \cdot X} = |X|$ is the length of the vector X. The same formula can be taken as the definition of the length of a vector $X \in \mathbb{R}^n$. That is, for $X \in \mathbb{R}^n$, we define the **length of** X to be the scalar $|X| = \sqrt{X \cdot X}$. We also define the **distance between** X **and** Y to be the length $|X - Y|$ of $X - Y$. Now, if X and Y are vectors in $\mathbb{R}^2$ or $\mathbb{R}^3$, then applying the law of cosines to the triangle with vertices $0, X$ and Y gives

$$X \cdot Y = |X||Y| \cos\theta$$

where θ is the angle subtended by the sides X and Y. If X and Y are both non-zero, then this formula shows that $X \cdot Y = 0$ iff. $\theta = \pi/2$. This motivates the following definition.

Definition 2.1.2 (Orthogonal) *Two vectors X and Y in $\mathbb{R}^n$ are* **orthogonal** *if $X \cdot Y = 0$. A set of vectors $S = \{X_1, \ldots, X_m\}$ is* **orthogonal** *if X_i and X_j are orthogonal for all $i \neq j$. If, in addition, we have $|X_i| = 1$ for all i, then S is called an* **orthonormal set**. *An orthonormal set that is also a basis is called an* **orthonormal basis**.

The following theorem justifies the repetitious use of the term orthogonal. Before we give the statement and proof, now is a good time to remind the reader that if A is an $n \times n$ matrix and e_i is the ith standard basis vector in $\mathbb{R}^n$, then $Ae_i \in \mathbb{R}^n$ is the ith column of A.

Theorem 2.1.3 *If A is a real $n \times n$ matrix, then the following are equivalent.*

1. *$A \in \mathrm{O}_n$.*
2. *The dot product is invariant under A. That is, $AX \cdot AY = X \cdot Y$ for all $X, Y \in \mathbb{R}^n$.*
3. *The columns of A are pair-wise orthogonal unit vectors in $\mathbb{R}^n$.*

Proof. ((1) $\Longrightarrow$ (2)) Suppose that $A \in \mathrm{O}_n$ so that $A^tA = I_n$. Then, recalling $X \cdot Y = X^tY$, we have for all $X, Y \in \mathbb{R}^n$,

$$AX \cdot AY = (AX)^t(AY) = X^tA^tAY = X^tY = X \cdot Y$$

so that the dot product in invariant under A.
((2) $\Longrightarrow$ (3)) If the dot product is invariant under A, then in particular we have for each pair of standard basis vectors (e_i, e_j),

$$\delta_{ij} = e_i \cdot e_j = Ae_i \cdot Ae_j.$$

Now, $c_i = Ae_i$ is the ith column of A so that we see $c_i \cdot c_j = \delta_{ij}$ and hence the columns of A form an orthonormal set $\{c_1, \ldots, c_n\}$. In particular, we have that each c_i is a unit vector and the c_i are pair-wise orthogonal.
((3) $\Longrightarrow$ (1)) We must show that $A^tA = I_n$. The ij-entry of the product A^tA is computed by taking the dot product of the ith row of A^t with the jth column of A. But the ith row of A^t is the ith column of A so that, using the notation above, we have that the ij-entry of A^tA is $c_i \cdot c_j$. If $\{c_1, \ldots, c_n\}$ is an orthonormal set, then we see that $c_i \cdot c_j = \delta_{ij}$ so that $A^tA = I_n$ as desired. ∎
This theorem is the first hint at the relationship between rotations in $\mathbb{R}^3$ and orthogonal matrices. That is, it shows that orthogonal matrices are linear maps that preserve angles between vectors. Actually, by preserving the dot product, an orthogonal operator preserves distance between vectors

as well (why?). Putting all of this together, an orthogonal operator is a linear map $\mathbb{R}^n \to \mathbb{R}^n$ that fixes the origin and preserves the distance and angles between vectors. Our next step is show that any map $\mathbb{R}^n \to \mathbb{R}^n$ with these properties is given by an orthogonal matrix! Let's begin with a definition.

Definition 2.1.4 (Isometry) *A map $m : \mathbb{R}^n \to \mathbb{R}^n$ is an* **isometry** *or a* **rigid motion** *if*

$$|m(X) - m(Y)| = |X - Y|$$

for all $X, Y \in \mathbb{R}^n$. That is m is an isometry if m preserves distance between vectors.

Note that every rotation of $\mathbb{R}^3$ is an isometry. We leave it as an exercise for the reader to show that the composition of isometries is an isometry. Of course the identity $1_{\mathbb{R}^n} : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry. Every isometry is invertible and its inverse is again an isometry so that the set M_n of all isometries of $\mathbb{R}^n$ form a group under function composition. We usually call the group M_n the **group of motions of** $\mathbb{R}^n$ or the **isometry group of** $\mathbb{R}^n$. We will also use the notation $\mathrm{Iso}(\mathbb{R}^n)$ to denote the isometry group of $\mathbb{R}^n$. (In fact, we prefer it!)

Theorem 2.1.5 *If $m : \mathbb{R}^n \to \mathbb{R}^n$ is a map, then the following are equivalent:*

1. *The map m is an isometry that fixes the origin.*
2. *The map m preserves dot product.*
3. *The map m is given by left multiplication by an $n \times n$ orthogonal matrix.*

Proof. ((1) $\Longrightarrow$ (2)) If m is an isometry, then for all $X, Y \in \mathbb{R}^n$, we have

$$(X - Y) \cdot (X - Y) = |X - Y|^2 = |m(X) - m(Y)|^2 = (m(X) - m(Y)) \cdot (m(X) - m(Y)).$$

Letting $Y = 0$ shows that $X \cdot X = m(X) \cdot m(X)$. If we expand both sides of the above equality and cancel $X \cdot X$ with $m(X) \cdot m(X)$ and $Y \cdot Y$ with $m(Y) \cdot m(Y)$, we see that $X \cdot Y = m(X) \cdot m(Y)$ so that m preserves dot product.

((2) $\Longrightarrow$ (3)) First, as a special case, suppose that m preserves dot product and $m(e_i) = e_i$ for all i. Then for any $X \in \mathbb{R}^n$,

$$x_i = X \cdot e_i = m(X) \cdot m(e_i) = m(X) \cdot e_i$$

so that $X = m(X)$ and m is the identity. Now, if m preserves dot product, we let

$$\mathcal{B} = \{m(e_1), \ldots, m(e_n)\}$$

and note that $\mathcal{B}$ is an orthonormal basis (why?). If $A = [\mathcal{B}]$, then A is an orthogonal matrix by theorem (2.1.3) and hence $A^{-1} = A^t$ is also orthogonal and therefore preserves dot product. It follows that the composition $A^{-1}m$ preserves dot product and maps e_i to e_i for all i. Therefore, by the special case proved above, $A^{-1}m$ is the identity on $\mathbb{R}^n$ so that $A = m$ is multiplication by an orthogonal matrix.

$((3) \Longrightarrow (1))$ Suppose that m is linear with an orthogonal matrix A representing m in the standard basis. Then $m(0) = 0$ since m is linear. Moreover, theorem (2.1.3) implies that m preserves dot product and hence distance so that m is an isometry. ∎

Definition 2.1.6 (Rotation) *A map $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ is a* **rotation about the origin** *if ρ is an isometry fixing the origin, ρ fixes a unit vector $X \in \mathbb{R}^3$ and the restriction of ρ to the plane orthogonal to the line spanned by X is a rotation.*

We can (finally) state our main theorem.

Theorem 2.1.7 *The rotations about the origin in $\mathbb{R}^2$ (respectively $\mathbb{R}^3$) are in one to one correspondence with elements of the special linear group $\mathrm{SO}_2(\mathbb{R})$ (respectively $\mathrm{SO}_3(\mathbb{R})$).*

We have already shown one direction of the theorem (why?). However, we still need one more technical lemma before we can give a concise proof. We omit the proof of the lemma, as it is written in Artin, and we do not have a "better" proof.

Lemma 2.1.8 *If $A \in \mathrm{SO}_3(\mathbb{R})$, then A has an eigenvalue $\lambda = 1$.* ∎

Proof of theorem (2.1.7) If $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ is a rotation, then ρ is an isometry that fixes the origin so that theorem (2.1.5) implies that ρ is given by an orthogonal matrix A. It follows that $\det A = \pm 1$. Now, the determinant is an integer valued continuous function of the angle of rotation, and hence constant. But the identity is the matrix of the 0 rotation so that this constant value is $+1$. Therefore $A \in \mathrm{SO}_3(\mathbb{R})$. (We remark that the same argument applies to $\mathbb{R}^2$, or $\mathbb{R}^n$ for any n.)

For the converse, we must specialize to the cases $n = 2, 3$. If $A \in \mathrm{SO}_2(\mathbb{R})$, let $v_1 = Ae_1$ and let ρ be the rotation of $\mathbb{R}^2$ that takes e_1 to v_1. Let B be the matrix of ρ and note that $B \in \mathrm{SO}_2(\mathbb{R})$ so that $C = A^{-1}B \in \mathrm{SO}_2(\mathbb{R})$. Moreover $Ce_1 = e_1$. Now Ce_2 is a unit vector orthogonal to e_1 so it is either e_2 or $-e_2$, the latter being ruled out because $\det C = 1$. Therefore $C = I_2$ and $A = B$ is a rotation. If $A \in \mathrm{SO}_3(\mathbb{R})$, then lemma (2.1.8) shows that A has an eigenvector X with an eigenvalue 1. Moreover, theorem (2.1.5) implies that A is an isometry that fixes the origin. It remains to show

that A acts as a rotation in the plane $\mathcal{P}$ orthogonal to the line spanned by X. Let X_2 and X_3 be any two orthogonal unit vectors in $\mathcal{P}$ and let $X = X_1$ so that $\mathcal{B} = (X_1, X_2, X_3)$ is an orthonormal basis for $\mathbb{R}^3$. If $P = [\mathcal{B}]^{-1}$, then $A' = PAP^{-1}$ represents the same linear operator as does A. Moreover, $A' \in \mathrm{SO}_3(\mathbb{R})$ (why?). Now, X_1 is an eigenvector with eigenvalue 1 for A' as well, and moreover, since A' is orthogonal, $A'(\mathcal{P}) = \mathcal{P}$ so that the matrix for A' with respect to the basis $\mathcal{B}$ has the form

$$\begin{bmatrix} 1 & 0 \\ 0 & B \end{bmatrix}.$$

Note that the columns of B are orthogonal unit vectors in $\mathcal{P}$ so that $B \in \mathrm{O}_2$ is orthogonal. Moreover $\det B = \det A' = 1$ so that $B \in \mathrm{SO}_2$ is a rotation as desired. ■

We end this lecture with a remark on isometries that do not fix the origin. If $b \in \mathbb{R}^n$ is a fixed vector, then the map $t_b : \mathbb{R}^n \to \mathbb{R}^n$ defined by $t_b(X) = X + b$ is an isometry (exercise). If $b \neq 0$, then t_b does not fix the origin. The following theorem is remarkable!

Theorem 2.1.9 *If m is an isometry of $\mathbb{R}^n$, then there exist unique $A \in \mathrm{O}_n(\mathbb{R})$ and $b \in \mathbb{R}^n$ such that $m(X) = AX + b$ for all $X \in \mathbb{R}^n$.*

Proof. Let $b = m(0)$ and note that $t_{-b}m$ is an isometry fixing the origin so that $A = t_{-b}m \in \mathrm{O}_n(\mathbb{R})$ by theorem (2.1.5). If we apply t_b to both sides of this equality, we are done. ■

2.2 Symmetry of figures in $\mathbb{R}^2$

The purpose of this lecture is to describe what a mathematician means when he or she speaks about "symmetry". We also will begin a careful study of the isometry group $\mathrm{Iso}(\mathbb{R}^2)$ of the Euclidean plane.

The word "symmetry" is common in everyday language, and the usage of the term in modern mathematics encompasses this common meaning and more. To begin, if S is a set, then by a **transformation of** S, a modern geometer means a bijection $S \to S$, and the permutation group $A(S)$ is called the **(full) transformation group**. One of the fathers of contemporary geometry was the German mathematician Felix Klein (1849-1925). He gave the following definition of a geometry in 1872.

Definition 2.2.1 (Geometry) *A* **geometry** *is the study of those properties of a space (set) that remain invariant under some fixed subgroup of the full transformation group.*

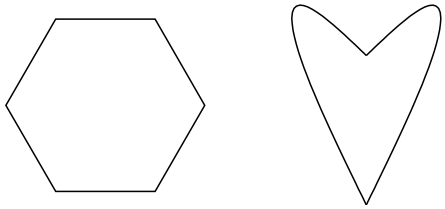
This definition is actually not quite as inclusive as the current definition of a geometry, but it will serve our purposes. In the next few lectures, we are going to study symmetries of figures in the Euclidean plane $\mathbb{R}^2$ and Euclidean 3-space $\mathbb{R}^3$. The definition of symmetry that we will give uses the language of geometry. We will therefore content ourselves to illustrating Klein's definition of geometry it applies to classical Euclidean geometry, our subject of study. However, the reader should keep in mind that *any* notion of a geometry can be defined in this way.

To give the following definition, we do not need that $n = 2$ or 3. Therefore let $S = \mathbb{R}^n$, $n \geq 1$, and consider the subgroup $\mathrm{Iso}(\mathbb{R}^n)$ of $A(\mathbb{R}^n)$. That is, we choose our fixed subgroup of the full transformation group $A(\mathbb{R}^n)$ to be the subgroup of distance preserving maps. Then the **Euclidean geometry of** $\mathbb{R}^n$ is the study of those properties of $\mathbb{R}^n$ that are left invariant under $\mathrm{Iso}(\mathbb{R}^n)$. We have seen that the dot product, and hence angles between vectors, is one such property. There are others such as area and volume for example.

From now on, we specialize to the case $n = 2$. To maintain the geometrical spirit of our work, will call subsets of $\mathbb{R}^2$ **figures**. Usually, it is possible to give a mathematical description of the figures we will be interested in. That is, we can specify the set of points $(x, y) \in \mathbb{R}^2$ that are contained in the figure. The degree of precision is often unnecessary, and we will usually just give a figure in $\mathbb{R}^2$ by drawing it. Here is the main definition of the lecture.

Definition 2.2.2 (Symmetry of a plane figure) *If F is a figure in $\mathbb{R}^2$, then a* **symmetry of** F *is an element $m \in \mathrm{Iso}(\mathbb{R}^2)$ such that $m(F) = F$. The set of all symmetries of F form a subgroup of* $\mathrm{Iso}(\mathbb{R}^2)$ *called the* **symmetry group of the figure**.

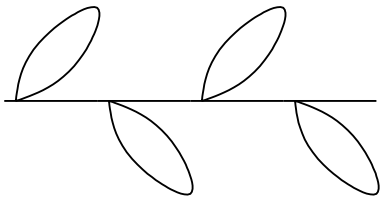
In other words, a symmetry of F is a distance preserving map $m : \mathbb{R}^2 \to \mathbb{R}^2$ that sends F onto itself. We often imagine m as a motion of the plane (an orthogonal motion followed by a translation in fact!), so that a symmetry of F is a motion of the plane that carries F onto itself. We will see in the next lecture that the group $\mathrm{Iso}(\mathbb{R}^2)$ acts on the plane in a natural way, and the symmetry group of a figure is nothing more that the isotropy subgroup of the figure under this $\mathrm{Iso}(\mathbb{R}^2)$ action. Before we begin our careful investigation of this group action, let us look at some examples of figures in the plane, and informally discuss their respective symmetry groups. Symmetries of figures in the plane are classified as having either **reflective, rotational, translational** or **glide** symmetry. Sometimes a figure can have all of these types of symmetries simultaneously! For example, the hexagon and heart shape shown here have rotational and reflective symmetries respectively.



Rotational and reflective symmetry. Reflective symmetry only.

Figure 2.1: The hexagon and heart shape shown here are examples of figures in the plane $\mathbb{R}^2$. The question of determining the symmetry groups of these figures is the question of finding all isometries of the plane $\text{Iso}(\mathbb{R}^2)$ that map these figures to themselves. In the case of the hexagon, the symmetry group has exactly 12 elements: 6 rotations and 6 reflections. In fact, this symmetry group is isomorphic to the dihedral group D_6. The symmetry group of the heart shape has just 2 elements and is therefore isomorphic to $\mathbb{Z}_2$.

Note that the hexagon has reflective symmetry as well. Neither figure has any translational symmetry, and hence no glide symmetry either. A glide symmetry in a figure is a composition of a reflective symmetry with a translation. The following figure is an example of a planar figure with glide symmetry. In this picture, the reader should imagine that the figure repeats infinitely in both directions.



The figure has an infinite symmetry group.

Figure 2.2: The figure shown here has glide symmetry. We can reflect the picture in the horizontal line and then shift it to the right. This is the glide reflection. Note that the composition of the glide reflection with itself is a non-zero translation. It follows that the symmetry group of this figure is infinite. (why?)

It is possible that a figure in the plane has a **trivial symmetry group**. That is, it is possible that the only element of the isometry group that maps the figure to itself is the identity element. If this is the case, we (somewhat incorrectly) say that the figure has **no symmetry** or is **asymmetrical**. It is

easy to draw asymmetrical figures. For example, the Roman alphabet contains many asymmetrical letters.

The roman letter "F" has no symmetry.

Figure 2.3: Paradoxically, if a figure has the trivial subgroup for its symmetry group, we say that the figure has no symmetries.

In the next few lectures, we are going to carefully study the possible symmetries of figures in the plane $\mathbb{R}^2$. We have already said that each such figure has a symmetry group - a subgroup of $\mathrm{Iso}(\mathbb{R}^2)$. We will therefore begin our investigation of symmetries with a thorough investigation of the possible subgroups of $\mathrm{Iso}(\mathbb{R}^2)$. We conclude this lecture with a remark on creating figures with a specified symmetry group. We have mentioned that the isometry group $\mathbb{R}^2$ acts on the plane by applying the isometry. Therefore if G is a subgroup of $\mathrm{Iso}(\mathbb{R}^2)$, and F is a subset of the plane, then the union of the sets in the orbit of F under the action of G is a figure with symmetry group G by definition. In other words, you can draw any figure in the plane, and then look at the action on G on that figure to determine a figure with symmetry group G. The following pictures illustrates this idea.

