

Permutation Groups
 Barry Dayton
 Northeastern Illinois University
 www.neiu.edu/ bhd Dayton
 June, 2002

Here is an elementary exposition of permutation groups making use of arrow diagrams to simplify matters. An explicit exposition of Lagrange's Theorem in the case of a group acting on a set leads directly to an elementary exposition and proof of Burnside's theorem. The prerequisites are simply a basic familiarity with the idea of a *group* with perhaps an acquaintance of the symmetry groups C_n, D_n and the modular arithmetic groups Z_n . These notes were written for my Modern Algebra for Elementary School Teachers course, Summer 2002.

1 Permutation Groups

A *rearrangement* of a set is a 1-1 correspondence from a set X to itself. In algebra, especially if the set is finite, these are called *permutations*. A little care must be used to distinguish our use of permutations with that in combinatorics, but, as you will see the concepts are quite related. Since the exact names of the members of the elements of X are unimportant, when X is finite we will usually assume that $X = \{1, 2, 3, \dots, n\}$ for some positive integer n . And, except as noted below, we will assume X is finite. We will use the notation $n(X) = n$ to denote the cardinality of this set.

The easiest way to denote a permutation is to give its function table and/or its *static* arrow diagram. For example when $n = 5$ we might have:

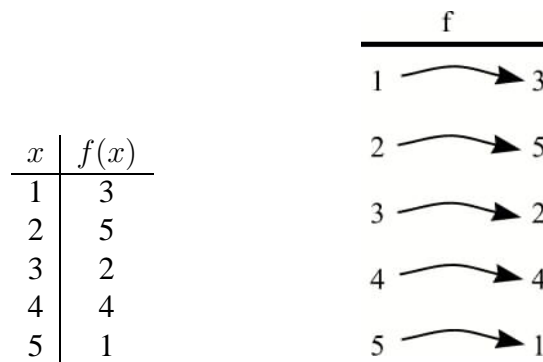


Figure 1: Static Arrow Diagram

To combine permutations we view them as functions and compose them. That is given permutations f, g then gf is the permutation given by $gf(x) = g(f(x))$. The easiest way to do this is with tables:

x	$f(x)$
1	3
2	5
3	2
4	4
5	1

x	$g(x)$
1	4
2	2
3	1
4	5
5	3

The trick is to draw the static arrow diagrams and, rearranging, place them next to each other so that the middle columns match up, then ignore the middle columns.

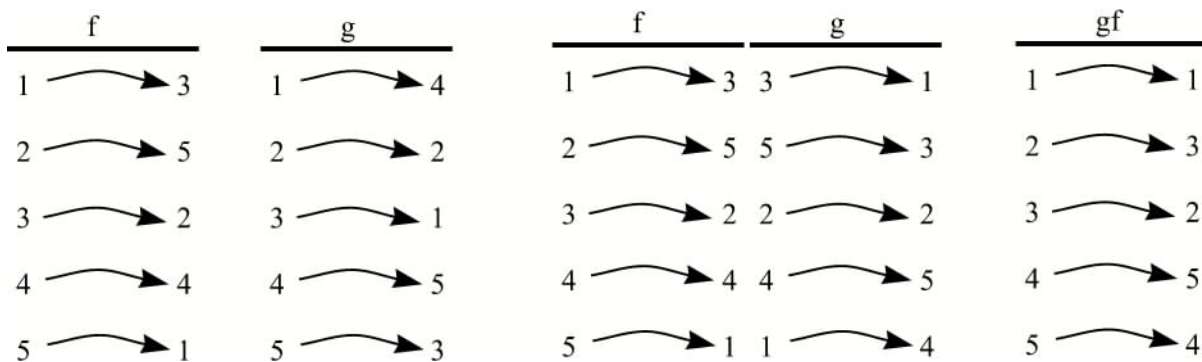


Figure 2: Composition of Permutations

Note that when we write gf it means that we do f first and g after. The order is important since combining permutations is not commutative in general.

