

## HANDOUT 5

FERNANDO RODRIGUEZ-VILLEGAS

### 1. GROUPS

A *group*  $G$  is a set with an associative binary operation  $\cdot$  (which we will call *product*) satisfying the following properties.

(i) There is an identity element  $1 \in G$  satisfying

$$1 \cdot g = g, \quad g \in G.$$

(ii) For every  $g \in G$  there exists an  $h \in G$  such that

$$g \cdot h = 1.$$

The identity element in (i) is unique. Also, the element  $h$  in (ii) is uniquely determined by  $g$ ; it is called the *inverse* of  $g$  and is denoted by  $g^{-1}$ .

For  $n = 1, 2, \dots$  we define  $g^n$  as the product  $g \cdot \dots \cdot g$  of  $g$  with itself  $n$  times. If  $n$  is a negative integer we define  $g^n = (g^{-1})^{-n}$ . Finally, we define  $g^0 = 1$ .

The following properties are not hard to prove.

- (1)  $g^{-1} \cdot g = 1,$
- (2)  $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$
- (3)  $g^m \cdot g^n = g^{m+n}$
- (4)  $(g^m)^n = g^{mn}$

For a finite group  $G$  we call  $|G|$ , its number of elements, the *order* of  $G$ .

As an example of a group consider the symmetries of a regular  $n$ -gon in the plane. It is not hard to verify that indeed the set of all such isometries forms a group. This group is called the *dihedral group*  $D_n$ . It is of order  $2n$  and consists of  $n$  rotations of angle a multiple of  $2\pi/n$  around the origin and  $n$  reflections about the different axis of symmetry of the polygon.

Two elements  $g, h \in G$  *commute* if  $g \cdot h = h \cdot g$ . If every pair of elements of  $G$  commute we say  $G$  is *commutative* or *abelian*. From now on we simplify the notation and simply write  $gh = g \cdot h$  if the operation in question is clear from the context.

Let  $\tau \in D_n$  be the counterclockwise rotation about the origin of angle  $2\pi/n$  and  $\sigma$  the reflection about a fixed axis of symmetry of the polygon. Note that  $\sigma = \sigma^{-1}$ .

One can check that

$$(5) \quad \sigma\tau\sigma^{-1} = \tau^{-1}.$$

In particular  $D_n$  is *not* abelian for  $n > 2$ . It is not hard to see from (5) that every element of  $D_n$  can be expressed as products of  $\sigma$  and  $\tau$ . We say that  $\sigma$  and  $\tau$  *generate* the group  $D_n$  and write  $D_n = \langle \tau, \sigma \rangle$ . (Another way to say it is that  $D_n$  is the smallest subgroup containing  $\sigma$  and  $\tau$ ; see below for the definition of subgroup.)

The identity (5), moreover, implies that every element of  $D_n$  can be written as

$$\tau^k \sigma^j, \quad k = 0, 1, \dots, n-1, \quad j = 0, 1$$

A subset  $H$  of  $G$  is a *subgroup* if  $H$  together with the binary operation of  $G$  is itself a group. It is easy to check that  $H \subset G$  is a subgroup if and only if

- (i)  $1 \in H$ .
- (ii)  $h \in H$  implies that  $h^{-1} \in H$ .
- (iii)  $h_1, h_2 \in H$  implies that  $h_1 h_2 \in H$ .

For example, the set of rotations of  $D_n$  form a subgroup of  $D_n$ .

The set of all powers  $g^n$  of an element  $g \in G$  is a subgroup of  $G$ ; we call it the subgroup *generated* by  $g$  and denote it  $\langle g \rangle$ .

## 2. PERMUTATIONS AND ORBITS

Let  $X$  be a non-empty set. A *permutation* of  $X$  is a bijection  $\sigma : X \rightarrow X$ . The set  $S_X$  of all permutations of  $X$  is a group for the binary operation given by composition of functions. If  $X = \{1, 2, \dots, n\}$  we write  $S_n$  for short.

A subgroup  $G$  of  $S_X$  *acts* on the set  $X$ . We call  $x, y \in X$  *G-equivalent* if  $y = gx$  for some  $g \in G$ . For example, if  $X$  is the set of vertices of the regular  $n$ -gon and  $G = D_n$  then all elements of  $X$  are  $G$ -equivalent since we may get from one to the other by, for example, rotating by the appropriate angle.

The relation of  $G$ -equivalence is indeed an equivalence relation on  $X$ . The different equivalence classes are called the *orbits* of  $G$ . We denote by  $Gx$  the orbit containing  $x$ .

For example, if  $G$  is the group of rotations of the plane about the origin and  $X$  is the plane then the orbits are the circles centered at the origin.

Given a point  $x \in X$  we let  $G_x$  be the *stabilizer* of  $x$  in  $G$ ; that is,  $G_x$  is the subgroup of all elements in  $G$  that fix  $x$ .

Let  $G \subset S_X$  be a group of permutations of a finite set  $X$ . For each  $g \in G$  define  $F(g)$  to be the number of  $x \in X$  fixed by  $g$ .

We will use the following result, whose proof we omit.

**Theorem 1.** *For any  $x \in X$  we have*

$$|Gx||G_x| = |G|$$

Note in particular that the size of any orbit divides the order of  $G$ .

We can now state and prove the main result we need.