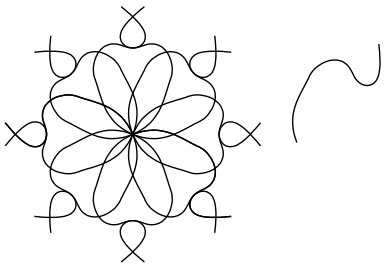


Figure 2.4: This figure was created by letting the dihedral group D_8 act on the curve shown on the right. The center of the rotations was chosen to be the lower end point of the curve and the line of reflection was chosen to be horizontal. The symmetry group of the figure on the left is therefore D_8.

To create nice looking figures with this process, it is usually best to begin with an asymmetrical figure. However, you can combine symmetries in your beginning figure with those in the group G to create very complex symmetrical patterns in the end result. The Artist M.C. Escher was a master

of this idea. We end this lecture some figures taken from *The World of M.C. Escher*, (Harry N. Abrams, Inc., New York). The first illustrates an action of $\mathbb{Z}\times\mathbb{Z}$ on $\mathbb{R}^2$. Can you find a fundamental region?

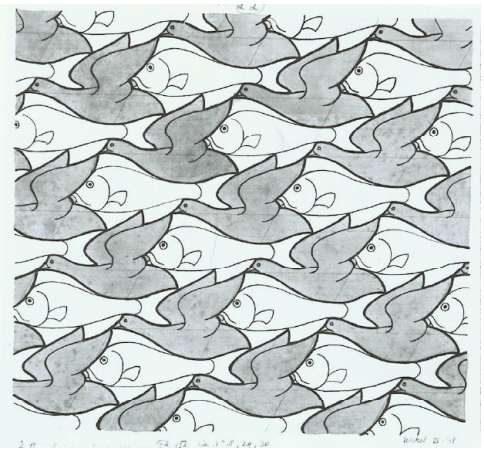


Figure 2.5: The symmetry group of this figure has two independent translations. It has no rotational nor reflective symmetry. The symmetry group is isomorphic to $\mathbb{Z}\times\mathbb{Z}$.

The figure in Figure 2.6 has a more complicated symmetry group. In addition to two independent translations, the symmetry group of this figure contains rotations of order 3. One of the consequences of our work will be that if the symmetry group of a figure contains rotations about distinct points, then it is infinite. Therefore the symmetry group of the figure in Figure 2.6 is infinite. We will also be able to show that no figure such as Figure 2.6 can have rotations of order 5.

We end with a figure (2.7) that illustrates the very same ideas that we have been discussing, but in another geometry! In terms of distance, the Euclidean geometry is given by the metric $ds^2 = dx^2 + dy^2$. This just means that the distance between two points in the plane is the sum of the squares of the changes in the x and y coordinates. The **hyperbolic plane** H^2 is modeled on the open upper half-plane

$$\mathbb{R}^2_+ = \{(x, y) \in \mathbb{R}^2 : y > 0\}$$

but with the metric $ds^2 = (1/y^2)(dx^2 + dy^2)$. By definition, **hyperbolic geometry** is the study of those properties of H^2 left invariant by the isometry group of H^2. This isometry group is not the same as the isometry group for Euclidean geometry. It is, however, generated by reflections in "hyperbolic lines". You can use linear fractional transformations to map the half-plane model of H^2 into the interior of the unit disc to obtain another model of H^2. The latter model is usually referred

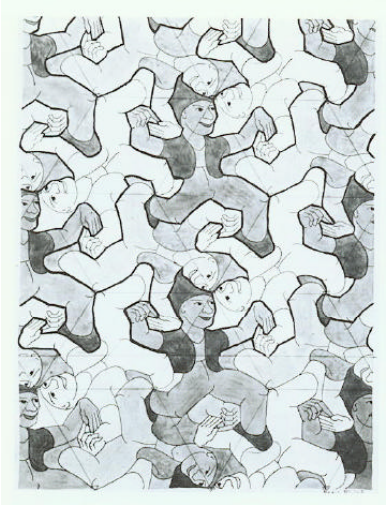


Figure 2.6: In addition to two independent translations, the symmetry group of this figure contains rotations of order 3. If you look carefully, you can see the artist's hexagonal grid on which the work is based.

to as the Poincaré disc. Figure 2.7 shows a figure in the Poincaré disc. It was generated by letting a certain subgroup of the hyperbolic isometry group act on one of the fundamental regions.

2.3 The isometry group of $\mathbb{R}^2$

We already know many facts about the group $\mathrm{Iso}(\mathbb{R}^n)$ of isometries of $\mathbb{R}^n$. The purpose of this lecture is to classify isometries of the plane $\mathbb{R}^2$ as well as give a set of generators for this group that facilitate computation. Recall that $\mathrm{Iso}(\mathbb{R}^2)$ is a subgroup of $A(\mathbb{R}^2)$, the full transformation group of the plane. The plane $\mathbb{R}^2$ is a $A(\mathbb{R}^2)$-set under the natural action (see Example 1.1.2(2)), and therefore $\mathbb{R}^2$ is an $\mathrm{Iso}(\mathbb{R}^2)$-set. To be specific, we have $(m, X) \mapsto m(X)$ for all $m \in \mathrm{Iso}(\mathbb{R}^2)$ and all $X \in \mathbb{R}^2$.

Recall that if m is an isometry of $\mathbb{R}^2$, then there exist unique elements $A \in \mathrm{O}_2$ and $b \in \mathbb{R}^2$ such that $m(X) = AX + b$ for all $X \in \mathbb{R}^2$. That is, m is given by an orthogonal operator followed by a translation. The uniqueness of A allows us to make the following definition.

Definition 2.3.1 *An isometry m is* **orientation preserving** *if* $\det A = 1$ *and* **orientation reversing** *if* $\det A = -1$ *where* $A \in \mathrm{O}_2$ *satisfies* $m = t_b \circ A$.

Figure 2.7: The artist M.C. Escher had a deep understanding of symmetry and actions of the isometry group on the plane. The original piece of art was done as a two color wood cut in 1960. It is entitled *Circle Limit IV*. As this picture shows, Escher was familiar with hyperbolic isometry groups.

Intuitively, m is orientation reversing if it flips the plane over, and orientation preserving if it does not flip the plane over. The proof of the following proposition is left as an exercise for the reader.

Proposition 2.3.2 *The map* $\mathrm{Iso}(\mathbb{R}^2) \to \{\pm 1\}$ *that maps* m *to* 1 *if* m *is orientation preserving and* -1 *if* m *is orientation reversing is a homomorphism and hence the orientation preserving motions form a normal subgroup of* $\mathrm{Iso}(\mathbb{R}^2)$. ∎

We can further classify motions of the plane if we look at fixed point behavior.

1. Translations $X \mapsto X + b$, $b \neq 0$. No fixed points.
2. Rotations about a point. Exactly one fixed point.
3. Reflections in a line l. Fixes every point on l.
4. Glide reflections. No fixed points.

It is absolutely remarkable that this list is complete! That is, every rigid motion of the plane is one of the four types listed above. Before we state and prove this theorem, let us define a convenient set of generators for the group $\mathrm{Iso}(\mathbb{R}^2)$. This is the exact analog of choosing our generators x and y for the dihedral groups D_n. In this case, the group $\mathrm{Iso}(\mathbb{R}^2)$ is infinite and we will need infinitely many generators. We will work in the standard basis, writing vectors as column vectors. We then

choose as generators the translations, rotations about the origin and the reflection in the e_1-axis. For notation, if $a \in \mathbb{R}^2$ is a non-zero vector, and $\theta \in \mathbb{R}$ is a real number, then we let

1. $t_a : \mathbb{R}^2 \to \mathbb{R}^2, t_a : x \mapsto x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$ denote translation by a;
2. $\rho_\theta(x) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ denote the rotation by θ radians about the origin;
3. $r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = R \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$ denote the reflection in the e_1-axis.

Proposition 2.3.3 *The elements* $\{t_a, \rho_\theta, r : 0 \neq a \in \mathbb{R}^2, \theta \in \mathbb{R}\}$ *generate the group of isometries* $\mathrm{Iso}(\mathbb{R}^2)$.

Proof. If $m \in \mathrm{Iso}(\mathbb{R}^2)$, then we know $m = t_a \circ A$ for some $A \in \mathrm{O}_2$. If $\det A = 1$, then A is a rotation by theorem (2.1.7) so that $m = t_a\rho_\theta$ for some θ. If $\det A = -1$, then $\det AR = 1$ so that $AR = \rho_\theta$ for some θ. It follows that $mr = t_aAR = t_a\rho_\theta$. But $r^2 = 1$ so that we have $m = t_a\rho_\theta r$. ∎

We will use these identities to compute in the group $\mathrm{Iso}(\mathbb{R}^2)$. The verification of each of these identities is left to the reader.

$$t_at_b = t_{a+b},\ \rho_\theta\rho_\varphi = \rho_{\theta+\varphi},\ r^2 = 1,$$
$$\rho_\theta t_a = t_{a'}\rho_\theta,\ \text{where } a' = \rho(a),$$
$$rt_a = t_{a'}r,\ \text{where } a' = r(a),$$
$$r\rho_\theta = \rho_{-\theta}r.$$

These identities, along with the following proposition will allow us to easily make computations in the group $\mathrm{Iso}(\mathbb{R}^2)$.

Proposition 2.3.4 *If* $m \in \mathrm{Iso}(\mathbb{R}^2)$, *then the expression* $m = t_a\rho_\theta r^j$, $j = 0$ *or* $j = 1$, *is unique.*

Proof. Suppose that $m = t_a\rho_\theta r^i = t_b\rho_\varphi r^j$. Then since m is either orientation preserving or reversing according to whether $i = 0$ or $i = 1$, we see that $i = j$ and we have $t_a\rho_\theta = t_b\rho_\varphi$. It follows that $t_{a-b} = \rho_{\varphi-\theta}$. But a translation is not a rotation unless both are the identity so that we must have $a = b$ and $\theta = \varphi$. ∎

We can now state and prove the main theorem of this lecture.

Theorem 2.3.5 *If $m \in \mathrm{Iso}(\mathbb{R}^2)$ is an isometry of the plane, then m is the identity, a translation t_a, a rotation about some point, a reflection in a line or a glide reflection.*

Proof. If $m \in \mathrm{Iso}(\mathbb{R}^2)$, then m either preserves orientation or it does not. Suppose that m does preserve orientation, but m is not a translation. We will show that m is a rotation about some point. Write $m = t_a\rho_\theta$ and let l be the line through the origin, perpendicular to the direction of a (see Figure 2.8). If we place a sector with angle θ so that l bisects the sector as shown, then the fixed point P is determined by placing the vector a in the sector as shown.

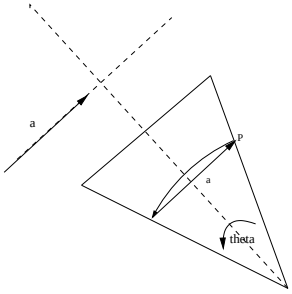


Figure 2.8: Since $m = t_a\rho_\theta$, this diagram shows that the point $\rho_\theta(P)$ will be translated to P under t_a and hence is fixed by m.

Now, a rigid motion that fixes a point is an orthogonal operator and, since m preserves orientation, it must be a rotation by theorem (2.1.7). Therefore we have shown that if m is an orientation preserving motion, then m is a translation or a rotation (we consider the identity as a rotation through zero radians).

Now suppose that m is orientation reversing so that $m = t_a\rho_\theta r$. First, we note that the product $\rho_\theta r = r'$ is a reflection in the line through the origin at an angle of $\theta/2$ with the positive e_1-axis (see Figure 2.9).

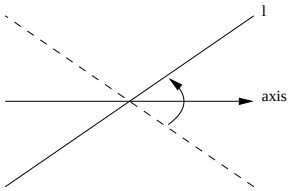


Figure 2.9: In this diagram, the line l is taken onto the dotted line under the reflection r. The rotation ρ_θ then maps $r(l)$ back to l.

Now, if we change basis so that this new line is the line spanned by the first basis vector, then the reflection r' has has the same matrix as r with respect to this basis. Now, t_a is still a translation in this new coordinate system (the coordinates of a have changed, but since we have not used any notation for the old coordinates, we will denote the new ones by $a = (a_1, a_2)^t$). Therefore, in the new coordinate system we have $m = t_a r$ and for any $x = (x_1, x_2)^t$, we have

$$m(x) = \begin{bmatrix} x_1 + a_1 \\ -x_2 + a_2 \end{bmatrix}.$$

Now, the reader should verify that the line $x_2 = (1/2)a_2$ is invariant under m. Moreover, if we restrict m to this line we see that the restriction is the translation $(x_1, (1/2)a_2)^t \mapsto (x_1 + a_1, (1/2)a_2)^t$ so that m is a glide reflection. ∎

In the remainder of this lecture, we want to investigate two important subgroups of $\mathrm{Iso}(\mathbb{R}^2)$. Let T denote the subgroup consisting of all translations and let O denote the subgroup of isometries that fix the origin. If we choose a basis for $\mathbb{R}^2$, then each element of O determines a matrix in $\mathrm{O}_2(\mathbb{R})$ by theorem (2.1.5). This correspondence is an isomorphism $O \xrightarrow{\sim} \mathrm{O}_2$ and we use this isomorphism to identify O_2 with the subgroup O. Also, if we let T denote the subgroup of $\mathrm{Iso}(\mathbb{R}^2)$ consisting of all translations, then the map $\mathbb{R}^2 \to T$ given by $a \mapsto t_a$ is an isomorphism since, as we have seen, $t_{a+b} = t_a + t_b$. The subgroups O and T are called the subgroups of **orthogonal operators** and **translations** respectively. We leave it as an exercise for the reader to show that of P is any point in the plane, the stabilizer of P under the action of $\mathrm{Iso}(\mathbb{R}^2)$ is isomorphic to O_2. It is no accident that the stabilizer of any point is isomorphic to the subgroup of orthogonal operators O. In particular, we have the following proposition.

Proposition 2.3.6 *If $P \in \mathbb{R}^2$ is any point in the plane and O' is the stabilizer of P, then $O' = t_p O t_P^{-1}$. That is, the stabilizer of the origin is conjugate to the stabilizer of P for all $P \in \mathbb{R}^2$.*

Proof. Let ρ_θ be a rotation about the origin through the angle θ and note that $\rho'_\theta = t_P \rho_\theta t_P^{-1}$ is an orientation preserving motion that fixes the point P. Therefore theorem (2.3.5) implies that ρ'_θ is a rotation about P. Similarly we see that $r' = t_P r t_P^{-1}$ is a reflection in the line through P, parallel to the "x-axis". Since every element of O_2 has the form ρ_θ or $\rho_\theta r$, we see that $t_P O t_P^{-1} \subset O'$. However, theorem (2.1.5) implies that every element of O' is an orthogonal operator (with the origin at P) so that every element of O' has the form ρ'_θ or $\rho'_\theta r'$ and hence $t_P O t_P^{-1} = O'$. ∎

We leave the proof of the next proposition to the reader.

Proposition 2.3.7 *The map* $\mathrm{Iso}(\mathbb{R}^2) \to O$ *defined by* $t_a\rho_\theta r^j \mapsto \rho_\theta r^j$, $j = 0, 1$, *is a homomorphism with kernel* T. ∎

It follows immediately from this proposition that T is a normal subgroup of $\mathrm{Iso}(\mathbb{R}^2)$ - it is a kernel! Moreover, since every element $m \in \mathrm{Iso}(\mathbb{R}^2)$ can be written in the form $m = t_a\rho_\theta r^j$, $j = 0, 1$, we see that $\mathrm{Iso}(\mathbb{R}^2) = TO$. Finally, note that $T \cap O = \{1_{\mathbb{R}^2}\}$. We leave the reader with a question: is $\mathrm{Iso}(\mathbb{R}^2) \cong T \times O$?

2.4 Finite subgroups of $\mathrm{Iso}(\mathbb{R}^2)$

The purpose of this lecture is to investigate the possible symmetries of bounded figures in the plane $\mathbb{R}^2$ such as those shown previously in Figure 2.1 or Figure 2.3. A bounded figure can not have any translational symmetry (why?), and hence the symmetry groups of such figures may be finite. We therefore begin our investigation with a look at the possible finite subgroups of the isometry group $\mathrm{Iso}(\mathbb{R}^2)$. We will achieve total success! That is, we will completely classify all finite subgroups of $\mathrm{Iso}(\mathbb{R}^2)$ up to isomorphism. It turns out that the following theorem is the key that unlocks all information about finite subgroups of isometries of the plane. The proof given here (and in Artin) is a beautiful example of the interaction between algebra and geometry. To prove the theorem, we will need a lemma about the centroid of a finite set of points in the plane. If $S = \{s_1, \ldots, s_n\} \subset \mathbb{R}^2$, then the **centroid of** S is the point

$$p = \frac{1}{n}(s_1 + s_2 + \cdots + s_n)$$

where the sum is vector addition in $\mathbb{R}^2$. We will need the following lemma.