Clearly composition is associative and the do-nothing function $\iota(x) = x$ is a unity. To find the inverse, just reverse the arrows:

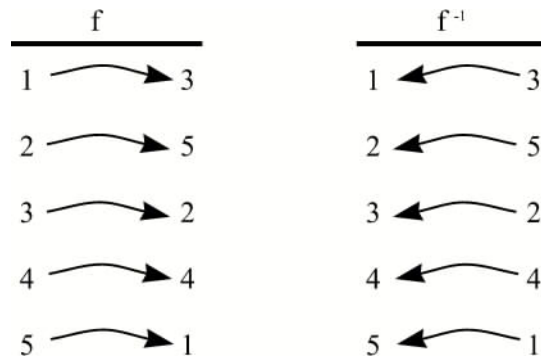


Figure 3: Inverse Permutation

Thus the set of permutations of $X = \{1, 2, 3, \dots, n\}$ is a group. This group is generally denoted by S_n and called the *symmetric group on n elements*. The right hand column of a table representation

for a permutation is a permutation (re-arrangement) of the numbers $1, 2, \dots, n$ and each such re-arrangement gives a different permutation. So by elementary combinatorics we see there are $n!$ permutations of the set of n -elements.

2 Dynamic Representation and Cycle Decomposition

It is useful to represent permutations by their *dynamic* arrow diagrams. Since the domain and range of these functions are the same we can list each element only once, with an arrow pointing towards the image of the element under the permutation. The definition of function requires that exactly one arrow leaves each element, but the fact that we actually have a 1-1 correspondence requires that there is exactly one arrow into each element. This requires that the diagram breaks into loops or *cycles*.

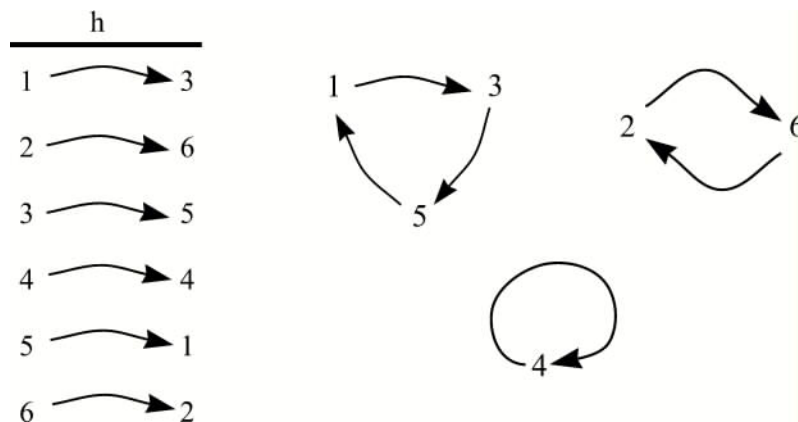


Figure 4: Static and Dynamic Arrow Diagrams

In this picture the diagram breaks into 3 cycles, one containing 1,3,5 another with 2,6 and the element 4 is alone in its own cycle since $h(4) = 4$. (4 is called a *fixed point*.) In general the dynamic arrow diagram is not convenient for composing permutations but in the special case we are composing a permutation with itself it is very useful: for h^2 go two steps around each cycle, for h^3 three steps, etc.

If we calculate powers of h of Figure 4 we get:

x	$h(x)$	x	$h^2(x)$	x	$h^3(x)$	x	$h^4(x)$	x	$h^5(x)$	x	$h^6(x)$
1	3	1	5	1	1	1	3	1	5	1	1
2	6	2	2	2	6	2	2	2	6	2	2
3	5	3	1	3	3	3	5	3	1	3	3
4	4	4	4	4	4	4	4	4	4	4	4
5	1	5	3	5	5	5	1	5	3	5	5
6	2	6	6	6	2	6	6	6	2	6	6

What we see is that if the length of a cycle divides an integer k then every element in that cycle remains fixed under h^k . So in particular since the length of every cycle of h divides 6 then every element is fixed under h^6 so, as seen by the table, $h^6 = \iota$ the do-nothing.