**Theorem 2.** *The number of orbits of  $G$  acting on  $X$  is given by*

$$(6) \quad \frac{1}{|G|} \sum_{g \in G} F(g)$$

*Proof.* In the sum on the right each element  $x \in X$  is counted  $|G_x|$  times. Hence, the elements in the orbit  $Gx$  containing  $x$  are counted  $|G_x||Gx|$  times. By the previous theorem each orbit is therefore counted  $|G|$  times and the identity follows.  $\square$

As an illustration consider again the case of  $G = D_n$  and  $X$  the set of vertices of the regular  $n$ -gon. As we discussed above there is only one orbit in this case. On the other hand,  $F(g)$  has the following values:  $n$  for the identity; 0 for any rotation (other than the identity); 1 for every reflection, if  $n$  is odd; 2 for half of the

reflections (those whose axis goes through two vertices) and 0 for the other half, if  $n$  is even. The formula of theorem 2 checks:  $1 = (n + 1 + \cdots + 1)/2n$  for  $n$  odd and  $1 = (n + 2 + \cdots + 2)/2n$  for  $n$  even.

### 3. COUNTING COLORINGS

How many different necklaces are there made out of  $n$  beads of  $m$  colors? We can use the theorem of the previous section (known as Burnside's lemma) to answer this question.

Abstractly, consider a finite group  $G$  acting on a finite set  $X$ . By a *coloring*  $\lambda$  of  $X$  we mean a function

$$\lambda : X \longrightarrow C$$

from  $X$  to another fixed finite set  $C$  of colors. We say that two colorings are equivalent if we can change one into the other by some element of  $G$ . Our goal is to count the number  $N$  of equivalence classes of colorings.

In order to set this up in the form of the previous section we define an action of  $G$  on the set  $C^X$  of colorings by

$$(g\lambda)(x) := \lambda(g^{-1}x), \quad x \in X.$$

The total number of colorings is  $m^n$ , where  $m = |C|$  and  $n = |X|$ . The number  $N$  we want is the number of orbits of the action of  $G$  on  $C^X$ ; to compute it using Burnside's lemma we need to work out the number  $F(g)$  of fixed colorings for every  $g \in G$ .

A coloring  $\lambda \in C^X$  is fixed by  $g \in G$  if and only if

$$\lambda(x) = \lambda(g^{-1}x), \quad x \in X.$$

From this it follows that we must have  $\lambda(x) = \lambda(gx) = \lambda(g^2x) = \cdots$  and conversely. In other words, a coloring  $\lambda$  is fixed by  $g$  if and only if  $\lambda$  is constant on the orbits of  $\langle g \rangle$  acting on  $X$ . Let  $l(g)$  denote the number of such orbits. Then the number  $F(g)$  of colorings fixed by  $g$  is  $m^{l(g)}$ .

By Burnside's lemma we have

$$(7) \quad N = \frac{1}{|G|} \sum_{g \in G} m^{l(g)}.$$

Notice two remarkable things about this formula. First, if we know the value of  $l(g)$  for every  $g$  we obtain in one swoop an expression for the number of colorings for every  $m$ . Second, this expression gives the number of different colorings a *polynomial function* of the number of colors  $m$ .

We are reduced to computing the values of  $l(g)$ . If  $g \in G$  is given as a product of disjoint cycles (viewed as a permutation of  $X$ ) with  $l_1$  cycles of length 1,  $l_2$  cycles of length 2, etc. then

$$l(g) = \sum_{k=1}^n l_k;$$

indeed, the cycles in the cycle decomposition of  $g$  are precisely the orbits of  $\langle g \rangle$  acting on  $X$ .

Let us count how many different necklaces there are made out of  $n = 6$  and  $m = 2$  colors. The group of symmetries of the necklace is  $G = D_6$  of order 12. Place the beads on the vertices of a regular hexagon in the plane and label the

them counterclockwise as  $1, 2, \dots, 6$ . The elements of  $G$  as permutations of the vertices and the corresponding value of  $l(g)$  are given in the following table

$g$	cycle decomp.	$l(g)$
1		6
$\tau$	(123456)	1
$\tau^2$	(135)(246)	2
$\tau^3$	(14)(25)(36)	3
$\tau^4$	(153)(264)	2
$\tau^5$	(165432)	1
$\sigma_1$	(26)(35)	4
$\sigma_2$	(12)(36)(45)	3
$\sigma_3$	(13)(46)	4
$\sigma_4$	(23)(14)(56)	3
$\sigma_5$	(24)(15)	4
$\sigma_6$	(16)(25)(34)	3

where  $\sigma_i$  are the reflections about the different axis of symmetry (starting with the axis going through the vertices labeled 1 and 4 going counterclockwise) and  $\tau$  is the counterclockwise rotation of angle  $2\pi/6$ .

Using the table we easily compute the terms in (7) for this example and get

$$N = \frac{1}{12}(m^6 + 3m^4 + 4m^3 + 2m^2 + 2m).$$

The number of necklaces with 6 beads and  $m = 1, 2, 3, \dots$  colors is then  $1, 13, 92, \dots$

### Homework (Due Tue April 8)

- (1) Explain why identity (5) above is valid.
- (2) Make a table like the one above for the action of  $D_5$  as permutation of the vertices of a regular pentagon in the plane.
- (3) Compute the polynomial in  $m$  giving the number of different necklaces with 5 beads and  $m$  colors.
- (4) How many different necklaces are there with 5 beads and 2 colors? Compute this number from the expression of the previous problem and verify it by drawing all the necklaces.
- (5) Find the polynomial in  $m$  giving the different ways of coloring the faces of a regular tetrahedron with  $m$  colors.
- (6) How many different ways can you the faces of a regular tetrahedron with 3 colors? Compute this number from the expression of the previous problem and verify it by drawing all the cases.