Lemma 2.4.1 *If* $S = \{s_1, \ldots, s_n\} \subset \mathbb{R}^2$ *and* $m \in \mathrm{Iso}(\mathbb{R}^2)$ *is an isometry, then* $m(p)$ *is the centroid of the set* $m(S) = \{m(s_1), \ldots, m(s_n)\}$. *That is, an isometry takes a centroid to a centroid.*

Proof. Since every isometry m is a product $t_a\rho_\theta r^j$, $j = 0, 1$, it suffices to show the lemma for these generators. For t_a, the centroid of $t_a(S)$ is

$$\frac{1}{n}((s_1 + a) + (s_2 + a) + \cdots + (s_n + a)) = \frac{1}{n}(s_1 + s_2 + \cdots + s_n) + a = p + a = t_a(p).$$

If m is a rotation or reflection, then m is a linear operator so that we can compute the centroid of $m(S)$ as

$$\frac{1}{n}(m(s_1) + m(s_2) + \cdots + m(s_n)) = m\left(\frac{1}{n}(s_1 + s_2 + \cdots + s_n)\right) = m(p).$$

■

Theorem 2.4.2 *If G is a finite subgroup of* $\mathrm{Iso}(\mathbb{R}^2)$*, then there exists a point $P \in \mathbb{R}^2$ such that $g(p) = p$ for all $g \in G$. That is, G has a fixed point.*

Proof. Let $s \in \mathbb{R}^2$ be any point in the plane and let $\mathcal{O}_s$ denote the orbit of s under the action of G. For notation, let

$$\mathcal{O}_s = \{s_1, s_2, \ldots, s_n\}$$

with say $s_1 = s$. Note that this orbit is also a G-set. That is, if $s_j \in \mathcal{O}_s$ and $g \in G$, then $g(s_j) \in \mathcal{O}_s$. In fact, each $g \in G$ is a permutation of $\mathcal{O}_s$. If p is the centroid of $\mathcal{O}_s$, then the lemma shows that $g(p)$ is the centroid of $g(\mathcal{O}_s)$ for all $g \in G$. But g is a permutation of $\mathcal{O}_s$ so that $g(\mathcal{O}_s) = \mathcal{O}_s$ for all $g \in G$. It follows that $g(p) = p$ for all $g \in G$ and hence p is a fixed point. ■

Corollary 2.4.3 *If G is a subgroup if* $\mathrm{Iso}(\mathbb{R}^2)$ *and G contains a non-zero translation, then G is infinite.* ■

Corollary 2.4.4 *If G is a subgroup if* $\mathrm{Iso}(\mathbb{R}^2)$ *and G contains rotations about two distinct points, then G is infinite.* ■

Since every finite subgroup G of $\mathrm{Iso}(\mathbb{R}^2)$ fixes a point, theorem (2.1.5) implies that G is a subgroup of orthogonal operators. If we change coordinates, we may assume without loss of generality that G is a subgroup of the orthogonal group O_2. We therefore turn our attention to finding all finite subgroups of the orthogonal group O_2. The following theorem is the complete classification we are after.

Theorem 2.4.5 *If G is a finite subgroup of* O_2*, then G is isomorphic to a cyclic group $\mathbb{Z}_n$ for some n or G is isomorphic to a dihedral group D_n for some n.*

Proof. We consider two cases. First, suppose that G contains only rotations. Since G is finite, there is a smallest $0 < \theta$ such that $\rho_\theta \in G$. We claim $\langle \rho_\theta \rangle = G$. If $\rho_\varphi \in G$, with $0 < \varphi$, then there is an integer $m \geq 1$ with $m\theta \leq \varphi$ and $m\theta + \beta = \varphi$ with $0 \leq \beta < \theta$. Now, $\rho_\varphi, \rho_\theta \in G$ implies that $\rho_\beta = \rho_{\varphi - \theta} \in G$ and hence $\beta = 0$ since $\beta < \theta$. It follows that $\rho_\varphi = \rho_\theta^m$ and our claim is established. Therefore, if G contains only rotations, $G = \langle \rho_\theta \rangle$ is cyclic and hence G is isomorphic to $\mathbb{Z}_n$ for some n.

In the second case, G contains a reflection r'. By changing coordinates, we may assume that $r' = r$ is a reflection in the x axis. By the first part of the proof, the subgroup of rotations in G is cyclic of order n, and is generated by an element ρ_θ, where θ is the smallest positive angle of any rotation in G. Clearly the subgroup $\langle \rho_\theta, r \rangle$ of G is isomorphic to D_n with the isomorphism $x \mapsto \rho_\theta$ and $y \mapsto r$, and this subgroup contains all of the rotations. If $g \in G$ is not a rotation, then $g = \rho_\varphi r$ for some φ. Therefore $gr = \rho_\varphi \in G$ so that $\rho_\varphi = \rho_{m\theta}$ for some m. It follows that $g \in \langle \rho_\theta, r \rangle$ and hence $G = \langle \rho_\theta, r \rangle$. Therefore G is isomorphic to D_n. ∎

2.5 Discrete subgroups of $\mathrm{Iso}(\mathbb{R}^2)$

In the previous lecture, we were able to completely classify all finite subgroups of $\mathrm{Iso}(\mathbb{R}^2)$. Namely, we saw that any such group is isomorphic to either a finite cyclic group $\mathbb{Z}_n$ or a dihedral group D_n. In the current lecture, we wish to extend our classification of subgroups of $\mathrm{Iso}(\mathbb{R}^2)$ to a class that includes the symmetry groups of unbounded figures like Figures 2.2 and 2.5. Geometrically, we want to classify doubly infinite patterns in the plane, or "wall paper patterns". In turns out, that to be successful, we must restrict our attention to subgroups that do not contain arbitrarily small translations or rotations. Certain figures in the plane such as straight lines and circles admit translations and rotations respectively through arbitrarily small lengths. If we forbid our patterns from containing such figures, then we can completely classify the corresponding symmetry groups. Here is the formal definition.

Definition 2.5.1 (Discrete subgroup) *A subgroup G of the isometry group $\mathrm{Iso}(\mathbb{R}^2)$ is called* **discrete** *if there exists a positive number $\epsilon > 0$ such that*

1. *For every non-zero vector a such that $t_a \in G$, $|a| \geq \epsilon$.*
2. *For every non-zero θ such that G contains a rotation through θ about some point, then $|\theta| \geq \epsilon$.*

This definition is just the mathematically precise way of saying that a discrete subgroup G does not contain arbitrarily small translations or rotations.

The key to classifying discrete subgroups of $\mathrm{Iso}(\mathbb{R}^2)$ is to look at translation group T and the orthogonal group $O \cong \mathrm{O}_2$. Recall that the translation group T is the subgroup of $\mathrm{Iso}(\mathbb{R}^2)$ of all translations and, if we choose coordinates for $\mathbb{R}^2$, the map $a \mapsto t_a$ is an isomorphism $\mathbb{R}^2 \to T$. Also recall that the map $\mathrm{Iso}(\mathbb{R}^2) \to O$ given by $t_a \rho_\theta r^j \mapsto \rho_\theta r^j$ is a homomorphism onto O with kernel

T. If G is a discrete subgroup of $\mathrm{Iso}(\mathbb{R}^2)$, then we will use T and O to define two *very important* subgroups as follows:

First, we define the **translation group** to be the subgroup of $\mathbb{R}^2$ given by

$$L_G = \{a \in \mathbb{R}^2 : t_a \in G\}.$$

Note that the isomorphism $T \to \mathbb{R}^2$ maps $T \cap G$ onto L_G. We leave it as an exercise for the reader to show that any subgroup of a discrete group G is also discrete. It follows that $T \cap G$ is discrete and hence the translation group L_G is a discrete subgroup of $\mathbb{R}^2$. We will be able to completely classify such subgroups into three types.

Next, we let $\overline{G}$ denote the image of G under the homomorphism $\mathrm{Iso}(\mathbb{R}^2) \to O$, and we call $\overline{G}$ the **point group**. Here is the key relationship we're after.

Proposition 2.5.2 *If G is a discrete subgroup of* $\mathrm{Iso}(\mathbb{R}^2)$ *with translation group L_G and point group $\overline{G}$, then*

$$\overline{G} \cong G/(T \cap G).$$

Proof. Apply the first isomorphism theorem to the map $G \to O$ (the restriction to G of the map $\mathrm{Iso}(\mathbb{R}^2) \to O$ to G defined above). That is, this map is onto $\overline{G}$ by definition and, since the kernel of $\mathrm{Iso}(\mathbb{R}^2) \to O$ is T, the kernel of the restriction is $T \cap G$. ∎

Now, by virtue of the previous proposition, a discrete subgroup G of $\mathrm{Iso}(\mathbb{R}^2)$ determines a discrete subgroup L_G of $\mathbb{R}^2$ and a discrete subgroup $\overline{G}$ of O. Therefore, if we want to classify discrete subgroups of $\mathrm{Iso}(\mathbb{R}^2)$, then we should begin by classify discrete subgroups of $\mathbb{R}^2$ and O. This is what we will now do. Lets begin with the translations.

Theorem 2.5.3 *If L is a discrete subgroup of $\mathbb{R}^2$, then exactly one of the following three cases holds.*

1. *$L = \{0\}$ is the trivial group.*
2. *$L = \mathbb{Z}a$, $0 \neq a \in \mathbb{R}^2$, and hence L is isomorphic to $\mathbb{Z}$.*
3. *$L = \mathbb{Z}a + \mathbb{Z}b$, $a, b \in \mathbb{R}^2$ are both non-zero and (a, b) is linearly independent, hence L is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.*

Proof. Let L be a discrete subgroup of $\mathbb{R}^2$. The main idea of the proof is to find a minimal (in the sense of length) vector in L in some direction and then consider two cases: L is contained in the

line through this vector or not. By a minimal vector, we mean a vector $a \in L$ such that $|a| \leq |b|$ for all $b \in L$. To establish the existence of such a minimal vector, we will need to borrow a tiny bit of analysis.

First, recall that since L is discrete, there is a real number $\epsilon > 0$ such that $|a| \geq \epsilon$ for all non-zero $a \in L$. Therefore if $a, b \in L$ are distinct, then $a - b \in L$ since L is a subgroup so that $|a - b| \geq \epsilon$. Therefore elements of L are not arbitrarily close to each other. Next, we note that a bounded discrete subset of $\mathbb{R}^2$ ($\mathbb{R}^n$ actually) is finite. To see this, we can break out some heavy analysis and note that since our set is bounded, it is contained in a closed ball B about the origin. Since B is closed and bounded, the Heine-Borel theorem implies that B is compact. Therefore if our discrete subset of B was infinite, it must have a limit point in B. It follows that points in L are arbitrarily close to this limit point, and hence arbitrarily close to each other, contrary to the first statement of this paragraph. Finally, we claim that a discrete subset of $\mathbb{R}^2$ contains a vector a of minimal length. To see this, let $b \in L$ be arbitrary and note that the closed ball B of radius $|b|$ is bounded. Therefore $B \cap L$ is finite and non-empty since $b \in B \cap L$. Now, of the finitely many $b \in B \cap L$, we choose one, say a, of minimal length. Clearly then $|a| \leq |b|$ for all $b \in L$.

We can now proceed with the algebraic portion of the proof. If $L = \{0\}$, we're done. Otherwise there exists a non-zero vector $a \in L$ and the previous paragraph implies we may assume that a has minimal (positive) length. We now consider the two cases.

Suppose that every element of L is on the line spanned by a. Then given $b \in L$, we have $b = \alpha a$ for some real number α. Write $\alpha = n + r$ where $n \in \mathbb{Z}$ and $0 \leq r < 1$. Then we have $b = \alpha a = na + ra$ so that $b - na = ra \in L$. But $|ra| = r|a| < |a|$ so that we must have $r = 0$ and hence $b = na \in \mathbb{Z}a$. It follows that $L \subset \mathbb{Z}a$ and hence $L = \mathbb{Z}a$, and hence $L \cong \mathbb{Z}$.

Now, if every element of L is not on the line through a, then we must have a vector $b \in L$ such that (a, b) is linearly independent. Let (a', b') be an arbitrary linearly independent set with $a', b' \in L$. Choose $a \in L$ on the line through a' so that a has minimal (positive) length and let P' denote the parallelogram with vertices at $0, a, b'$ and $a + b'$ (see figure).

The argument given in case 1 shows that the intersection of the line through a with L is precisely $\mathbb{Z}a$. The parallelogram P' together with its interior is a bounded subset that intersects L and hence there at most finitely many points of L in P'. Of all such points, we choose $b \in P' \cap L$ so that b has the smallest positive distance to the line spanned by a. Let P denote the parallelogram with vertices at $0, a, b$ and $a + b$. We claim that there are no points of L in the interior of P. To see this,

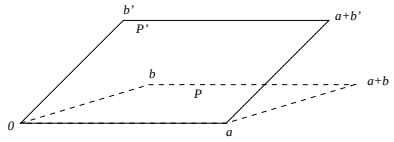


Figure 2.10: If we choose b closest to the line spanned by a, then the parallelogram P will not contain any point of L in its interior.

first note that if $c \in P \cap L$, and c is not a vertex of P, then c must either be on the line segment $[0, a]$ or $[b, a+b]$. Otherwise, the points c and $c-a$ are closer to the line spanned by a than is b, and one of these two points lies in P'. Next, we rule out the segment $[0, a]$ since a is the minimal length element of L on the line spanned by a. Finally, if c were on the segment $[b, a+b]$, then $b-c \in L$ and $b-c$ is on $[0, a]$, a contradiction.

So, in the case that L contains linearly independent vectors (a', b'), we have found independent vectors $a, b \in L$ such that the only elements of L contained in the parallelogram P spanned by a and b are the vertices $0, a, b$ and $a+b$. We claim that $L = \mathbb{Z}a + \mathbb{Z}b$. Clearly $\mathbb{Z}a + \mathbb{Z}b \subset L$ since $a, b \in L$. Now let $v \in L$ be arbitrary. Since a and b are linearly independent, (a, b) is a basis for $\mathbb{R}^2$ and hence there are unique real numbers $\alpha, \beta \in \mathbb{R}$ such that $v = \alpha z + \beta b$. Write $\alpha = n + r$ and $\beta = m + s$ where $n, m \in \mathbb{Z}$ and $0 \leq r, s < 1$. We have

$$v = \alpha a + \beta b = na + mb + ra + sb$$

so that $v - na - mb = ra + sb \in L$. However, $ra + sb \in P$ so that we must have $r = s = 0$ and hence $v = na + mb \in \mathbb{Z}a + \mathbb{Z}b$. It follows that $L = \mathbb{Z}a + \mathbb{Z}b$.

Now, $\mathbb{Z}a$ and $\mathbb{Z}b$ are normal subgroups of L, and since (a, b) is linearly independent, $\mathbb{Z}a \cap \mathbb{Z}b = \{0\}$. It follows that $L \cong \mathbb{Z} \times \mathbb{Z}$ and the proof is complete. ■

To get the idea of why this theorem is useful in our classification, we let G be any discrete subgroup of $\mathrm{Iso}(\mathbb{R}^2)$ and note that this theorem implies that the translation group L_G is isomorphic to one of three groups: 0, $\mathbb{Z}$ or $\mathbb{Z} \times \mathbb{Z}$. Therefore we have at least classified discrete groups into three classes. Usually, an discrete subgroup of isometries is called a **rosette** if $L_G = 0$, a **frieze** if $L_G = \mathbb{Z}$ and a **wall pattern** if $L_G = \mathbb{Z} \times \mathbb{Z}$. That is, if F is some figure in the plane with discrete symmetry, then the symmetry group of F is a rosette if F has no translational symmetry (Figure 2.4 for example), the symmetry group is a frieze if it contains translations, but they are all parallel (Figure 2.2 for example), and it is a wall pattern if it contains translations in all sorts of directions (Figure 2.5

for example). Each of these types of isometry groups can be further classified by looking at the corresponding point group $\overline{G}$.

Since the point group $\overline{G}$ is a subgroup of the group of orthogonal transformations, every element of $\overline{G}$ is either a rotation ρ_θ or a reflection in the x-axis followed by a rotation $\rho_\theta r$. Now, $\rho_\theta \in \overline{G}$ if and only if $t_a\rho_\theta \in G$ for some translation t_a. Recall that the motion $t_a\rho_\theta$ is a rotation through the angle θ (possibly zero) about some point in the plane. Also, $\rho_\theta r \in \overline{G}$ if and only if $t_a\rho_\theta r \in G$ for some translation t_a, and the motion $t_a\rho_\theta r$ is a reflection or a glide reflection. Now, if G is discrete, then it contains no arbitrarily small rotations nor translations so that we see that $\overline{G}$ is discrete as well. We therefore want to classify discrete subgroups of the orthogonal group O. The following proposition states that, in fact, we have already done so!

Proposition 2.5.4 *A discrete subgroup of the group O of orthogonal transformations is finite.*

Proof. Exercise. ∎

If we couple this proposition with the classification of finite subgroups of O given in the last lecture, then we have the following corollary.

Corollary 2.5.5 *If $\overline{G}$ is a discrete subgroup of O, then $\overline{G}$ is isomorphic to a cyclic group $\mathbb{Z}_n$ or a dihedral group D_n for some positive integer n.* ∎

Recall that the goal of this lecture is to classify discrete subgroups of the isometry group $\mathrm{Iso}(\mathbb{R}^2)$. So far, we have seen that each such subgroup has a translation group that is either trivial, isomorphic to $\mathbb{Z}$, or isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Moreover, we know each such group has a point group $\overline{G}$ that is isomorphic to a finite cyclic group or a dihedral group. This is half of the classification we seek in the sense that we know two discrete subgroups are different if they have different translation or point groups. It remains to show how to reconstruct G from L_G and $\overline{G}$. The following theorem is the key to the relationship between the point group $\overline{G}$ and the translation group L_G.

Theorem 2.5.6 *Let G be a discrete subgroup of $\mathrm{Iso}(\mathbb{R}^2)$ with point group $\overline{G}$ and translation group L_G. Then for all $\overline{g} \in \overline{G}$ and all $a \in L_G$, $\overline{g}(a) \in L_G$. That is the point group $\overline{G}$ is a subgroup of the symmetry group of L_G, considered as a subset of the plane $\mathbb{R}^2$.*

Proof. Let $\varphi : G \to \overline{G}$ denote the restriction of the projection $\psi : \mathrm{Iso}(\mathbb{R}^2) \to O$ to G so that $\overline{G} = \varphi(G)$ by definition. Therefore, given $\overline{g} \in \overline{G}$, we may choose $g \in G$ with $\varphi(g) = \overline{g}$. Since $a \in L_G$, we have $t_a \in G$ so that the conjugate $gt_ag^{-1} \in G$. We claim that $gt_ag^{-1} = t_{\overline{g}(a)}$ and hence

$\overline{g}(a) \in L_G$ as desired. To establish our claim, we write $g = t_b\rho_\theta$ or $g = t_b\rho_\theta r$, whatever the case may be, so that $\overline{g} = \rho_\theta$ or $\overline{g} = \rho_\theta r$ respectively. In the first case, we compute

$$gt_a g^{-1} = t_b\rho_\theta t_a \rho_{-\theta} t_{-b} = t_b t_{\rho_\theta(a)} \rho_\theta \rho_{-\theta} t_b = t_{\rho_\theta(a)},$$

and $t_{\rho_\theta(a)} = t_{\overline{g}(a)}$ as desired. Similarly one handles the case $g = t_b\rho_\theta r$. ∎

To illustrate how this theorem further classifies discrete subgroups G, let us consider the case $L_G = \mathbb{Z}$. Here, all translations $t_a \in G$ are parallel, or equivalently, the vectors $a \in L_G$ all lie on a single line. It follows that any rotation in $\overline{G}$ must have order 1 or 2 since it must map this line to itself. Similarly, any lines of reflection must be this line, or perpendicular to it. A careful investigation of the possibilities (which we will not do) shows that there are exactly 7 distinct possible figures with such symmetry groups. That is, there are exactly 7 distinct frieze patterns.