This works in general and we have the theorem:

Theorem 1 Let m be the least common multiple of the lengths of all cycles of the permutation $f \neq \iota$. Then $f^m = \iota$ but $f^k \neq \iota$ for $1 \leq k < m$.

We call the number m above the *order* of the permutation f .

Exercise 1 Consider the permutations f, g of Figure 2. Find the dynamic arrow diagrams and the orders of f, f^2, f^3, g, gf, fg and gfg^{-1} .

For the permutation in Figure 4 we see that the different cycles work separately. Thus, as in Figure 5 below, we can write h as a product of *cyclic* permutations, permutations with only one non-trivial (length bigger than one) cycle. In the literature it is common to denote a cyclic permutation by a symbol such as $(1\ 3\ 5)$ which denotes the cyclic permutation taking 1 to 3, 3 to 5 and 5 back to 1.

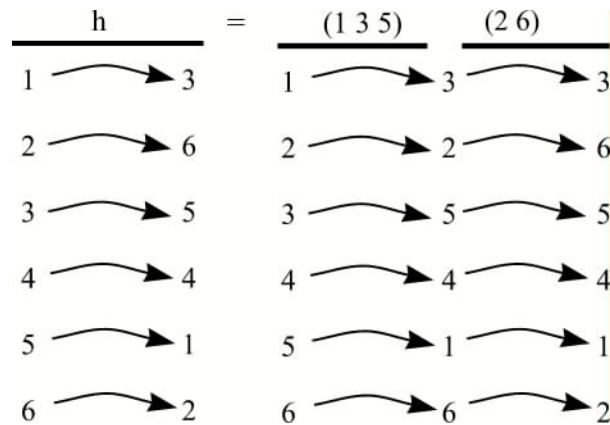


Figure 5: Product of Disjoint Cycles

In general, every permutation is, in this way, a product of disjoint cycles. Here the order in which we multiply does not matter since the cycles act on different elements of the set X . In texts on permutation groups you may see h represented by $(1\ 3\ 5)(2\ 6)$.

3 Groups acting on Sets

We can observe that many of our familiar groups remind us of permutation groups. For example since a symmetry of the square must take the vertices to vertices, each symmetry can be thought of as a permutation of the vertices. In this way D_4 is isomorphic to a subgroup of S_4

More generally we say the group G acts on the set X if each element $g \in G$ can be represented by a permutation $g(x)$ of X in such a way that

- (i) For $g, h \in G$ the combination gh is represented by the composition $g(h(x))$
- (ii) The unity in G is represented by ι , the do-nothing.

We do not require here that different elements g, h of G are represented by different permutations $g(x), h(x)$, however if this does happen then G is isomorphic to a subgroup of the group of permutations on X .

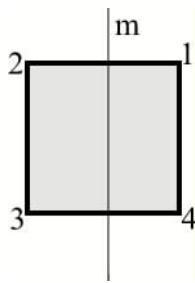


Figure 6: The Square

Consider again the symmetry group D_4 of the square (Figure 6). We represent r by the cycle $(1\ 2\ 3\ 4)$ and m as the product of cycles $(1\ 2)(3\ 4)$. Then a typical element of D_4 is of the form $r^j m^k$ where $j = 0, 1, 2$ or 3 and $k = 0$ or 1 . Then $r^j m^k$ should go to $(1\ 2\ 3\ 4)^j (1\ 2)^k (3\ 4)^k$. The reader should generate the multiplication table for these permutations herself and check the the resulting subgroup of S_4 is, in fact, isomorphic to D_4 .

Given a group G we can define for each $a \in G$ a function $a(x)$ from G to itself by $a(x) = ax$ for all x , where ax is multiplication in the group. The existence of inverses in the group implies that this function has an inverse function and therefore must be a permutation of G . Laws (i) and (ii) hold so G is acting on itself, here $X = G$. Finally cancellation again says different elements of G act differently so we have shown:

Cayley's Theorem Every group is isomorphic to a subgroup of a permutation group.

In the special case of a finite group G Cayley's theorem says that G is isomorphic to a subgroup of S_n where $n = n(G)$. Unfortunately for group theorists this does not help much in understanding finite groups. But in a sense, the symmetric groups are the most general groups.

Let G act on X . We say an element $a \in X$ is a fixed point, or an *invariant* for group element f if $f(w) = w$. For a given set element w the set of all invariant group elements f with w as an invariant is called the *isotropy subgroup*, in symbols $I(w) = \{f \in G | f(w) = w\}$. On the other hand the *orbit of w* is the set of all set elements which are images of w under some permutation in G , in symbols $\text{orb}(w) = \{x \in X | f(w) = x \text{ for some } f \in G\}$. The French mathematician Lagrange noticed in some specific examples that there was a very striking relationship between the sizes of these sets and $n(G)$. Lets look at an example.

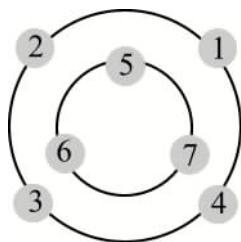


Figure 7: Orbits

We let G be the subgroup of S_7 consisting of the cycle $R = (1\ 2\ 3\ 4)$, the cycle $r = (5\ 6\ 7)$ and all powers and products of those permutations. You might discover, if you had the patience to work out the multiplication table, that this group is determined by the relations $R^4 = \iota, r^3 = \iota$ and the commutative relation $Rr = rR$. G has 12 elements. (It is also true that G is isomorphic to Z_{12} , can you show this?) Now lets see where the 12 elements of G take 1:

$$\begin{array}{cccc} \iota(1) = 1 & R(1) = 2 & R^2(1) = 3 & R^3(1) = 4 \\ r(1) = 1 & Rr(1) = 2 & R^2r(1) = 3 & R^3r(1) = 4 \\ r^2(1) = 1 & Rr^2(1) = 2 & R^2r^2(1) = 3 & R^3r^2(1) = 4 \end{array}$$

What do you see in this table? First, we note from the first column that the isotropy group $I(1) = \{\iota, r, r^2\}$ and from the first row that the orbit of 1 is $\{1, 2, 3, 4\}$. Next we note that since powers of r leave 1 fixed if we multiply some group element by a power of r on the right then the location that 1 is sent to does not change. So, for example $R\iota, Rr$ and Rr^2 all send 1 to 2 and a similar observation holds for the last two columns. Thus, since $n(I(1)) = 3$ there are exactly 3 permutations taking 1 to each of the members of its orbit. This partitions the group G into $4 = n(\text{orb}(1))$ sets of $3 = n(I(1))$. (The sets of 3 are called *cosets*.) So, besides giving another proof that $12 = 4 * 3$, we see that in this example that

$$n(G) = n(I(1)) * n(\text{orb}(1))$$

This is a special case of

Lagrange's Theorem for permutation groups Let G be a finite group acting on a set X . Then for every $x \in X$

$$n(G) = n(I(x)) * n(\text{orb}(x))$$

The proof in general is similar to the example, if y is in the orbit of x with $f(x) = y$ then the full set of elements of G sending x to y is $\{fg | g \in I(x)\}$ which is a set of cardinality $n(I(x))$. There is one of these sets for each element of the orbit and every member of G is in exactly one of these, depending on which element of the orbit it sends x to. The conclusion follows.

The important thing about this theorem is its generalization, due to C. Jordan, to all groups. However, here is a simple application to a familiar problem in combinatorics.