The following theorem gives the possible point groups of discrete subgroups $G \leq \mathrm{Iso}(\mathbb{R}^2)$ when L_G isomorphic to $\mathbb{Z} \times \mathbb{Z}$. It is usually referred to as the **crystallographic restriction** because such subgroups also classify the types of patterns you can find in two dimensional crystal lattices.

Theorem 2.5.7 (Crystallographic restriction) *Let $H \leq O$ be a finite subgroup of symmetries of a lattice L. Then*

1. *Every rotation in H has order $1, 2, 3, 4$ or 6.*
2. *H is isomorphic to a cyclic group $\mathbb{Z}_n$ or a dihedral group D_n where $n = 1, 2, 3, 4$ or 6.*

Proof. We note that (2) follows from (1) because of theorem (2.5.5). Therefore we need only show (1). Let θ be the smallest positive angle of any rotation in H and let $a \in L$ have minimal length. Since H is a group of symmetries of L, we know that $\rho_\theta(a) \in L$, and therefore $b = \rho_\theta(a) - a \in L$ as well since L is a lattice. Now, of course $|b| \geq |a|$ so that we must have $\theta \geq 2\pi/6$ so that all rotations in H have order less than or equal to six. We rule out the case that $\theta = 2\pi/5$ by noting that in this case, the vector $\rho_\theta^2(a) + a \in L$ is shorter than a (draw the picture!) ∎

We are now in a position to completely classify all discrete subgroups of $\mathrm{Iso}(\mathbb{R}^2)$! Given such a group G, we have already classified G as a rosette, frieze or wall pattern according to the point group L_G being trivial, isomorphic to $\mathbb{Z}$, or isomorphic to $\mathbb{Z} \times \mathbb{Z}$ respectively.

If L_G is trivial, then G is isomorphic to the point group $\overline{G}$, and hence G is isomorphic to $\mathbb{Z}_n$ or D_n by proposition (2.5.4). Therefore there are exactly two "types" of rosettes.

If L_G is isomorphic to $\mathbb{Z}$, then we have already remarked that it can be shown that there are exactly 7 possible frieze patterns.

Finally, if L_G is isomorphic to $\mathbb{Z}\times\mathbb{Z}$, then L_G is a lattice and one can show using the crystallographic restriction that there are exactly 17 possible such figures. Therefore there are 17 possible wall patterns.

2.6 Finite subgroups of $\mathrm{SO}_3(\mathbb{R})$

The goal of this lecture is to classify all finite subgroups of the rotation group SO_3 of $\mathbb{R}^3$. Our classification will use the counting formula for the action of SO_3 on a certain subset of the unit sphere S^2. We remind the reader that if $n \geq 0$ is an integer, the **unit n-sphere** or just **n-sphere** is the set

$$S^n = \{x \in \mathbb{R}^{n+1} : |x| = 1\}.$$

In this notation, $S^1 \subset \mathbb{R}^2$ is the unit circle (this agrees with our earlier notation (MAT 150A) for the unit circle group $S^1 \subset \mathbb{C}^\times$), $S^2 \subset \mathbb{R}^3$ is the unit sphere, $S^3 \subset \mathbb{R}^4$ is the 3-sphere (use your imagination!), etc.. Since every element of SO_3 is an isometry (a rotation in fact), it is clear that for all $A \in \mathrm{SO}_3$ and all $x \in S^2$, $Ax \in S^2$ and hence SO_3 acts on the sphere S^2.

Let $G \leq \mathrm{SO}_3$ be a finite subgroup and recall that for each non-identity element $1 \neq g \in G$, g is a rotation about some line l in $\mathbb{R}^3$. It follows that there are exactly two points $p, -p \in S^2$ in $\mathbb{R}^3$ such that $gp = p$ and $g(-p) = -p$. We call p and $-p$ the **poles of** g. We let

$$\mathcal{P} = \{p \in S^2 : gp = p \text{ for some } g \in G,\, g \neq 1\}$$

denote the set of all poles for G.

Lemma 2.6.1 *If $p \in \mathcal{P}$ and $h \in G$, then $hp \in \mathcal{P}$ and hence $\mathcal{P}$ is a G-set.*

Proof. Since $\mathbb{R}^3$ is a G-set under the natural action, the last assertion follows immediately from the first. Now, if $p \in \mathcal{P}$, then there exists an element $g \in G$ with $g \neq 1$ and $gp = p$. Then we note that for any $h \in G$, $hgh^{-1} \in G$ and

$$hgh^{-1}(hp) = hgp = hp.$$

Moreover $g \neq 1$ implies $hgh^{-1} \neq 1$ so that $hp \in \mathcal{P}$ as desired. ∎

We can now state an prove our main theorem. For notation, we let T denote the (orientation preserving) symmetry group of a regular tetrahedron centered at the origin, O denote the (orientation preserving) symmetry group of a regular octahedron centered at the origin, I denote the (orientation preserving) symmetry group of a regular icosahedron centered at the origin. If we have time, we will come back and show that $T \cong A_4$, $O \cong S_4$ and $I \cong A_5$. For now, we will assume this. Here is the classification we are after.

Theorem 2.6.2 *If G is a non-trivial finite subgroup of the rotation group SO_3, then exactly one of the following holds:*

1. *G is isomorphic to a cyclic group $\mathbb{Z}_n$ for some $n \geq 2$.*
2. *G is isomorphic to a dihedral group D_n for some $n \geq 1$.*
3. *G is isomorphic to A_4.*
4. *G is isomorphic to S_4.*
5. *G is isomorphic to A_5.*

Proof. For notation, we let $N = |G|$ so that $N > 1$ and we continue to let $\mathcal{P}$ denote the set of all poles of G. We note that for each $p \in \mathcal{P}$, the stabilizer G_p is a finite group of rotations about the line through p and $-p$ so that G_p is cyclic and hence isomorphic to $\mathbb{Z}_{r_p}$. We note that $r_p > 1$ since p is a pole. If we let $n_p = |\mathcal{O}_p|$ denote the size of the orbit containing p, then for all $p \in \mathcal{P}$, the counting formula implies we have

$$r_p n_p = N.$$

Now, for every $p \in \mathcal{P}$, there are exactly $r_p - 1$ non-identity elements g of G such that $gp = p$. Moreover, for each $g \neq 1$, there are exactly two poles $p \in \mathcal{P}$. Therefore we have the fundamental formula

$$\sum_{p \in \mathcal{P}} (r_p - 1) = 2N - 2.$$

If we note that $\mathcal{O}_p = \mathcal{O}_{p'}$ implies $r_p = r_{p'}$, then we can collect the terms with the same orbit above and we have

$$\sum_i n_{p_i}(r_{p_i} - 1) = 2N - 2$$

where the sum is over the distinct orbits $\mathcal{O}_{p_i}$. Now, $n_{p_i} r_{p_i} = N$ for all i so that dividing both sides of this equation by N gives

$$\sum_i \left(1 - \frac{1}{r_{p_i}}\right) = 2 - \frac{2}{N}. \tag{2.1}$$

Now, the right hand side of this formula is clearly less than 2. However, since $r_{p_i} > 1$ for all i, each term of the sum on the left is at least one half. It follows that there are at most three terms and hence at most 3 orbits of G under the action on $\mathcal{P}$. We examine the cases of 1, 2 or 3 orbits separately.

Case 1. One orbit. In this case, the formula (2.1) becomes

$$1 - \frac{1}{r_{p_1}} = 2 - \frac{2}{N}.$$

But this is impossible since $1 - \frac{1}{r_{p_1}} < 1$ whereas $2 - \frac{2}{N} \geq 1$.

Case 2. Two orbits. In this case, the formula (2.1) becomes

$$\frac{1}{r_{p_1}} + \frac{1}{r_{p_2}} = \frac{2}{N}.$$

Now, $r_{p_i} \leq N$ since $r_{p_i} | N$ so that we must have $r_{p_1} = r_{p_2} = N$. It follows that $n_{p_1} = n_{p_2} = 1$ so that there are two orbits, each with on point. Each of these points is fixed by every element in G and it is clear that G is a group of rotations through the line through these poles. Since G is finite, G is cyclic and hence isomorphic to $\mathbb{Z}_N$ and $N \geq 2$.

Case 3. Three orbits. In this case, the formula (2.1) becomes

$$\left(\frac{1}{r_{p_1}} + \frac{1}{r_{p_2}} + \frac{1}{r_{p_3}}\right) - 1 = \frac{2}{N}.$$

We assume that $r_{p_1} \leq r_{p_2} \leq r_{p_3}$ and note that it is not possible that $r_{p_i} \geq 3$ for all i because $2/N > 0$. Therefore $r_{p_1} = 2$. We again consider two cases.

Case 3.1 $r_{p_2} = 2$. It then follows that $2r_{p_3} = N$ and hence $n_{p_3} = 2$. Therefore there are three orbits: $\mathcal{O}_{p_1}$ and $\mathcal{O}_{p_2}$ have $N/2$ elements, each of which is stabilized by exactly 1 non-identity element of G, and $\mathcal{O}_{p_3} = \{p_3, -p_3\}$ has 2 elements, which are opposite one another on the sphere. Every element of G either fixes both of these elements, or interchanges them. If $g \in G$ interchanges them, then g is a rotation through π radians in a line l' in the plane orthogonal to the line l through p_3 and $-p_3$. The other poles all lie in this plane. One orbit, say $\mathcal{O}_{p_1}$ form the vertices of a regular $(N/2)$-gon and the other orbit lies over the midpoints of the edges of this polygon. In this case, G is isomorphic to the dihedral group D_r where $r = r_{p_3}$.

Case 3.2 $r_{p_2} \geq 3$. We note that $r_{p_2} \geq 4$ and $r_{p_3} \geq 4$ is impossible since $(1/2 + 1/4 + 1/4) - 1 = 0$ and $2/N > 0$. Similarly, $(1/2 + 1/3 + 1/6) - 1 = 0$ shows that $r_{p_2} = 3$ and $r_{p_3} \geq 6$ is impossible. The remaining possibilities are then

3.2.1 $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 3)$.

3.2.2 $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 4)$.

3.2.3 $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 5)$.

3.2.1 Note that $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 3)$ implies that $N = 12$ and hence $(n_{p_1}, n_{p_2}, n_{p_3}) = (6, 4, 4)$. Now, let p be one of the four poles in the orbit $\mathcal{O}_{p_3}$, and let $q \in \mathcal{O}_{p_2}$ be nearest to p. Since the stabilizer G_{p_3} has order 3, the images of q under G_{p_3} give three equally spaced nearest neighbors to p. These points form an equilateral triangle and, together, these four triangles assemble into a regular tetrahedron. The poles in $\mathcal{O}_{p_1}$ lie above the midpoints of the six edges of this tetrahedron, the poles in $\mathcal{O}_{p_2}$ lie above the four vertices of this tetrahedron, and the poles in $\mathcal{O}_{p_3}$ lie above the four centers of the faces of this tetrahedron. It follows that each element of G is a rotation fixing this tetrahedron and hence $G = T$ since $|G| = 12$.

3.2.2 Note that $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 4)$ implies that $N = 24$ and hence $(n_{p_1}, n_{p_2}, n_{p_3}) = (12, 8, 6)$. Now, let p be one of the six poles in the orbit $\mathcal{O}_{p_3}$, and let $q \in \mathcal{O}_{p_2}$ be nearest to p. Since the stabilizer G_{p_3} has order 4, the images of q under G_{p_3} give four equally spaced nearest neighbors to p. These points form the vertices of a square and, together, these six squares assemble into a cube. The poles in $\mathcal{O}_{p_1}$ lie above the midpoints of the 12 edges of this cube, the poles in $\mathcal{O}_{p_2}$ lie above the 8 vertices of this cube, and the poles in $\mathcal{O}_{p_3}$ lie above the 6 centers of the faces of this cube. It follows that each element of G is a rotation fixing this cube and hence $G = O$ since $|G| = 24$.

3.2.3 Note that $(r_{p_1}, r_{p_2}, r_{p_3}) = (2, 3, 5)$ implies that $N = 60$ and hence $(n_{p_1}, n_{p_2}, n_{p_3}) = (30, 20, 12)$. Now, let p be one of the 12 poles in the orbit $\mathcal{O}_{p_3}$, and let $q \in \mathcal{O}_{p_2}$ be nearest to p. Since the stabilizer G_{p_3} has order 5, the images of q under G_{p_3} give 5 equally spaced nearest neighbors to p. These points form the vertices of a regular pentagon and, together, these 12 pentagons assemble into a regular dodecahedron. The poles in $\mathcal{O}_{p_1}$ lie above the midpoints of the 30 edges of this dodecahedron, the poles in $\mathcal{O}_{p_2}$ lie above the 20 vertices of this dodecahedron, and the poles in $\mathcal{O}_{p_3}$ lie above the 12 centers of the faces of this dodecahedron. It follows that each element of G is a rotation fixing this dodecahedron and hence $G = I$ since $|G| = 60$. ■

Chapter 3

Linear Groups

3.1 The classical linear groups

If $\mathbb{F}$ is a field, the general linear group $\mathrm{GL}_n(\mathbb{F})$ and its subgroups are arguably among the most important groups in all of mathematics. We have just seen the the rotation groups of $\mathbb{R}^2$ and $\mathbb{R}^3$ are SO_2 and SO_3 respectively. We saw that the orthogonal group O_n is isomorphic to the group of isometries fixing the origin. The purpose of this lecture is to pose a question about the "shape" of a linear group as well as describe three important subgroups from a group action point of view.
First, the "shape" of a group? From now on, we specialize to the case $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$. Since an element $A \in \mathrm{GL}_n(\mathbb{F})$ is an $n \times n$ matrix, we can think of A as an element of $\mathbb{F}^{n^2}$. Therefore if G is a subgroup of $\mathrm{GL}_n(\mathbb{F})$, G is a subset of $\mathbb{F}^{n^2}$ and hence we can ask what this subset looks like. This is what we mean by the shape of the group.

Example 3.1.1 *If $G = \mathrm{GL}_1(\mathbb{C})$, then G is the "punctured complex plane", that is the complex plane minus the origin.*

Example 3.1.2 *If $G = \mathrm{U}_1(\mathbb{C})$, then $G = \{z \in \mathbb{C} : z\overline{z} = 1\} = S^1$ is a circle.*

In the next two lectures, we will discover the shape of the special unitary group $\mathrm{SU}_2(\mathbb{C})$ and the rotation group $\mathrm{SO}_3(\mathbb{R})$.
We end this lecture with a definition of the **classical linear groups** that uses group actions. Let $G = \mathrm{GL}_n(\mathbb{R})$ and let

$$S = M_n(\mathbb{R}) = \{A : A \text{ is an } n \times n \text{ matrix over } \mathbb{R}\}$$

be the set of all $n \times n$ matrices over $\mathbb{R}$. We leave the proof of the following proposition to the reader.

Proposition 3.1.3 *The operation $G \times S \to S$ defined by $(P, A) \mapsto (P^t)^{-1}AP^{-1}$ is an action of G on S and hence S is a G-set.* ∎

Example 3.1.4 *The stabilizer of the identity matrix I_n under the action $(P, A) \mapsto (P^t)^{-1}AP^{-1}$ is the orthogonal group $O_n(\mathbb{R})$.*

Example 3.1.5 *If $n = 2m$ is even, the stabilizer of the matrix*

$$J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$$

is called the **symplectic group** $\mathrm{SP}_{2m}(\mathbb{R})$.

Recall that if A is a complex matrix, then $A^* = (\overline{A})^t$, where $\overline{A}$ means take the complex conjugate of each entry in A. Here is another proposition for the reader.

Proposition 3.1.6 *If $G = \mathrm{GL}_n(\mathbb{C})$ and S is the set of all $n \times n$ matrices over $\mathbb{C}$, then the operation $G \times S \to S$ defined by $(P, A) \mapsto (P^*)^{-1}AP^{-1}$ is an action of G on S and hence S is a G-set.* ∎

Example 3.1.7 *The stabilizer of the identity matrix I_n under the action $(P, A) \mapsto (P^*)^{-1}AP^{-1}$ is the unitary group $U_n(\mathbb{C})$.*

For the orthogonal group $O_n(\mathbb{R})$ and the unitary group $U_n(\mathbb{C})$, we have the subgroups consisting of those elements with determinant 1. We call these subgroups **special** so that

$$\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{O}_n(\mathbb{R}) : \det A = 1\}$$

is the **special orthogonal group** and

$$\mathrm{SU}_n(\mathbb{C}) = \{A \in \mathrm{U}_n(\mathbb{C}) : \det A = 1\}$$

is the **special unitary group**.

Although it is far from obvious from the definition, each element of the symplectic group $\mathrm{SP}_{2m}(\mathbb{R})$ has determinant 1 so that the letter "S" is appropriate here.

3.2 The special unitary group SU_2

The purpose of this lecture is to describe the shape of the special unitary group $\mathrm{SU}_2 = \mathrm{SU}_2(\mathbb{C})$ as well as give algebraic descriptions of certain important subsets of SU_2. This material should be of particular interest to anyone interested in applications of mathematics to physics.

Recall that SU_2 is the group of 2×2 unitary matrices with determinant 1. That is,

$$\mathrm{SU}_2 = \left\{ P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{C}, P^*P = I_2, \det P = 1 \right\}.$$

Note that $P^*P = I_2$ implies that $P^* = P^{-1}$ so that using the familiar formula for the inverse of a 2×2 matrix, we must have

$$\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Therefore we have $d = \overline{a}$ and $c = -\overline{b}$. Moreover, since $\det P = 1$ we have $a\overline{a} + b\overline{b} = 1$. If we put all of this together, we have the following (better) description of SU_2:

$$\mathrm{SU}_2 = \left\{ P = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} : a, b \in \mathbb{C}, a\overline{a} + b\overline{b} = 1 \right\}.$$

Now, if $a, b \in \mathbb{C}$ are two complex numbers, then the pair $(a, b) \in \mathbb{C}^2$. The above description of SU_2 shows that we can identify SU_2 with all pairs $(a, b) \in \mathbb{C}^2$ such that $a\overline{a} + b\overline{b} = 1$. That is, we have shown that each element of SU_2 determines such a pair, and conversely, a pair $(a, b) \in \mathbb{C}^2$ with $a\overline{a} + b\overline{b} = 1$ determines an element of SU_2 as above.

Recalling that the complex dot-product on $\mathbb{C}^2$ is given by

$$(a_1, b_1) \cdot (a_2, b_2) = a_1\overline{a}_2 + b_1\overline{b}_2,$$

we see that $a\overline{a} + b\overline{b} = 1$ iff. the pair $(a, b) \in \mathbb{C}^2$ has length 1.

The following proposition is left as an exercise.

Proposition 3.2.1 *If $a = x_1 + ix_2$ and $b = x_3 + ix_4$, then $a\overline{a} + b\overline{b} = 1$ if and only if*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1,$$

and hence there is a bijective correspondence between elements of SU_2 and the unit 3-sphere S^3. ■

The explicit correspondence given in proposition (3.2.1) is

$$(x_1, x_2, x_3, x_4) \mapsto \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix}. \tag{3.1}$$

Now, this is not an analysis course, but it is worth mentioning that the map (3.1) is continuous, as is its inverse. In analysis, such a mapping is called a **homeomorphism**, and we will refer to the map (3.1) and the **canonical homeomorphism**. One way to interpret proposition (3.2.1) is to say that the 3-sphere S^3 is a group. Maybe this does not surprise the reader since, after all, the 1-sphere S^1 is also a group. There is a very deep theorem in algebraic topology (deep means the known proofs of the theorem involve a substantial amount of sophisticated mathematics) that states that S^1 and S^3 are the **only** spheres that admit the structure of a group! There is no way to impose a group law on the 2-sphere S^2, for example, in such a way that the multiplication is continuous.

We now proceed to describe algebraically the analogs of longitudes and latitudes in S^3. That is, we will give a geometric definition of latitudes and longitudes in S^3 and then use the map (3.1) to describe these sets algebraically in SU_2. The results are very beautiful!

We begin with latitude. If the 2-sphere S^2 is placed in $\mathbb{R}^3$ with the "poles" at $(\pm 1, 0, 0)$, then the lines of latitude are the level curves $x_1 = c$, $-1 < c < 1$. By analogy, we declare the poles of S^3 to be the points $(\pm 1, 0, 0, 0)$ and then "latitudes" are the level surfaces $x_1 = c$, $-1 < c < 1$. Note that for each such c, the latitude at $x_1 = c$ is a 2-sphere, embedded into $\mathbb{R}^4$ by

$$\{(c, x_2, x_3, x_4) : x_2^2 + x_3^2 + x_4^2 = 1 - c^2\}.$$

We ask the question: how do we describe the latitude spheres algebraically in SU_2? First note that the poles $(\pm 1, 0, 0, 0)$ correspond to the matrices I_2 and $-I_2$. Note that $\pm I_2$ are in the center of SU_2 and hence are the only elements of their conjugacy classes. The following theorem states that except for these two elements of SU_2, the remaining conjugacy classes are precisely the latitudes. Our proof will use the trace operator so the the reader may wish to review the important properties of the trace operator before proceeding. We begin with a lemma.

Lemma 3.2.2 *If $P, P' \in \mathrm{SU}_2$, then P and P' have the same eigenvalues if and only if $P' = QPQ^*$ for some $Q \in \mathrm{SU}_2$.*

Proof. We know from linear algebra that if $P' = QPQ^*$, then P and P' have the same eigenvalues. To establish the converse, we note that if $P \in \mathrm{SU}_2$, the characteristic polynomial of P has the form

$$\lambda^2 - (\operatorname{tr} P)\lambda + 1$$

and hence has real coefficients since $\operatorname{tr} P = 2x_1 \in \mathbb{R}$. It follows that the two complex roots of this polynomial, the eigenvalues of P, are complex conjugates $\lambda, \overline{\lambda}$. Since conjugation is a transitive relation, it suffices to show that if $P \in \mathrm{SU}_2$ has eigenvalues λ and $\overline{\lambda}$, then P is conjugate to the matrix

$$\begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix}.$$

Now, there is a theorem from linear algebra called the Spectral Theorem for unitary operators that states that if $P \in \mathrm{SU}_2$, then there is an element $Q \in \mathrm{U}_2$ such that

$$QPQ^* = \begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix} \in \mathrm{SU}_2$$

is diagonal. If $\det Q = 1$, we are done. Otherwise, we let $\delta = \det Q$ and note that $\overline{\delta}\delta = 1$ since $Q \in \mathrm{U}_2$. Now, if $\epsilon \in \mathbb{C}$ is a square root of δ, then $\overline{\epsilon}\epsilon = 1$ and if we let $Q_1 = \overline{\epsilon}Q$, then $Q_1 \in \mathrm{SU}_2$ since $\det Q_1 = \overline{\epsilon}^2\delta = \overline{\delta}\delta = 1$. Moreover $Q_1 P Q_1^*$ is diagonal with diagonal entries λ and $\overline{\lambda}$. This shows P is conjugate to the diagonal matrix with the eigenvalues of P on the diagonal. ∎

If we take another look at the characteristic polynomial of an element $P \in \mathrm{SU}_2$, then we see that its roots, the eigenvalues of P, depend only on the trace of P. This is the key observation in the proof of the following theorem.

Theorem 3.2.3 *The non-trivial conjugacy classes of* SU_2 *correspond with the latitudes in* S^3 *under the canonical homeomorphism. In particular, if* $-1 < c < 1$*, then the elements* $P \in \mathrm{SU}_2$ *that correspond with the elements of the latitude at* c *make up a non-trivial conjugacy class.*

Proof. Let $P \in \mathrm{SU}_2$, so that the characteristic polynomial of P is

$$\lambda^2 - (\operatorname{tr} P)\lambda + 1.$$

Since the leading and constant terms in this polynomial are both constant, we wee that the eigenvalues of P depend only on $\operatorname{tr} P = 2x_1$. Therefore lemma (3.2.2) implies that $P, P' \in \mathrm{SU}_2$ are conjugate if and only if they have the same trace. Now, if $-1 < c < 1$, then (x_1, x_2, x_3, x_4) is in the latitude at c if and only if $x_1 = c$ so that $P \in \mathrm{SU}_2$ corresponds to a point in this latitude if and only if $\operatorname{tr} P = 2c$. Therefore two points of S^3 are in the latitude at c if and only if the corresponding elements of SU_2 have the same trace if and only if they are conjugate. ∎

Now we will turn our attention to the analogs of longitudes. If $(\pm 1, 0, 0)$ are the poles on S^2, then a longitude of S^2 is the intersection of a plane through $(\pm 1, 0, 0)$ and S^2. Note that every point

except the two poles is contained on a unique longitude. By analogy, we define a **longitude** of S^3 to be the intersection of a 2 dimensional subspace of $\mathbb{R}^4$ containing $(\pm 1, 0, 0, 0)$ and S^3. Note that each longitude is the unit circle in the plane the defines it. Moreover, every point $p \in S^3$ except $(\pm 1, 0, 0, 0)$ is on a unique longitude. This follows since if $p \neq (\pm 1, 0, 0, 0)$, then there is a unique 2 dimensional subspace W of $\mathbb{R}^4$ with basis $((1, 0, 0, 0), p)$ and hence $W \cap S^3$ is the unique longitude containing p. The following proposition gives a particularly nice longitude. We leave the proof as an exercise for the reader.

Proposition 3.2.4 *The longitude defined by the plane $x_3 = x_4 = 0$ corresponds to the set*

$$T = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix} : \lambda\overline{\lambda} = 1 \right\}.$$

and hence is a subgroup of SU_2. ∎

Our next step is to show that all other longitudes correspond to the conjugate subgroups of T. As usual, we begin with a lemma.

Lemma 3.2.5 *Let W be the plane defined by $x_3 = x_4 = 0$. If $Q \in \mathrm{SU}_2$, then Q defines a real linear map $L_Q : W \to \mathbb{R}^4$ by the formula*

$$L_Q(w) = Q \begin{bmatrix} w_1 + iw_2 & 0 \\ 0 & w_1 - iw_2 \end{bmatrix} Q^*.$$

Moreover, the image $L_Q(W)$ is 2-dimensional.

Proof. If we let $Q = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix}$, then a direct computation gives

$$Q \begin{bmatrix} w_1 + iw_2 & 0 \\ 0 & w_1 - iw_2 \end{bmatrix} Q^* = \begin{bmatrix} u_1 + iu_2 & u_3 + iu_4 \\ -u_3 + iu_4 & u_1 - iu_2 \end{bmatrix}$$

where

$$a = x_1 + ix_2,\ b = x_3 + ix_4,$$

$$u_1 = w_1,\ u_2 = (x_1^2 + x_2^2 - x_3^2 - x_4^2)w_2,$$

$$u_3 = (x_1x_4 + x_2x_3)w_2,\ u_4 = (x_2x_4 - x_1x_3)w_2.$$

These formulas show that the coordinates of $L_Q(w)$ are real linear combinations of w_1 and w_2 and hence $L_Q : W \to \mathbb{R}^4$ is a linear map. We leave it as an exercise for the reader to show that $\ker L_Q = 0$ so that $\dim_{\mathbb{R}}(L_Q(W)) = 2$. ■

Theorem 3.2.6 *The longitudes of S^3 correspond to the conjugate subgroups QTQ^*, $Q \in \mathrm{SU}_2$.*

Proof. Let $Q \in \mathrm{SU}_2$. Then lemma (3.2.5) shows that the conjugate subgroup QTQ^* corresponds to the the subset $S^3 \cap L_Q(W)$ so that QTQ^* corresponds to a longitude.
Conversely, if $\mathcal{L}$ is a longitude in S^3, then for every $p \in \mathcal{L}$, $p \neq (\pm 1, 0, 0, 0)$, there is a unique 2 dimensional subspace W' of $\mathbb{R}^4$ containing p and $(1, 0, 0, 0)$. Also, if $P \in \mathrm{SU}_2$ corresponds to p, then the proof of lemma (3.2.2) shows that

$$P = Q \begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix} Q^*$$

for some $Q \in \mathrm{SU}_2$ so that $P \in QTQ^*$. However, we know from the first part of this proof that QTQ^* is a longitude and since p belongs to only one longitude, we see that the longitude defined by W' corresponds to QTQ^*. ■

We end this lecture with a remark on the cosets of the subgroup T. Since T is a longitude, T is a circle, and consequently each of the left cosets QT is also a circle. Together, the union of all of these circles partition S^3 so that S^3 is a disjoint union of great circles. This decomposition is called the Hopf fibration and it had (has?) important consequences in algebraic topology.

3.3 The orthogonal representation of SU_2

The goal of this lecture is to introduce the notion of a group representation by means of a very important example. We will also investigate the "shape" of the rotation group SO_3. A rigorous discussion of the shape of this group is best left to a topology class (and I strongly suggest you take one, especially if you are going to go to graduate school in math!), so we will content ourselves with a brief overview of the topological ideas. First, the algebra.
Our goal is to show the existence of a homomorphism $\varphi : \mathrm{SU}_2 \to \mathrm{SO}_3$ with $\ker \varphi = \{\pm I\}$. We will see in the last part of our course that such a map is called a representation of SU_2. In particular, the map we will construct is called the orthogonal representation of SU_2. You can remember this name since $\varphi(A)$ represents $A \in \mathrm{SU}_2$ as an orthogonal motion - a rotation.

Recall that all of the conjugacy classes of SU_2 except $\{\pm I\}$ are 2-spheres. Since SU_2 is a group, it acts on each conjugacy class via conjugation. The main idea in the construction of φ will be to show that each $A \in \mathrm{SU}_2$ acts on these spheres via conjugation as a rotation. We will use the same notation as the previous lecture for elements of SU_2. In particular, we have the correspondence (3.1):

$$(x_1, x_2, x_3, x_4) \mapsto \begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix}. \tag{3.2}$$

We also recall the longitude at $-1 < c < 1$ is the conjugacy class defined by $\operatorname{tr} P = 2c$. Our proof will involve the notion of skew-hermitian matrices. Since we have not seen this class of matrices before, we make a formal definition.

Definition 3.3.1 (Hermitian / skew-hermitian) *A $n \times n$ complex matrix $A \in M_n(\mathbb{C})$ is called* **hermitian** *if $A^* = A$. We say A is* **skew-hermitian** *if $A^* = -A$.*

The proof of the following lemma will be left as an exercise.

Lemma 3.3.2 *The set*

$$V = \{A \in M_2(\mathbb{C}) : A^* = -A, \operatorname{tr} A = 0\}$$

is a vector space over $\mathbb{R}$ under usual matrix addition and the set

$$\mathcal{B} = \left\{ \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$$

is a basis for V, and hence $\dim_{\mathbb{R}}(V) = 3$. ∎

This brings us to our main theorem of this lecture.

Theorem 3.3.3 *There exists a surjective homomorphism $\varphi : \mathrm{SU}_2 \to \mathrm{SO}_3$ with $\ker \varphi = \{\pm I\}$, and hence $\mathrm{SU}_2 / \{\pm I\} \cong \mathrm{SO}_3$.*

Proof. First, we choose the conjugacy class defined by $\operatorname{tr} P = 0$. If we denote this class by $\mathcal{E}$, then we have $A \in \mathcal{E}$ iff. A has the form

$$A = \begin{bmatrix} iy_2 & y_3 + iy_4 \\ -y_3 + iy_4 & -iy_2 \end{bmatrix}$$

where $y_2^2 + y_3^2 + y_4^2 = 1$. (We use the symbol $\mathcal{E}$ since $\mathcal{E}$ corresponds to the latitude with radius 1 so it is the "equator".) Note that the matrix A is skew-hermitian and $\operatorname{tr} A = 0$ so that $A \in V$,

the vector space of all 2×2 skew hermitian matrices. If $\mathcal{B}$ is the basis for V given in the previous lemma, then the coordinate vector of A with respect to $\mathcal{B}$ is $(y_2, y_3, y_4)^t$. Therefore the canonical homeomorphism takes the basis (e_2, e_3, e_4) to the basis $\mathcal{B}$. Moreover, the condition $y_2^2 + y_3^2 + y_4^2 = 1$ implies that the conjugacy class $\mathcal{E}$ corresponds to the unit 2-sphere in V.

Claim 1. The group SU_2 acts on the space V by conjugation.

To see this, we note that if $A \in V$ and $P \in \mathrm{SU}_2$, then $\mathrm{tr}(PAP^*) = \mathrm{tr}(PAP^{-1}) = \mathrm{tr}\, A = 0$ and $(PAP^*)^* = PA^*P^* = -PAP^*$, and hence $PAP^* \in V$. The group action axioms follow immediately since conjugation is an action on the space of all matrices.

Claim 2. Conjugation by a fixed element $P \in \mathrm{SU}_2$ is a linear operator on V.

To see this, we note that if $P \in \mathrm{SU}_2$, $A, B \in V$ and $\alpha \in \mathbb{R}$, then

$$P(\alpha A + B)P^* = P(\alpha A)P^* + PBP^* = \alpha PAP^* + PBP^*.$$

Now, together, these two claims imply that each $P \in \mathrm{SU}_2$ determines a linear map $V \to V$. Let $\varphi(P)$ denote the matrix of this map with respect to the basis $\mathcal{B}$ for V. Therefore $\varphi(P)$ is a 3×3 real matrix for each $P \in \mathrm{SU}_2$. This gives a function $\varphi : \mathrm{SU}_2 \to M_3(\mathbb{R})$.

Claim 3. $\varphi(P) \in \mathrm{GL}_3(\mathbb{R})$ for all $P \in \mathrm{SU}_2$ and the map $\varphi : \mathrm{SU}_2 \to \mathrm{GL}_3(\mathbb{R})$ is a group homomorphism.

To see this, we note that, using the associative law for matrix multiplication, for all $P, Q \in \mathrm{SU}_2$, and all $A \in V$

$$(PQ)A(PQ)^* = P(QAQ^*)P^*.$$

This shows that the product PQ acts as the composition of the action of Q followed by the action of P. Now, since the matrix of a composition is the product of the two matrices, we have $\varphi(PQ) = \varphi(P)\varphi(Q)$ for all $P, Q \in \mathrm{SU}_2$ so that φ preserves multiplication. Now, for all $P \in \mathrm{SU}_2$, we have

$$\varphi(P^{-1})\varphi(P) = \varphi(P^{-1}P) = \varphi(I_2) = I_3$$

since the identity matrix acts as the identity on V. It follows that $\varphi(P)$ is invertible for all $P \in \mathrm{SU}_2$ and hence $\mathrm{im}\, \varphi \subset \mathrm{GL}_3(\mathbb{R})$ and $\varphi : \mathrm{SU}_2 \to \mathrm{GL}_3(\mathbb{R})$ is a homomorphism as claimed.

Claim 4. The matrix $\varphi(P) \in \mathrm{SO}_3(\mathbb{R})$ for all $P \in \mathrm{SU}_2$.