Example How many different, mostly nonsense, words can you get by re-arranging the letters in "Mississippi"? We can let the group S_{11} act on the set of all 11 letter words by re-arranging the letters in the same way the permutation re-arranges the numbers $1, 2, \dots, 11$. For instance, if the permutation f is given in cycle notation by $(1\ 11)(2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$ then "Mississippi" is re-arranged to "iissipssipM". What we are looking for is the orbit of "Mississippi" under this group action. We need only calculate the isotropy group. For example the two p's must either remain where they are or switch places so any permutation fixing Mississippi will have neither 9 nor 10 in any of its cycles, alternatively the trivial cycles $(9)(10)$ or will have the cycle $(9\ 10)$. Likewise to keep the s's in the same place positions 3,4,6,7 must be permuted among them selves, there are $4!$ ways to do this. And there are $4!$ ways to permute the "i" places 2,5,8 and 11. The M must stay where it is. From this it is not too hard to see that the isotropy group of "Mississippi" has $2! * 4! * 4!$ elements. Thus the size of the "Mississippi" orbit is

$$n(\text{orb}(\text{Mississippi})) = \frac{n(G)}{n(I(\text{Mississippi}))} = \frac{11!}{2! * 4! * 4!} = 34650$$

4 Burnside's Theorem

In combinatorics direct applications of Lagrange's theorem can generally be replaced by direct arguments as in the usual solution of the example above. But a very non-trivial application of group theory to combinatorics comes from Burnside's theorem which follows fairly easily from Lagrange's theorem.

In these applications it is the number of orbits that we wish to calculate. Suppose again the finite group G acts on the now finite set X . We first note from Lagrange's Theorem that if we know the size of the orbit we can calculate the size of the isotropy group:

$$n(I(x)) = \frac{n(G)}{n(\text{orb}(x))}$$

But then this is the same for every x in the orbit. But using the simple fact that multiplication is repeated addition we can rephrase Lagrange's theorem as

$$n(G) = \sum_x n(I(x))$$

where the sum is taken over all x in the given orbit. Using the fact that each element of X is in exactly one orbit, if we add up the sizes of all isotropy groups for all $x \in X$ we get

$$kn(G) = \sum_x n(I(x))$$

where k is the number of different orbits.

We pause to look at the example of Figure 7. We have

$$I(1) + I(2) + I(3) + I(4) + I(5) + I(6) + I(7) = 3 + 3 + 3 + 3 + 4 + 4 + 4 = 24 = 2 * n(G)$$

since $I(5) = I(6) = I(7) = \{t, R, R^2, R^3\}$. But this is consistent with the fact that there are two orbits.

Unfortunately $\sum_x n(I(x))$ is usually too hard to calculate directly but we note that this sum gives the total number of invariances, i.e. the number of ordered pairs in the set $\{(f, x) | f(x) = x, f \in G, x \in X\}$. But grouping these pairs by the first component, i.e. by the group elements we see that we get a sum $\sum_f \psi(f)$ where $\psi(f) = n(\{x | f(x) = x\})$ and the sum is taken over all $f \in G$. If G is a small group this can be calculated. We have proven

Burnside's Theorem If the finite group G acts on the finite set X then the number of distinct orbits is given by

$$n(\text{orbits}) = \frac{1}{n(G)} \sum_f \psi(f)$$

where $\psi(f)$ is the number of elements held invariant by f and the sum ranges over all elements of G .

Example As an application we will count the number distinct necklaces of 6 beads made up of green, blue and red beads. Generally when this problem is discussed in the literature (see for example the author's web site www.neiu.edu/bhdayton/necksum.htm) it is assumed that two necklaces are the same if one can be rotated to match the other but may be different if they are flipped. Here we will assume that after a reflection a necklace is still the same necklace.

We start with the set X consisting of 6 numbered beads which could be colored red, blue or green. In other words, the necklaces we would have if rotated and reflected necklaces were different. Since each bead could be arbitrarily assigned one of 3 colors there are $3^6 = 729$ elements in X . Now we will allow the group D_6 to act on this set where we think of the beads as the vertices of a regular hexagon. Since a symmetry will take a necklace to the "same" necklace all the necklaces in any given orbit are considered the same. So we must count the number of orbits.