We could prove this claim by explicitly computing the matrix $\varphi(P)$ with respect to the basis $\mathcal{B}$ and verifying that the columns are an orthonormal basis for $\mathbb{R}^3$. This computation is not difficult, but it is tedious. We therefore choose to prove the claim by showing that $\varphi(P)$ preserves dot

product in V. It will then follow that $\varphi(P) \in \mathrm{O}_3(\mathbb{R})$. Then we will tackle the determinant. If $A, A' \in \mathcal{E}$, then we can use the inverse of the canonical homeomorphism to compute the dot product $\langle A, A' \rangle = y_2y_2' + y_3y_3' + y_4y_4'$. We leave it as an exercise for the reader to verify that for all $A, A' \in \mathcal{E}$,

$$\langle A, A' \rangle = -\frac{1}{2}\operatorname{tr}(AA').$$

Now, if $P \in \mathrm{SU}_2$, then for all $A, A' \in V$, we have

$$\langle PAP^*, PA'P^* \rangle = -\frac{1}{2}(PAP^*PA'P^*) = -\frac{1}{2}(AA') = \langle A, A' \rangle.$$

This shows that $\varphi(P)$ preserves the dot product for all $P \in \mathrm{SU}_2$ and hence $\varphi(P) \in \mathrm{O}_3$. To complete the proof of the claim, we note that the composition $\det \circ \varphi : \mathrm{SU}_2 \to \{\pm 1\}$ is continuous, and hence constant. But clearly $\det \varphi(I_2) = 1$ and hence $\det \varphi(P) = 1$ for all $P \in \mathrm{SU}_2$ and hence $\varphi(P) \in \mathrm{SO}_3$ as claimed.

Together, claims 3 and 4 imply that we have a homomorphism $\varphi : \mathrm{SU}_2 \to \mathrm{SO}_3$. It remains to compute $\ker \varphi$ and show that φ is onto SO_3. Note that $P \in \ker \varphi$ if and only if $PAP^* = A$ for all $A \in V$. In particular, $PAP^* = A$ for the three basis vectors in $\mathcal{B}$. This implies that $b = 0$ and $a = \overline{a}$ so that $P = \pm I$ are the only possibilities. Easily both of these elements are in the kernel so that $\ker \varphi = \{\pm I\}$.

To show that φ is surjective, we first take an arbitrary rotation about the e_2 axis. The matrix of this rotation in the standard basis is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}.$$

If we let $a = e^{i\theta/2}$ and $z = y_3 + iy_4$, then a direct computation shows that

$$PAP^* = \begin{bmatrix} a & 0 \\ 0 & \overline{a} \end{bmatrix} \begin{bmatrix} iy_2 & z \\ -\overline{z} & -iy_2 \end{bmatrix} \begin{bmatrix} \overline{a} & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} iy_2 & a^2z \\ -\overline{a}^2\overline{z} & -iy_2 \end{bmatrix}.$$

This computation shows that $\varphi(P)$ fixes the line through e_2 and rotates the plane $e_2 = 0$ by θ. Therefore $\varphi(P)$ is the given rotation matrix and hence the image of φ contains the subgroup H of all rotations about the line through e_2.

Now, the point e_2 corresponds to the matrix $E = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, and since $\mathcal{E}$ is a conjugacy class, given any other $A \in \mathcal{E}$, there is a $Q \in \mathrm{SU}_2$ such that $QEQ^* = A$. If $Y \in V$ is the vector that corresponds

to A, then we have $\varphi(P)e_2 = Y$. The conjugate subgroup $\varphi(Q)H\varphi(Q^*)$ is the subgroup of rotations about the line through Y. If $B \in \mathrm{SO}_3$, then B is a rotation about a line through some Y, so that $B \in \varphi(Q)H\varphi(Q^*)$. Since $H \in \operatorname{im}\varphi$, we have $B \in \operatorname{im}\varphi$ and hence φ is surjective.

The final statement of the theorem follows immediately from the first isomorphism theorem. ■

Chapter 4

Group Representations

4.1 Group representations

In this lecture, we begin our study of the very important notion of a group representation. As we will see, this idea is not completely new to us. Indeed, we have been studying a type of group representation all quarter; namely group actions. For the convenience of the reader, we recall here an important theorem from the very first lecture of the course.

Theorem 4.1.1 *Let G be a group and S be a set. Then S is a G-set if and only if there exists a homomorphism $\rho : G \to A(S)$ where $A(S)$ denotes the permutation group of S.* ∎

One way to describe the content of this theorem is to say that S is a G-set if and only if we can "represent" each element $g \in G$ as a permutation of the set S. The fact that $\rho : G \to A(S)$ is a homomorphism means that the permutation represented by the product gh of two elements of G is simply the composition of the permutations represented by g and h separately. In our next topic of study, group representations, the principal idea is the same, except that we will represent each $g \in G$ as an invertible linear operator on a vector space. Just as with permutations, we will require the product gh of two elements of the group to be represented by the composition of linear operators. This will give rise to a group homomorphism. In the first definition, we will work with matrices instead of linear operators. Here is the main definition.

Definition 4.1.2 (Matrix representation) *Let G be a group and $\mathbb{F}$ a field. A* **matrix repre-**

sentation of G *is a group homomorphism*

$$R : G \to \mathrm{GL}_n(\mathbb{F}).$$

The number $n \geq 1$ *is called the* **dimension** *of the representation. We will denote the matrix* $R(g)$ *by* R_g*.*

Therefore if $R : G \to \mathrm{GL}_n(\mathbb{F})$ is a matrix representation of G, then for each $g \in G$, $R_g \in \mathrm{GL}_n(\mathbb{F})$ is an invertible matrix over $\mathbb{F}$ and $R_g R_h = R_{gh}$ for all $g, h \in G$.

Example 4.1.3 Let $n \geq 1$ and let $G = S_n$ be the symmetric group on n letters. We define $R : S_n \to \mathrm{GL}_n(\mathbb{R})$ by letting R_p denote the permutation matrix defined by $p \in S_n$. That is, R_p is the $n \times n$ matrix over $\mathbb{R}$ whose jth column is the standard basis vector $e_{p(j)}$.

Example 4.1.4 Another rich source of examples of matrix representations can be found among the finite rotation groups. We will illustrate this idea with the rotation group O of the cube. If we place a cube in $\mathbb{R}^3$ with its center at the origin, then the three coordinate axes pass through the midpoints of opposite pairs of faces as shown here.

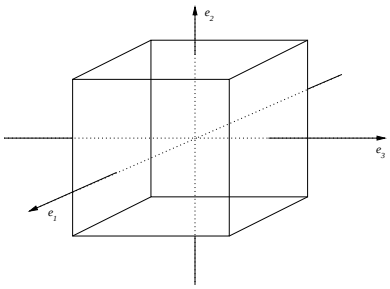


Figure 4.1: If a unit edge length cube is placed with its center at the origin, then the three coordinate axis intersect the cube at the midpoints of the faces.

If we let $x \in O$ denote the rotation through the e_1 axis through $\pi/2$ radians (clockwise when viewed from the positive e_1 axis), then the matrix of x in the standard basis (e_1, e_2, e_3) is

$$R_x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}.$$

If we let y denote the rotation through π radians about the line joining the midpoints of the edges through $(1,-1,1),(1,1,1)$ and $(-1,-1,-1),(-1,1,-1)$, then we have

$$R_y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Similarly, the reader can write down the matrices R_g for all 24 elements $g \in O$.

In both of the previous examples, each element of G gives rise to a unique matrix R_g. In terms of the homomorphism $R : G \to \mathrm{GL}_n(\mathbb{F})$, this means that R is injective, or equivalently, $\ker R = \{e\}$. This does not have to be the case in general. In particular, we make the following formal definition.

Definition 4.1.5 (Faithful) *A matrix representation $R : G \to \mathrm{GL}_n(\mathbb{F})$ is called* **faithful** *if $\ker R = \{e\}$ where $e \in G$ denotes the identity.*

The following proposition is left as an exercise for the reader.

Proposition 4.1.6 *If $R : G \to \mathrm{GL}_n(\mathbb{F})$ is a faithful matrix representation of G, then G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{F})$.* ∎

Now, it turns out that it is much easier to study the notion of a group representation if we do not work with matrices in a given basis. That is, we want to define the notion of representing an element of a group as a linear operator, without choosing a particular basis. To this end, if V is a finite dimensional vector space of a field $\mathbb{F}$, then we let $\mathrm{GL}(V)$ denote the group of all invertible linear operators $T : V \to V$, where of course the group operation is composition of functions. The following proposition gives the relationship between $\mathrm{GL}(V)$ and $\mathrm{GL}_n(\mathbb{F})$ where $n = \dim_{\mathbb{F}}(V)$.

Proposition 4.1.7 *If V is a vector space over $\mathbb{F}$ with $\dim_{\mathbb{F}}(V) = n$, then choosing a basis $\mathcal{B}$ for V gives rise to a group isomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(\mathbb{F})$ that maps $T \in \mathrm{GL}(V)$ to the matrix of T with respect to the basis $\mathcal{B}$.*

Proof. We saw in MAT 150A that every linear map $T : V \to V$ determines a matrix A_T over $\mathbb{F}$. Moreover, the matrix that corresponds to the composition of two operators T and T' is the product of the two matrices. This shows that the map that sends T to its matrix A_T satisfies $A_{T \circ T'} = A_T A_{T'}$. Since each $T \in \mathrm{GL}(V)$ is invertible, we have

$$I_n = A_{1_V} = A_{T \circ T^{-1}} = A_T A_{T^{-1}}$$

so that $A_T \in \mathrm{GL}_n(\mathbb{F})$ for all $T \in \mathrm{GL}(V)$. If $A_T = A_{T'}$, then $T(v_j) = T'(v_j)$ for all basis vectors $v_j \in \mathcal{B}$ and hence $T = T'$. This shows that the map $T \mapsto A_T$ is an injective group homomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(\mathbb{F})$. Finally, if $A \in \mathrm{GL}_n(\mathbb{F})$, then left multiplication by A defines a linear operator $T : V \to V$ and clearly $A_T = A$. ∎

This proposition motivates the following definition.

Definition 4.1.8 (Group representation) *A* **(finite dimensional) representation of a group** *G is a group homomorphism*

$$\rho : G \to \mathrm{GL}(V)$$

where V is a finite dimensional vector space over a field $\mathbb{F}$. If $\dim_{\mathbb{F}}(V) = n$, then n is called the **dimension** *of the representation or the* **degree** *of the representation. As with matrix representations, we will write $\rho_g = \rho(g)$. As with matrix representations, a representation $\rho : G \to \mathrm{GL}(V)$ is called* **faithful** *if $\ker \rho = \{e\}$.*

To test if the above definitions are sinking in, the reader is invited to supply a proof of the following proposition.

Proposition 4.1.9 *If $\rho : G \to \mathrm{GL}(V)$ is an n-dimensional representation of G, and $\mathcal{B}$ is a basis for V, then the map $R : G \to \mathrm{GL}_n(\mathbb{F})$ given by $R_g =$ (the matrix of ρ_g with respect to the basis $\mathcal{B}$) is a matrix representation of G.* ∎

Before we go any further, we want to make a remark about notation an terminology in the representation theory of groups. Strictly speaking, a representation of a group G is a homomorphism $\rho : G \to \mathrm{GL}(V)$ where V is a vector space over $\mathbb{F}$. That is, a representation is a function (a homomorphism). However, if one is only dealing with one representation at a time, it is customary to suppress ρ from the notation altogether and simply refer to the "representation V". Similarly, one can speak of the dimension of V as the dimension of the representation (since they are the same number). So, if you are reading about group representations, do not be surprised if the author (present author included!) refers to the vector space V itself as the representation.

We want to conclude this lecture with a closely related notion of the operation of a group on a vector space. The reader is encouraged to take another look at the "two" notions of group actions developed earlier (the main definition and the homomorphism) before proceeding here.

Definition 4.1.10 *Let G be a group and V a vector space over a field $\mathbb{F}$. We say G* **operates on** *V if there is a map $G \times V \to V$, written $(g, v) \mapsto gv$ that satisfies the following axioms:*

O1. *The mapping $G \times V \to V$ is an action of G on V.*

O2. *$g(v + v') = gv + gv'$ for all $g \in G$ and all $v, v' \in V$.*

O3. *$g(\alpha v) = \alpha(gv)$ for all $g \in G$, $v \in V$ and $\alpha \in \mathbb{F}$.*

The essence of this definition is as follows. A group G operates on a vector space V if V is a G-set in the usual sense **and** each $g \in G$ acts as a linear map $V \to V$. The relationship between a representation of G and an operation of G on V is given in the following theorem.

Theorem 4.1.11 *Let G be a group and V be a vector space over $\mathbb{F}$. Then there exits an representation $\rho : G \to \mathrm{GL}(V)$ if and only if G operates on V.*

Proof. ($\Longrightarrow$) Suppose that $\rho : G \to \mathrm{GL}(V)$ is a representation and define a map $G \times V \to V$ by $(g, v) \mapsto \rho_g(v)$. The axiom **O1** follows immediately since ρ is a homomorphism and $\mathrm{GL}(V)$ is a subgroup of the group $A(V)$ of all permutations of V. Moreover, the axioms **O2** and **O3** follow at once since $\rho_g : V \to V$ is a linear map for all $g \in G$.
($\Longleftarrow$) If G operates on V, then for each $g \in G$, the axioms **O2** and **O3** show that the assignment $v \mapsto gv$ is a linear function $V \to V$. Moreover this function is invertible since the function determined by g^{-1} is obviously an inverse to the function determined by g. This gives a map $\rho : G \to \mathrm{GL}(V)$ defined by $\rho(g)(v) = gv$. Now, the axiom **O1** shows that for all $g, h \in G$ and all $v \in V$, we have

$$\rho(gh)(v) = (gh)(v) = g(hv) = \rho(g)(hv) = \rho(g)(\rho(h)(v)) = \rho(g)\rho(h)(v)$$

so that ρ is a homomorphism. Therefore V is a representation of G. ∎

Although the definition of group representation is valid over any field $\mathbb{F}$, we will primarily focus on the case $\mathbb{F} = \mathbb{C}$. Such representations are called **complex representations**. Similarly, representations over $\mathbb{R}$ are called **real representations**. Note that every real representation can be viewed as a complex representation since $\mathrm{GL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{C})$.

4.2 G-invariant forms and unitary representations

For the rest of the course, we are going to study the problem of decomposing representations of groups into simpler ones. Although all of the definitions that we will give are valid over arbitrary fields, most of our proofs will require special properties of the field of complex numbers $\mathbb{C}$. Therefore, from

now on, we will assume that all representations (abstract and matrix) are complex representations. Therefore, from now on, "vector space" means "complex vector space", and so on.
Now, recall that if $x, y \in \mathbb{C}^n$, then the dot product is the complex number

$$x \cdot y = x_1\overline{y}_1 + \cdots + x_n\overline{y}_n.$$

This dot product is a special case of the following, more general, definition.

Definition 4.2.1 (Hermitian form) *If V is a vector space, then a map $V \times V \to \mathbb{C}$, written $(v, w) \mapsto \langle v, w\rangle$ is a* **hermitian form** *if it satisfies*

1. $\langle v + v', w\rangle = \langle v, w\rangle + \langle v', w\rangle$,
2. $\langle v, w + w'\rangle = \langle v, w\rangle + \langle v, w'\rangle$,
3. $\langle \alpha v, w\rangle = \alpha\langle v, w\rangle$,
4. $\langle v, \alpha w\rangle = \overline{\alpha}\langle v, w\rangle$,
5. $\langle w, v\rangle = \overline{\langle v, w\rangle}$,

for all $v, v', w, w' \in V$ and all $\alpha \in \mathbb{C}$. A hermitian form $\langle \cdot, \cdot \rangle$ is called **positive definite** *if, in addition, we have*

6. $\langle v, v\rangle \geq 0$ *for all $v \in V$ and $\langle v, v\rangle = 0$ iff. $v = 0$.*

Example 4.2.2 *The usual dot product $x \cdot y = \langle x, y\rangle$ is a positive definite hermitian form on $\mathbb{C}^n$.*

Definition 4.2.3 (Hermitian space) *A vector space V together with a positive definite hermitian form $\langle \cdot, \cdot \rangle$ is called a* **hermitian space**. *If V is a hermitian space, then two elements $v, w \in V$ are* **orthogonal** *if $\langle v, w\rangle = 0$. A basis $\mathcal{B} = (v_1, \ldots, v_n)$ for V is* **orthonormal (with respect to $\langle \cdot, \cdot \rangle$)** *if $\langle v_i, v_j\rangle = \delta_{ij}$.*

We will omit the proof of the following theorem. The proof can be found in any elementary linear algebra text.

Theorem 4.2.4 (Gram-Schmidt) *If V is a finite dimensional hermitian space with a positive definite hermitian form $\langle \cdot, \cdot \rangle$, then V has an orthonormal basis with respect to this form.* ∎

Definition 4.2.5 (Unitary operator) *If V is a hermitian space, a linear operator $T : V \to V$ is called* **unitary** *if*

$$\langle T(v), T(w)\rangle = \langle v, w\rangle$$

for all $v, w \in V$.

Here is the relationship between this new usage of the word unitary for operators and the old usage for matrices.

Proposition 4.2.6 *If V is a finite dimensional hermitian space and $\mathcal{B}$ is an orthonormal basis for V, then an operator $T : V \to V$ is unitary if and only if the matrix $[T]_{\mathcal{B}}$ of T with respect to $\mathcal{B}$ is a unitary matrix.*

Proof. Suppose that $\mathcal{B} = (v_1, \ldots, v_n)$ is an orthonormal basis. Then we compute

$$\begin{aligned}
\langle T(v), T(w)\rangle = \langle v, w\rangle \text{ for all } v, w \in V &\iff \langle T(v_i), T(v_j)\rangle = \langle v_i, v_j\rangle \text{ for all } i \\
&\iff T(\mathcal{B}) \text{ is an orthonormal basis} \\
&\iff \text{the columns of } [T]_{\mathcal{B}} \text{ are orthogonal} \\
&\iff ([T]_{\mathcal{B}})^*([T]_{\mathcal{B}}) = I_n.
\end{aligned}$$

■

Definition 4.2.7 (Unitary representation) *If G is a group, a matrix representation $R : G \to \mathrm{GL}_n(\mathbb{C})$ is called* **unitary** *if $R_g \in \mathrm{U}_n(\mathbb{C})$ for all $g \in G$. If V is a hermitian space, a representation $\rho : G \to \mathrm{GL}(V)$ is* **unitary** *if ρ_g is a unitary operator for all $g \in G$. That is, ρ is unitary if*

$$\langle \rho_g(v), \rho_g(w)\rangle = \langle v, w\rangle$$

for all $v, w \in V$ and all $g \in G$.