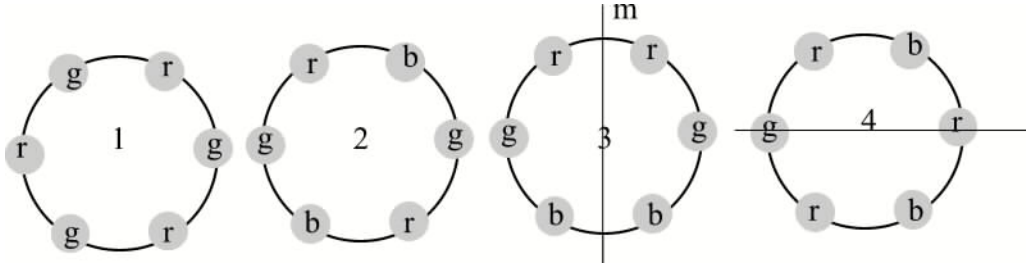


Figure 8: Necklaces with symmetries

We will use, of course, Burnside's Theorem. We have to decide how many elements of X are invariant under each of the 12 symmetries in D_6 . The do-nothing leaves all elements of X in place so $\psi(1) = 729$. On the other extreme r, r^5 , the $1/6$ -turns leave only the necklaces all of one color unchanged, so $\psi(r) = \psi(r^5) = 3$. But r^2 and r^4 leave necklaces with alternate colored beads unchanged (see necklace 1 in Figure 8) and there are 9 of these. r^3 is a half turn and leaves those necklaces with opposite beads the same color (necklace 2 in Figure 8) invariant, there are $3^3 = 27$ of these. Finally, The three reflections with mirror not on the beads (necklace 3 with vertical reflection) requires opposite beads to be the same so again we have $3^3 = 27$ and finally the three reflections with mirror through opposite beads (necklace 4 with horizontal reflection) only require the beads not on the mirror to match up so there are $3^4 = 81$ of these.

Hence the number of necklaces, i.e. orbits is

$$\frac{1}{n(G)} \sum_f \psi(f) = \frac{1}{12} \left(\overbrace{729 + 3 + 3 + 9 + 9 + 27}^{\text{rotations}} + \overbrace{3(27) + 3(81)}^{\text{reflections}} \right) = \frac{1104}{12} = 92$$

5 Conjugate Subgroups

In the last section we saw that the isotropy subgroups of elements in the same orbit had the same size. Actually these isotropy subgroups are even more closely related. In the example given by Figure 7 all the isotropy groups of the outside orbit were actually the same, and we saw that that was also true of the inside orbit. In general this is not the case.

Consider D_4 acting on the 4 vertices of the square (see Figure 6), r the counter-clockwise $\frac{1}{4}$ -turn and m the vertical reflection. The isotropy subgroup at 1 is $I(1) = \{1, mr\}$. Suppose we want to calculate the isotropy subgroup at $2 = r(1)$. We can do the following: rotate clockwise by r^{-1} so that 2 goes to 1. We know which elements keep 1 fixed so apply one of them, call it f , so $fr^{-1}(2) = f(1) = 1$. Now apply r to get $rfr^{-1}(2) = r(1) = 2$. In this simple case where the only choices for f are $1, mr$ we get $\{r1r^{-1} = 1, r(mr)r^{-1} = rm = mr^3\}$ which can be seen to be

the full isotropy subgroup at 2.

This works in general, if G acts on a set X suppose $g(a) = b$, for some $a, b \in X$. Let f be in the isotropy subgroup at a . Then $gfg^{-1}(b) = gf(a) = g(a) = b$ so $gfg^{-1} \in I(b)$. On the other hand suppose $h \in I(b)$. Then $f = g^{-1}hg \in I(a)$ because $g^{-1}hg(a) = g^{-1}h(b) = g^{-1}(b) = a$. But $gfg^{-1} = g(g^{-1}hg)g^{-1} = h$ So we see that $I(b) = \{gfg^{-1} | f \in I(a)\}$ exactly.

We call the group element gfg^{-1} a *conjugate* of f and the subgroup $gHg^{-1} = \{gfg^{-1} | f \in H\}$ a *conjugate subgroup* to the subgroup H . In general, as in the Figure 6 example, the group is not commutative and conjugate elements are not equal, nor are conjugate subgroups. But they always have the same number of elements. In the case of an abelian group then $gfg^{-1} = gg^{-1}f = f$ so conjugate elements and subgroups are equal, as in the example with Figure 7.

In the special case of isotropy subgroups conjugation takes the isotropy subgroup of one point to that of another, so conjugation moves position. So if conjugation by at least one element of the full group G takes the subgroup H to a different subgroup gHg^{-1} then we think of H as being a “positional” subgroup. So in D_4 (Figure 6) the subgroups $I(1), I(2), I(3), I(4)$ which are conjugate but not equal all measure a position. But in D_4 the subgroup $\{r, r^2, r^3\}$ remains the same (as a group, r, r^3 may change places as elements) under any conjugation. Thus this subgroup measures a “geometrical idea”, in this case the idea of “rotation”.

More generally we call a subgroup H of G *normal* if $gHg^{-1} = H$ for all $g \in G$. Normal subgroups relate to *global* properties whereas non-normal subgroups measure *local* properties.

Finally we look at one more example.

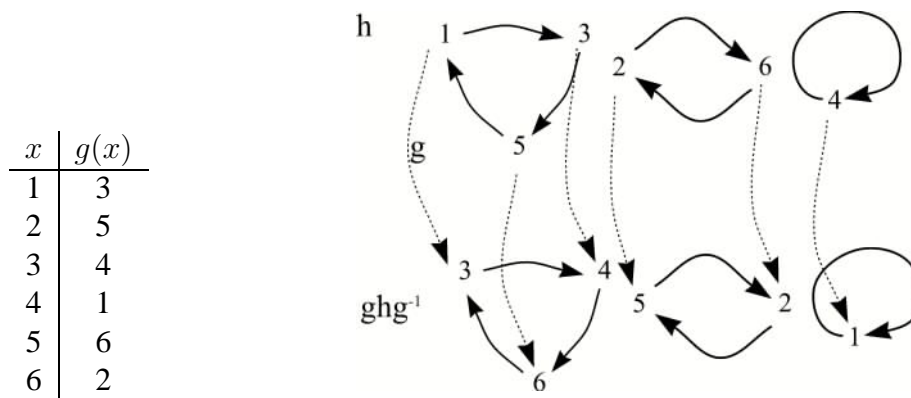


Figure 9: Conjugate Permutations

The top arrow diagram in Figure 9 shows the dynamic arrow diagram of the permutation of Figure 4, and the dotted arrows show the static arrow diagram of the permutation g given in the table of Figure 9. I claim that the lower dynamic arrow diagram is the arrow diagram of ghg^{-1} . For example, $ghg^{-1}(6) = gh(5) = g(1) = 3$ as shown on the lower diagram. The reader can check

the rest herself, just follow the rule: start at one point in the lower diagram, go back (up) on the g arrow, across on the h arrow and down on g again.

This happens in general, two permutations from S_n are conjugate if and only if their disjoint cycle decompositions are the “same” in the sense that there are the same number of cycles of the same sizes. For example $f = (1\ 3\ 7)(12\ 5\ 8\ 6)(2\ 9)(10\ 11)$ is conjugate to $h = (10\ 5\ 4)(3\ 11\ 7\ 8)(2\ 12)(1\ 9)$ in S_{12} because each has 2 two-cycles, 1 three-cycle and 1 four-cycle.

Exercise 2 Find a permutation $g \in S_{12}$ so that for permutations f, h of the previous paragraph $h = gfg^{-1}$. Hint: you can draw a picture like Figure 9.