Corollary 4.2.8 *If V is a hermitian space with orthonormal basis $\mathcal{B}$, then a representation $\rho : G \to \mathrm{GL}(V)$ is unitary iff. the induced matrix representation $\rho_{\mathcal{B}}$ is unitary.*

Proof. Exercise. ■

The goal of this lecture is to show that every representation of a finite group G is conjugate to a unitary representation. That is, given a representation $\rho : G \to \mathrm{GL}(V)$, we can find an orthonormal basis in which $\rho_{\mathcal{B}}$ is unitary. Recall that $\rho : G \to \mathrm{GL}(V)$ is unitary iff.

$$\langle \rho_g(v), \rho_g(w)\rangle = \langle v, w\rangle$$

for all $v, w \in V$ and all $g \in G$. The key to understanding these representations is to view this equality as a condition on the hermitian form rather than as a condition on ρ. Specifically, we make the following definition.

Definition 4.2.9 *If V is a vector space and $\rho : G \to \mathrm{GL}(V)$ is a representation, we say that a hermitian form $\langle \cdot, \cdot \rangle$ on V is G-**invariant** if*

$$\langle \rho_g(v), \rho_g(w) \rangle = \langle v, w \rangle$$

for all $v, w \in V$ and all $g \in G$.

Here is the main theorem of the lecture.

Theorem 4.2.10 *If G is a finite group and $\rho : G \to \mathrm{GL}(V)$ is a representation of G on a hermitian space V, then there exists a G-invariant, positive definite hermitian form $\langle \cdot, \cdot \rangle$ on V.*

Proof. Since V is a hermitian space, there exists a positive definite hermitian form $\{\cdot, \cdot\}$ on V. We definite a form $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ by

$$\langle v, w \rangle = \frac{1}{N} \sum_{g \in G} \{\rho_g(v), \rho_g(w)\}$$

where $N = |G|$ is the order of G. We leave it as an exercise for the reader to show that the map $\langle \cdot, \cdot \rangle$ is a positive definite hermitian form on V. To see that the form is G-invariant, we note for all $v, w \in V$ and all $h \in G$, we have

$$\langle \rho_h(v), \rho_h(w) \rangle = \frac{1}{N} \sum_{g \in G} \{\rho_g(\rho_h(v)), \rho_g(\rho_h(w))\} = \frac{1}{N} \sum_{g \in G} \{\rho_{gh}(v), \rho_{gh}(w)\}.$$

Now, since G is a group, for a fixed $h \in G$, the products gh range over G as g ranges over G. Therefore, rearranging the summation we have

$$\langle \rho_h(v), \rho_h(w) \rangle = \frac{1}{N} \sum_{g \in G} \{\rho_{gh}(v), \rho_{gh}(w)\} = \frac{1}{N} \sum_{g' \in G} \{\rho_{g'}(v), \rho_{g'}(w)\} = \langle v, w \rangle$$

and hence $\langle \cdot, \cdot \rangle$ is G invariant. ∎

Corollary 4.2.11 *If G is a finite group and $R : G \to \mathrm{GL}_n(\mathbb{C})$ is a matrix representation, then there exists a matrix $P \in \mathrm{GL}_n(\mathbb{C})$ such that the conjugate representation $R' : G \to \mathrm{GL}_n(\mathbb{C})$ defined by $R'_g = P R_g P^{-1}$ is unitary.*

Proof. We can think of R as the matrix representation of $\rho : G \to \mathrm{GL}(\mathbb{C}^n)$ in the standard basis. Therefore, theorem (4.2.10) implies that there is a positive definite hermitian form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^n$ that is G-invariant. If $\mathcal{B}$ is an orthonormal basis for this form, then the matrices $R'_g = [\rho_g]_{\mathcal{B}}$ are unitary by proposition (4.2.6). If we let P be the change of basis matrix from the standard basis to $\mathcal{B}$, then $R'_g = PR_gP^{-1}$ for all $g \in G$ and $R'_g \in \mathrm{U}_n$ for all $g \in G$. ∎

Corollary 4.2.12 *Every finite subgroup of* $\mathrm{GL}_n(\mathbb{C})$ *is conjugate to a subgroup of* U_n*.*

Proof. If G is a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$, then the inclusion map $R : G \to \mathrm{GL}_n(\mathbb{C})$ given by $R_g = g$ is a representation of G so that applying the previous corollary to this representation shows there exists an element $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PgP^{-1} \in \mathrm{U}_n(\mathbb{C})$ for all $g \in G$ and hence $PGP^{-1} \leq \mathrm{U}_n(\mathbb{C})$ as desired. ∎

We end this lecture with a discussion on what it means for two representations of a group G to be "the same".

Definition 4.2.13 (Equivalent representations) *Let G be a group and let V and W be vector spaces. Two representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ are called* **equivalent** *or* **isomorphic** *if there is an isomorphism of vectors spaces $T : V \to W$ such that $T(\rho_g(v)) = \rho'_g(T(v))$ for all $g \in G$ and $v \in V$. That is, for every $g \in G$, the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\rho_g} & V \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ W & \xrightarrow[\rho'_g]{} & W \end{array}$$

commutes.

It is a nice exercise to show that equivalence of representations of a group G is an equivalence relation on the set of all representations of G. Therefore to classify all representations of G, for example, we need only classify all possible equivalence classes. We have already made a huge step in that direction for finite groups in this lecture. Namely, the following corollary implies that in order to classify representations of finite groups, we need only classify unitary representations.

Corollary 4.2.14 *If G is a finite group, then every representation $\rho : G \to \mathrm{GL}(V)$ is equivalent to a unitary representation $\rho' : G \to \mathrm{GL}(V)$.*

Proof. Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G and let R be the matrix representation of ρ in some basis $\mathcal{B}$. Corollary (4.2.11) implies that R is conjugate to a unitary matrix representation R'. That is, if $\mathcal{B}'$ is an orthonormal basis for the G-invariant inner product on V, then the change of basis matrix $P \in \mathrm{GL}_n(\mathbb{C})$ from $\mathcal{B}$ to $\mathcal{B}'$ satisfies $R'_g = PR_gP^{-1} \in \mathrm{U}_n(\mathbb{C})$ for all $g \in G$. We define $\rho' : G \to \mathrm{GL}(V)$ by letting $\rho'_g : V \to V$ be the unitary operator defined by R'_g. That is, if $v = \mathcal{B}'x$ (x is the coordinate vector of $v \in V$), then

$$\rho'_g(v) = \mathcal{B}'R'_gx$$

for all $g \in G$. If $T : V \to V$ is defined by mapping $\mathcal{B}$ to $\mathcal{B}'$, then T is an isomorphism. Moreover, if $x \in \mathbb{C}^n$ is the coordinate vector of $v \in V$ with respect to $\mathcal{B}$, then Px is the coordinate vector of $T(v)$ with respect to the basis $\mathcal{B}'$. In hyper-vector notation, we have

$$v = \mathcal{B}x \iff T(v) = \mathcal{B}'Px.$$

Now, if $v \in V$ and $v = \mathcal{B}x$, then for all $g \in G$ we have

$$T(\rho_g(v)) = \mathcal{B}'PR_gx = \mathcal{B}'R'_gPx = (\rho'_g(T(v))$$

and hence we have $T \circ \rho_g = \rho'_g \circ T$ for all $g \in G$. ∎

4.3 Invariant subspaces and irreducibility

Recall that if $T : V \to V$ is a linear operator on a vector space V, a subspace $W \leq V$ is called T-invariant if $T(W) \subset W$. This idea is generalized in the following definition.

Definition 4.3.1 (G-invariant) *If $\rho : G \to \mathrm{GL}(V)$ is a representation, a subspace $W \leq V$ is called* **G-invariant** *if*

$$\rho_g(W) \subset W$$

for all $g \in G$.

In other words, W is a G-invariant subspace if and only if it is ρ_g-invariant for all $g \in G$.

Example 4.3.2 Let $G = D_n$ and let $\rho : D_n \to \mathrm{SO}_3$ be the representation of D_n that maps $g \in D_n$ to the corresponding rotational symmetry of a regular n-gon in the xy-plane. Clearly the plane containing the n-gon is a 2-dimensional invariant subspace since every element of D_n maps this

plane to itself. Similarly, the line through the center of the n-gon perpendicular to this plane is a 1-dimensional invariant subspace.

Example 4.3.3 If O is the orientation preserving symmetry group of the cube, then the representation $\rho : O \to \mathrm{SO}_3$ has no 1 or 2-dimensional invariant subspaces. That is, there is no line or plane through the origin that every element of O maps to itself.

Every representation has invariant subspaces. Indeed, the zero subspace and V are always G-invariant. The representations for which these are the only G-invariant subspaces play a special role in representation theory.

Definition 4.3.4 (Irreducible) *A representation $\rho : G \to \mathrm{GL}(V)$ is called* **irreducible** *if it has no, non-zero proper G-invariant subspaces. Otherwise it is* **reducible**.

Example 4.3.5 The representation of D_n above is reducible. The representation of the rotations of the cube is irreducible.

Proposition 4.3.6 *Suppose that $\rho : G \to V$ is a representation and $V = V_1 \oplus V_2$ where both V_1 and V_2 are G-invariant subspaces. If $\mathcal{B}_i$ is a basis for V_i, and $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$, then the matrices R_g in the matrix representation of ρ with respect to the basis $\mathcal{B}$ of V have the block form*

$$\begin{bmatrix} A_g & 0 \\ 0 & B_g \end{bmatrix}$$

where A_g is the matrix of the restriction ρ_{1g} of ρ_g to V_1 and B_g is the matrix of ρ_{2g} to V_2.

Proof. Exercise. ∎

We usually write $\rho = \rho_1 \oplus \rho_2$ if V is the direct sum of invariant subspaces V_1 and V_2 and ρ_i is the restriction of ρ to V_i. In this case, we say the representation ρ is the **direct sum of the representations** ρ_i.

Example 4.3.7 Let $\rho : D_n \to \mathrm{SO}_3$ be the standard representation of D_n considered above. We choose an orthonormal basis $\mathcal{B} = (v_1, v_2, v_3)$ for $\mathbb{R}^3$ so that v_1 is perpendicular to the plane containing the n-gon and v_2 passes through a vertex so that the matrices of the generators $x, y \in D_n$ in this basis have the form

$$R_x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & c_n & -s_n \\ 0 & s_n & c_n \end{bmatrix}, \qquad R_y = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

where $c_n = \cos(2\pi/n)$ and $s_n = \sin(2\pi/n)$. In this case, the representation $R : D_n \to \mathrm{SO}_3$ is the direct sum $R = A \oplus B$, where $A : D_n \to \mathrm{GL}_1(\mathbb{R})$ is the 1-dimensional matrix representation given by

$$A_x = [1], \qquad A_y = [-1],$$

and $B : D_n \to \mathrm{GL}_2(\mathbb{R})$ is the 2-dimensional representation given by

$$B_x = \begin{bmatrix} c_n & -s_n \\ s_n & c_n \end{bmatrix}, \qquad R_y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

One of the main problems in group representation theory is to determine if a give group representation is irreducible. In general, this problem is difficult. One reason for this difficulty is that even if a representation of G is reducible, the matrices of ρ_g will not necessarily have block form. That is, the chosen basis may not be compatible with the invariant subspace decomposition. Therefore it can be hard to recognize when a representation is reducible by looking at matrices. We will see that we can always find a compatible basis for the case of a unitary representation. Before we can state this fact as a theorem, we need to briefly review some facts about inner product spaces.

Definition 4.3.8 *Let V be a hermitian space with inner product $\langle \cdot, \cdot \rangle$ and let $W \leq V$ be a subspace of V. We define the* **orthogonal complement of** *W as the set*

$$W^\perp = \{v \in V : \langle v, w \rangle = 0 \text{ for all } w \in W\}.$$

Lemma 4.3.9 *If W is a subspace of a hermitian space V, then the orthogonal complement of W is also a subspace of V and $V = W \oplus W^\perp$.*

Proof. We leave the proof that $W^\perp$ is a subspace of V to the reader. To show that $V = W \oplus W^\perp$, it suffices to show that $W \cap W^\perp = \{0\}$ and that $W + W^\perp = V$. First, if $w \in W \cap W^\perp$, then $\langle w, w \rangle = 0$ so that $w = 0$. This show that $W \cap W^\perp = \{0\}$. Now, we let $(w_1, \ldots, w_k)$ be an orthonormal basis for W and extend it to as basis $(w_1, \ldots, w_k, v_{k+1}, \ldots, v_n)$ for V. If we apply the Gram-Schmidt process to this basis, we will not change any vector w_i since $(w_1, \ldots, w_k)$ is already an orthonormal basis. Therefore, an application of Gram-Schmidt to this basis gives an orthonormal basis

$$\mathcal{B} = (w_1, \ldots, w_k, w_{k+1}, \ldots, w_n)$$

for V. Now, given $v \in V$, we write

$$v = \sum_{i=1}^{k} \alpha_i w_i + \sum_{j=1}^{n-k} \alpha_{k+j} w_{k+j} = v' + v''.$$

Clearly $v' \in W$. Moreover, for all $1 \leq i \leq k$, we have

$$\langle w_i, v'' \rangle = \langle w_i, \sum_{j=1}^{n-k} \alpha_{k+j} w_{k+j} \rangle = \sum_{j=1}^{n-k} \alpha_{k+j} \langle w_i, w_{k+j} \rangle = 0$$

since $\langle w_j, w_{k+j} \rangle = 0$ for $j \geq 1$. This shows that $v'' \in W^\perp$ and hence $v = v' + v'' \in W + W^\perp$ and the proof is complete. ∎

For general representations, it is possible that there is an invariant subspace W in V, but that all possible complementary subspaces to W are not invariant. In other words, we may not be able to write ρ as a direct sum of two sub-representations. The following theorem states that this is not the case for unitary representations.

Theorem 4.3.10 *Let $\rho : G \to \mathrm{GL}(V)$ be a unitary representation of a group G into a hermitian space with positive definite hermitian form $\langle \cdot, \cdot \rangle$. If $W \leq V$ is a G-invariant subspace, then the orthogonal complement $W^\perp$ is also G-invariant and hence $V = W \oplus W^\perp$ as representations of G.*

Proof. If $W \leq V$ is a subspace, the previous lemma implies that $V = W \oplus W^\perp$ as vector spaces. Therefore, to prove the theorem, it suffices (by proposition (4.3.6)) to show that $W^\perp$ is also G-invariant. Let $v \in W^\perp$ and let $g \in G$ be arbitrary. We want to show that $\rho_g(v) \in W^\perp$. Let $w \in W$ be arbitrary and note that $\rho_g \rho_{g^{-1}}(w) = w$ for all $g \in G$ and $\rho_{g^{-1}}(w) \in W$ since W is G-invariant. Then, since ρ_g is unitary, we may compute

$$\langle \rho_g(v), w \rangle = \langle \rho_g(v), \rho_g \rho_{g^{-1}}(w) \rangle = \langle v, \rho_{g^{-1}}(w) \rangle = 0$$

where the last equality follows since $v \in W^\perp$ and $\rho_{g^{-1}}(w) \in W$. We have shown that $\langle \rho_g(v), w \rangle = 0$ for all $w \in W$ and hence $\rho_g(v) \in W^\perp$. Since $v \in W^\perp$ and $g \in G$ were arbitrary, this shows that $W^\perp$ is G-invariant. Now, an application of proposition (4.3.6) finishes the proof. ∎

Corollary 4.3.11 *Every unitary representation $\rho : G \to \mathrm{GL}(V)$ is the direct sum of irreducible representations.*

Proof. We proceed by induction on $n = \dim_{\mathbb{C}}(V)$. If $\dim_{\mathbb{C}}(V) = 1$, then V has no proper subspaces at all so that, in particular, V has no G-invariant subspaces and hence V is irreducible. Suppose that $n = \dim_{\mathbb{C}}(V) > 1$ and that all unitary representations of G with dimension less that n can be written as a direct sum of irreducible representations. If G has no proper invariant subspace, then V is irreducible and we are done. Otherwise, there is a proper subspace $W \leq V$ that is G-invariant.

By the previous proposition, $V = W \oplus W^{\perp}$ as representations of G. Now, if W is a proper subspace of V, then $W^{\perp}$ is also a proper subspace so that $\dim_{\mathbb{C}}(W) < n$ and $\dim_{\mathbb{C}}(W^{\perp}) < n$. The induction hypothesis then implies that W and $W^{\perp}$ can be written as a direct sum of irreducible representations. Since $V = W \oplus W^{\perp}$, substituting gives V as a direct sum of irreducible representations. ■

Corollary 4.3.12 (Maschke's Theorem) *Every representation $\rho : G \to \mathrm{GL}(V)$ of a finite group G is the direct sum of irreducible representations.*

Proof. If G is finite, then we may assume that every representation of G is unitary. ■

4.4 Characters

In this final lecture of the course, we will take a brief look at one of the most powerful, and beautiful, tools in representation theory: characters. Although some of our definitions are valid for infinite groups, the theory we want to develop is far more complicated in that case. Therefore, for the rest of this lecture (the rest of the course!), **all groups we consider are finite**.

As Artin points out in his introduction to characters, "The secret to understanding representations is not to write down the matrices explicitly unless absolutely necessary". Indeed, as we will see in the following definition, given a representation, we will ignore virtually everything about the corresponding matrices. We will keep only the trace!

Definition 4.4.1 (Character) *Let G be a (finite) group and let $\rho : G \to \mathrm{GL}(V)$ be a representation of G. We define the* **character of** *ρ to be the complex valued function*

$$\chi : G \to \mathbb{C}$$

defined by

$$\chi(g) = \mathrm{tr}(\rho_g).$$

The **dimension of the character** *χ is defined to be the dimension of the representation ρ. If ρ is an irreducible representation, then we say χ is an* **irreducible character**.