6 Even and Odd Permutations

A useful fact about the symmetric groups S_n is that they contain a special subgroup of $\frac{n!}{2}$ elements called the *even* permutations. Unfortunately there is no really easy way to describe them, arrow diagrams again seem to be the best.

Here we draw the static arrow diagram but insist that the numbers in the range and domain match up horizontally, for example they should both be in order $1, 2, \dots, n$.

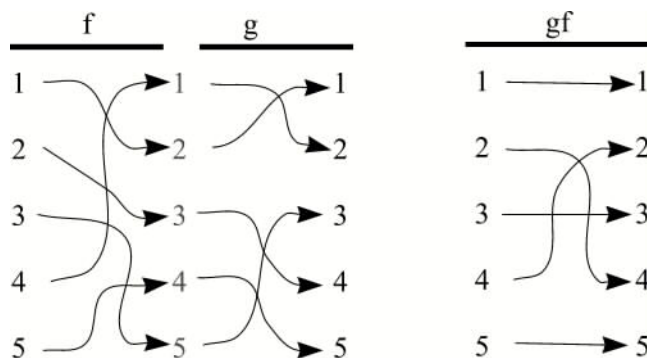


Figure 10: Even and odd permutations

It is then likely that some arrows will need to cross. Count how many crossings, for example in f in Figure 10 there are 4 crossings, for g there are 3. It is not difficult to arrange the crossings so that no three or more arrows cross at the same point. If the number of crossings is an even number then we call the permutation an *even* permutation (such as f), if the number of crossings is odd we say the permutation is *odd* (such as g).

Now to compose permutations we could simply, as on the left of Figure 10, eliminate the middle column of numbers, then we get the crossings of f plus the crossings of g , in this example we could say gf has $3 + 4 = 7$ crossings.

However if we look at the right of Figure 10 we see a problem with this definition of even and odd, mainly that there is more than one way to draw the static arrow diagram, the arrow diagram on the right also gives gf in the correct form but has only 3 crossings. What we need to show, as in Figure 10, is that the number of crossings in different pictures always differ by an even number. Unfortunately this is hard to do in a precise way, so this method of defining even and odd permutations is generally not used. But intuitively it is fairly easy to see why this works. On the left the long arrow, ignoring the middle column of numbers, starting from 1 goes to 2 and then back to 1 crossing the arrow from 4 to 1 to 2 twice. But on the right the first goes directly from 1 to 1 and the second stays under it, so when we “untangle” the arrows to eliminate one crossover we also eliminate the cross back. We see the same phenomena for the arrows starting from 3 and 5.

Once we agree that our definitions of even and odd make sense we can proceed. Since the sum of two even numbers is even it would follow that the set of even permutations is closed under composition. Also taking inverses just reverses arrows and does not affect the number of crossings so the inverse of an even permutation is also even. It then follows that the set of even permutations is a group, called the *alternating* group A_n .

The permutation g of Figure 10 clearly has the cycle decomposition $(1\ 2)(3\ 4\ 5)$ and we see the first cycle has one crossing while the second has two. More generally a cycle of even length is an odd permutation while a cycle of odd length is even. This gives a practical way of telling even from odd permutations, just find the disjoint cycle decomposition.

If we fix one particular odd permutation, say $h = (1\ 2)$, and multiply each even permutation by h we get a set of $n(A_n)$ odd permutations which all must be different by the cancellation property in groups. So there are at least as many odd permutations as even. But if we now multiply each odd permutation by h we then get that many different even permutations so there are at least as many evens. We conclude that there are the same number of odd and even permutations. Hence $n(A_n) = \frac{1}{2}n(S_n) = \frac{n!}{2}$.

Lastly we note that conjugation preserves the cycle lengths of the disjoint cycle decomposition so a conjugate of an even permutation is again even. Thus A_n is a normal subgroup of S_n .