Now is a good time to remind the reader that the number $\mathrm{tr}(\rho_g)$ is defined to be the trace of any matrix of the operator ρ_g. If two matrices represent the same operator with respect to different bases, then they are conjugate and hence have the same trace. Therefore the trace of an operator is well defined. In fact, we have an even stronger statement.

Proposition 4.4.2 *Let $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ be two representations of a group G and let χ is the character of ρ and χ' is a character of ρ'. If ρ is equivalent to ρ', then $\chi = \chi'$.*

Proof. If ρ is equivalent to ρ', then there is an isomorphism $T : V \to W$ such that $\rho_g = T^{-1}\rho'_g T$ for all $g \in G$. It follows that $\operatorname{tr} \rho_g = \operatorname{tr} \rho'_g$ for all $g \in G$ and hence $\chi = \chi'$. ∎

We will see (soon!) that the converse of this proposition is also true. This correspondence between characters and equivalence classes of representations is a powerful tool in studying representations. We will need to know some basic properties of characters, so we'll put some in the following proposition. Before we state it, we note that since characters are complex valued functions, we can add them pointwise. That is $(\chi + \chi')(g) = \chi(g) + \chi'(g)$.

Proposition 4.4.3 *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group G and let χ be the character of ρ. Then,*

1. *$\chi(e)$ is the dimension of χ, where $e \in G$ is the identity.*
2. *$\chi(g) = \chi(hgh^{-1})$ for all $g, h \in G$.*
3. *$\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.*
4. *If ρ' is another representation of G with character χ', then the character of the direct sum representation $\rho \oplus \rho'$ is the sum $\chi + \chi'$.*

Proof. (1) Since $\rho_e = 1_V$, the matrix of ρ_e in any basis is the identity matrix I_n where $n = \dim(V)$. Therefore $\chi(e) = \operatorname{tr} I_n = n = \dim \chi$.
(2) If $g, h \in G$, then $\rho_{hgh^{-1}} = \rho_h \rho_g \rho_h^{-1}$ so that $\operatorname{tr}(\rho_{hgh^{-1}}) = \operatorname{tr}(\rho_g)$. The result follows.
(3) To show this, we note that $\chi(g) = \lambda_1 + \cdots + \lambda_n$ where $\{\lambda_i\}$ is the set of eigenvalues of ρ_g. Now the eigenvalues of $\rho_{g^{-1}} = \rho_g^{-1}$ are the λ_i^{-1}. Since G is a finite group, each ρ_g has finite order and hence the eigenvalues satisfy $\lambda_i^k = 1$ for some k. It follows that $|\lambda_i| = 1$ so that $\lambda_i^{-1} = \overline{\lambda}_i$. Therefore we have

$$\chi(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda}_1 + \cdots + \overline{\lambda}_n = \overline{\chi(g)}.$$

(4) This follows since the trace of the block matrix of $\rho \oplus \rho'$ is the sum of the traces of the blocks. ∎

We want to make two important remarks. First, part (2) of the previous theorem implies that each character χ is constant on the conjugacy classes of G. Therefore to determine all values of χ, we need only determine $\chi(g)$ for a single representative of each conjugacy class of G. Second, since the

trace of ρ_g does not depend on any choice of basis, we may choose a convenient basis for each g to compute $\chi(g)$. Now lets look at an example.

Example 4.4.4 Let $R : D_4 \to \mathrm{SO}_3$ be the standard 3-dimensional representation of the dihedral group D_4 (see the example in the previous lecture), and let χ denote the character of R. Recall that $R = A \oplus B$ where

$$A_x = [1],\ A_y = [-1],\ B_x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ B_y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Recall also that the conjugacy classes of D_4 are

$$C_1 = \{1\},\ C_x = \{x, x^3\},\ C_{x^2} = \{x^2\},\ C_y = \{y, x^2y\},\ C_{xy} = \{xy, x^3y\}.$$

Let χ^A and χ^B denote the characters of the representations A and B respectively so that $\chi = \chi^A + \chi^B$. Now, we compute χ^A on each conjugacy class of D_4:

$$\chi^A(1) = 1,\ \chi^A(x) = 1,\ \chi^A(x^2) = 1,\ \chi^A(y) = -1,\ \chi^A(xy) = -1.$$

If we list the elements of each conjugacy class in some fixed order, then we can list all the values of χ^A as a vector in $\mathbb{C}^8$. Let us use the order $D_4 = \{1, x, x^3, x^2, y, x^2y, xy, x^3y\}$ so that we have

$$\chi^A = (1, 1, 1, 1, -1, -1, -1, -1).$$

Similarly we can compute

$$\chi^B = (2, 0, 0, -2, 0, 0, 0, 0),$$

and therefore

$$\chi = \chi^A + \chi^B = (3, 1, 1, -1, -1, -1, -1, -1).$$

Note that $\chi(1) = 3$ is indeed the dimension of R.

As we saw in the previous example, if χ is the character of a representation $\rho : G \to \mathrm{GL}(V)$, then we can think of χ as a vector in $\mathbb{C}^{|G|}$. We simply list the conjugacy classes in some order, and then list the elements in each class in some order and then if $g \in G$ is in the ith position, we write $\chi(g)$ in the ith coordinate of the vector. It is useful to keep this construction in mind as you read the following definition.

Definition 4.4.5 *Let G be a group of order N and let χ and χ' be the characters of two representations of G. We define a form on the space of characters by defining*

$$\langle \chi, \chi' \rangle = \frac{1}{N} \sum_{g \in G} \chi(g) \overline{\chi'(g)}.$$

We note that if we think if χ as an element of $\mathbb{C}^N$ as described above, then this is just the usual hermitian inner product on $\mathbb{C}^N$, re-normalized by the factor $1/N$. It follows immediately that $\langle \cdot, \cdot \rangle$ is a positive definite hermitian form! The following theorem is one of the most beautiful theorems in the representation theory of finite groups. We will not prove this theorem in this course (it would take approximately 2 weeks of preparation). However, we will understand its statement as well as learn how to use it in classifying representations of finite groups. Here is the statement of the theorem.

Theorem 4.4.6 (Orthogonality relations) *Let G be a group of order N and let $\rho_1, \rho_2, \ldots$ denote representatives from each isomorphism class of the irreducible representations of G. If χ_i is the irreducible character of ρ_i, then*

1. *$\langle \chi_i, \chi_j \rangle = \delta_{ij}$. That is, the irreducible characters are a pairwise orthogonal set of unit vectors with respect to the inner product $\langle \cdot, \cdot \rangle$.*
2. *The number of irreducible representations of G is precisely the number of conjugacy classes of G. We denote this number by r.*
3. *If $d_i = \dim \rho_i$, then d_i divides N and*

$$d_1^2 + \cdots + d_r^2 = N.$$

■

Before we begin with the applications of this theorem, we want to point out that since the characters of the representations of G are functions $G \to \mathbb{C}$ that are constant on the conjugacy classes, they are special examples of the following type a functions called class functions.

Definition 4.4.7 (Class function) *If G is a finite group, a function $f : G \to \mathbb{C}$ is called a* **class function** *if f is constant on each conjugacy class of G.*

Proposition 4.4.8 *Let G be a finite group with r distinct conjugacy classes. The the set $\mathcal{C}(G)$ of all class functions on G is a vector space over $\mathbb{C}$ with $\dim_{\mathbb{C}}(\mathcal{C}(G)) = r$.*

Proof. Since each class function $f \in \mathcal{C}(G)$ is constant on the conjugacy classes of G, f defines a function $\tilde{f} : C_G \to \mathbb{C}$ by $\tilde{f}(C_g) = f(g)$ where C_G denotes the set of conjugacy classes of G. We have already remarked that the set of complex valued functions on a finite set is a vector space over $\mathbb{C}$ under pointwise addition and scalar multiplication so that $\mathcal{C}(G)$ is a complex vector space. We leave it as an exercise for the reader [Artin 9.5.1] to show that $\dim_{\mathbb{C}}(\mathcal{C}(G)) = r$, where $r = |C_G|$ is the number of conjugacy classes in G. ∎

Now, together, this proposition and theorem (4.4.6) give us the following (very important!) corollary.

Corollary 4.4.9 *If G is a finite group, then the form $\langle \cdot, \cdot \rangle$ makes $\mathcal{C}(G)$ into a hermitian space and the irreducible characters $\chi_1, \ldots, \chi_r$ form an orthonormal basis for $\mathcal{C}(G)$.*

Proof. We have already commented that the form $\langle \cdot, \cdot \rangle$ is a positive definite hermitian form since it is a non-zero scalar multiple of the usual hermitian form on $\mathbb{C}^{|G|}$, and therefore $\mathcal{C}(G)$ is a hermitian space. By the previous proposition, we have $\dim_{\mathbb{C}}(\mathcal{C}(G)) = r$. Moreover, by theorem (4.4.6), the irreducible characters χ_i are linearly independent since they are pairwise orthogonal. Since there are r such characters and $\dim_{\mathbb{C}}(\mathcal{C}(G)) = r$, we see that $(\chi_1, \ldots, \chi_r)$ form a basis. Finally, $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ shows that this basis is orthonormal. ∎

Corollary 4.4.10 *If G is a finite group and χ is the character of a representation ρ of G, then there are unique integers $n_i \in \mathbb{Z}$ such that*

$$\chi = n_1\chi_1 + \cdots + n_r\chi_r$$

where $\chi_1, \ldots, \chi_r$ are the irreducible characters of G. Moreover, the integer n_i is precisely the number of times the irreducible representation ρ_i occurs in the direct sum decomposition of ρ.

Proof. Given χ, we know there exist complex numbers $n_1, \ldots, n_r \in \mathbb{C}$ such that $\chi = n_1\chi_1 + \cdots + n_r\chi_r$ since the irreducible characters form a basis $(\chi_1, \ldots, \chi_r)$ for the class functions. In fact, since this basis is orthonormal, we have $n_i = \langle \chi, \chi_i \rangle$ for all i. Now, by Maschke's theorem (4.3.12), we can write ρ as a direct sum

$$\rho = m_1\rho_1 \oplus m_2\rho_2 \oplus \cdots \oplus m_r\rho_r$$

where $m_i \in \mathbb{Z}$ for all i and $m_i\rho_i$ means the direct sum of m_i copies of the representation ρ_i. Now, since the character of a direct sum is the sum of the characters, we have

$$\chi = m_1\chi_1 + m_2\chi_2 + \cdots + m_r\chi_r$$

and hence $n_i = m_i \in \mathbb{Z}$ for all i by uniqueness. Moreover, we see that $\langle \chi, \chi_i \rangle = n_i$ is precisely the number of times the irreducible representation ρ_i occurs in the the direct sum decomposition of ρ. ■

Here is the promised converse to the first proposition of this lecture.

Corollary 4.4.11 *If ρ and ρ' are two representations of a finite group G and the characters χ and χ' of ρ and ρ' respectively satisfy $\chi = \chi'$, then ρ is equivalent to ρ'.*

Proof. Let m_i denote the number of copies of ρ_i in the direct sum decomposition of ρ into irreducibles and let m_i' be defined similarly for ρ'. If $\chi = \chi'$, then $\langle \chi, \chi_i \rangle = \langle \chi', \chi_i \rangle$ for all $i = 1, \ldots, r$ and hence $m_i = m_i'$ for all i. It follows that

$$\rho \sim m_1\rho_1 \oplus \cdots \oplus m_r\rho_r = m_1'\rho_1 \oplus \cdots \oplus m_r'\rho_r \sim \rho'.$$

■

Corollary 4.4.12 *If χ is the character of a representation ρ of a finite group G, then $\langle \chi, \chi \rangle = 1$ if and only if χ is irreducible.*

Proof. We know from theorem (4.4.6) that if χ is irreducible, then $\langle \chi, \chi \rangle = 1$. Conversely, if $\langle \chi, \chi \rangle = 1$, then if we write $\chi = \sum n_i\chi_i$ as in corollary (4.4.10), then we have

$$n_1^2 + \cdots + n_r^2 = 1.$$

Since $n_i \in \mathbb{Z}$ for all i, the only solution to this equation is exactly one $n_i = 1$ and the rest equal to zero. Hence $\chi = \chi_i$ is irreducible. ■

Corollary (4.4.12) is a practical way of checking the irreducibility of a given representation, as the following examples show.

Example 4.4.13 The standard representation $R : D_4 \to \mathrm{SO}_3$ is easily seen to be reducible. We can also see this by computing

$$\langle \chi, \chi \rangle = \frac{1}{8}(9 + 1 + 1 + 1 + 1 + 1 + 1 + 1) = 2.$$

Example 4.4.14 The 2-dimensional representation $B : D_4 \to \mathrm{SO}_2$ is irreducible. To see this, we compute

$$\langle \chi^B, \chi^B \rangle = \frac{1}{8}(4 + 0 + 0 + 4 + 0 + 0 + 0 + 0) = 1.$$

Example 4.4.15 Let us determine the possible dimensions of the irreducible representations of D_4. We know D_4 has 5 conjugacy classes, and therefore D_4 has 5 irreducible representations, $\rho_1, \rho_2, \rho_3, \rho_4$ and ρ_5, by part (2) of theorem (4.4.6). If $d_i = \dim \rho_i$, then part (3) of the same theorem implies that each d_i is a divisor of $|D_4| = 8$ and $\sum d_i^2 = 8$. The only possible solution to this equation is $8 = 1 + 1 + 1 + 1 + 4$ and hence D_4 has four 1-dimensional irreducible representations $\rho_1, \rho_2, \rho_3, \rho_4$ and one 2-dimensional irreducible representation ρ_5. We have seen that $B : D_4 \to \mathrm{SO}_2$ is an irreducible 2-dimensional representation so that it is the matrix representation of ρ_5 in some basis. Every group has the trivial 1-dimensional representation ($\rho_g(\alpha) = \alpha$ for all $\alpha \in \mathbb{C}$) which we will always denote by ρ_1. The matrix representation $A : D_4 \to \{\pm 1\}$ is the matrix representation of the *sign* representation ρ_2. The remaining two 1-dimensional representations ρ_3 and ρ_4 have matrix representations $C_x = -1, C_y = 1$ and $D_x = -1, D_y = -1$ respectively.

Example 4.4.16 As one last example, let's try to find all irreducible representations of the symmetric group S_4. Now, S_4 has five conjugacy classes, and hence five irreducible representations. These five classes are represented by the identity $1 \in S_4$ along with the following four elements:

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \; z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \; x^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

The orders of these conjugacy classes are $|C_1| = 1, |C_y| = 6, |C_z| = 8, |C_{x^2}| = 3$ and $|C_x| = 6$. We will always list the conjugacy classes in the order $1, y, z, x^2, x$ so that the class equation for S_4 is

$$24 = 1 + 6 + 8 + 3 + 6.$$

Now, S_4 has the trivial 1-dimensional representation ρ_1 and the sign permutation ρ_2. We also have the 3-dimensional representation

$$S_4 \xrightarrow{\sim} O \xrightarrow{R} \mathrm{SO}_3$$

which we have claimed to be irreducible (here, O is the rotational symmetry group of the cube). Let's prove this claim by computing the character χ. First, we choose an isomorphism $S_4 \to O$, by placing a cube in $\mathbb{R}^3$ and labeling the four diagonals as shown here.

The permutations $x, y \in S_4$ correspond to the rotations x and y in our previous example (section 1). The permutation z corresponds to the rotation through $2\pi/3$ radians in the diagonal labeled 4

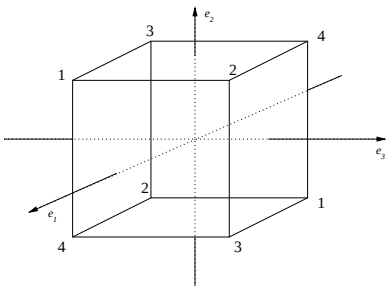


Figure 4.2: If we label the four diagonals as shown, the permutations $x, y \in S_4$ correspond to the rotations x and y in our previous example (section 1).

(CCW viewed from $(1, -1, -1)$). The matrices in the standard basis for $\mathbb{R}^3$ are

$$R_y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \; R_z = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix}$$

$$R_x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \; R_{x^2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Therefore we have

$$\chi(1) = 3, \; \chi(y) = -1 \, \chi(z) = 0, \; \chi(x^2) = -1, \chi(x) = 1.$$

Now, if we remember that the conjugacy classes have $1, 6, 8, 3$ and 6 elements, we can compute

$$\langle \chi, \chi \rangle = \frac{1}{24}(9 + 6 \cdot 1 + 8 \cdot 0 + 3 \cdot 1 + 6 \cdot 1) = 1$$

and hence R is irreducible.

Now, using the the orthogonality relations (4.4.6), we know that $24 = 1 + 1 + d_2^2 + d_3^2 + 9$, where d_2 and d_3 are the dimensions of the remaining two irreducible representations. The only solution to this equation is $d_2 = 2$ and $d_3 = 3$ so that S_4 has another 3-dimensional representation and one irreducible 2-dimensional representation.

To find the other 3-dimensional representation, we consider the 4-dimensional permutation representation $\rho : S_4 \to \mathrm{GL}_4(\mathbb{C})$. Since the inverse of a permutation matrix is its transpose, this representation is unitary. The subspace spanned by the vector $(1, 1, 1, 1)$ is S_4-invariant, and hence so is the perpendicular space V. The restriction $\rho : S_4 \to \mathrm{GL}(V)$ is a three dimensional representation

whose matrices in the basis $((1,-1,0,0),(1,0,-1,0),(1,0,0,-1))$ are

$$R'_y = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ R'_z = \begin{bmatrix} -1 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$R'_x = \begin{bmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ R'_{x^2} = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Now we compute

$$\langle \chi', \chi' \rangle = \frac{1}{24}(9 + 6 \cdot 1 + 8 \cdot 0 + 3 \cdot 1 + 6 \cdot 1) = 1$$

so that R' is irreducible. Moreover $\chi \neq \chi'$ so that R' is a new 3-dimensional irreducible representation. It remains to find the 2-dimensional irreducible representation, but alas, we're out of time!

Index