Parity of permutations

Given a permutation σ of $\{1, 2, \ldots, n\}$, draw a diagram consisting of two horizontal rows of dots labelled 1, 2, ..., n, and n lines L_1, L_2, ..., L_n, where L_i connects the dot in the upper row whose label is i with the dot in the lower row whose label is i^σ. In other words, L_1 joins 1 to whatever it is that 1 "goes to" under the permutation, L_2 joins 2 to whatever 2 goes to, and so on. The lines should be drawn in such a way that two lines do touch without crossing each other; also, you should never have more than two lines crossing at any given point, and the lines are not allowed to cross themselves or to ever go above the upper row of dots or below the lower row of dots. (The lines do not have to be straight.)

We say that the permutation is even if a diagram drawn in accordance with the above rules has an even number of line crossings, or odd if the number of crossings is odd.

Although the number of crossings can be altered by drawing the diagram differently, the oddness or evenness of the number of crossings cannot be changed. The reason for this is as follows. The total number of crossings in the diagram is

$$\sum (\text{the number of times } L_i \text{ and } L_j \text{ cross})$$

where the sum ranges over all pairs of lines L_i and L_j. We may choose the notation so that $i < j$. Now if $i^\sigma > j^\sigma$ then upper and lower endpoints of L_i are on opposite sides of L_j, and this means that L_i and L_j must cross an odd number of times, whereas if $i^\sigma < j^\sigma$ then the endpoints of L_i are on the same side of L_j, and the number of crossings is even. But whether the sum of a collection of integers is even or odd just depends on how many of the summands are odd: the total is odd if the number of odd summands is odd; the total is even if the number of odd summands is even. So, if we define

$$\mathscr{N}(\sigma) = \{(i, j) \mid i < j \text{ and } i^\sigma > j^\sigma\},$$

then L_i and L_j cross an odd number of times if and only if (i, j) is in $\mathscr{N}(\sigma)$, and we conclude that

$$\sigma \text{ is odd if and only if } \#\mathscr{N}(\sigma) \text{ is odd,}$$
$$\sigma \text{ is even if and only if } \#\mathscr{N}(\sigma) \text{ is even.}$$

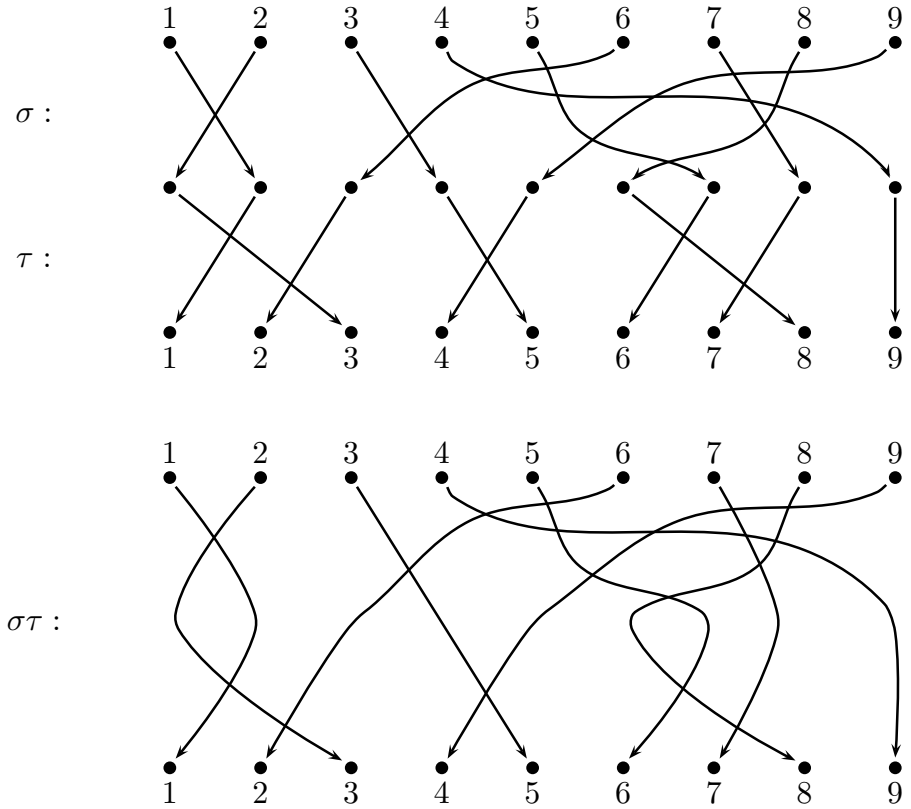
The following lemma is the key to the theoretical importance of these diagrams.

Theorem. *Let σ, τ be permutations of $\{1, 2, \ldots, n\}$, and suppose that σ has a diagram with N crossings and τ has a diagram with M crossings. Then $\sigma\tau$ has a diagram with $N + M$ crossings.*

Proof. One can obtain a diagram for $\sigma\tau$ by merging the diagrams of σ and τ, in the following way: simply identify the lower row of dots in the σ diagram with the upper row of dots in the τ diagram, and then remove the middle row of dots. The diagram obtained in this way has $N + M$ crossings. □

To illustrate this proof, consider the permutations $\sigma = (1, 2)(3, 4, 9, 5, 7, 8, 6)$ and $\tau = (1, 3, 2)(4, 5)(6, 8, 7)$ in Sym(9). We draw a diagram for σ and a diagram for τ, with

the lower row of the σ diagram coinciding with the upper row of the τ diagram, and then merge the two.



To compute the product $\sigma\tau$ one applies σ first and then τ. Since (for example) σ takes 5 to 7 and τ takes 7 to 6, the top part of the diagram has a line from dot 5 (top row) to dot 7 (middle row), and lower part has a line from dot 7 (middle row) to dot 6 (bottom row). The merged diagram thus has a line from 5 to 6, in accordance with the fact that $\sigma\tau$ takes 5 to 6. Similarly, $3 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 5$ results in $3 \xrightarrow{\sigma\tau} 5$ and a line from 3 to 5 in the merged diagram. Indeed, the diagram shows us that $\sigma\tau = (2,3,5,6)(4,9)$. And, of course, since the chosen diagrams for σ and τ had 13 and 5 crossings respectively, the diagram for $\sigma\tau$ obtained by the merging process has 18 crossings.

As an immediate consequence of the lemma we deduce the key result about parity of permutations.

Theorem. *Let σ, τ be permutations of $\{1, 2, \ldots, n\}$. Then $\sigma\tau$ is even if σ and τ are both even or both odd, and odd if one is odd and the other even.*

Proof. Choose a diagram for σ and a diagram for τ, and suppose that they have N and M crossings respectively. By the lemma, $\sigma\tau$ has a diagram with $N + M$ crossings, which is is even if N and M are both even or both odd, and odd if one of N or M is odd and the other even. □

Definition. If σ is a permutation we define $\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$

With this definition, the theorem above can be restated as follows:

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) \qquad \text{for all } \sigma, \tau \in \mathrm{Sym}(n). \tag{1}$$

This equation says that the function ε *preserves multiplication*. Functions with this property are very important in group theory, and we shall meet other examples later.

The following result is a consequence of Eq. (1).

Theorem. *The set of all even permutations of* $\{1, 2, \ldots, n\}$ *is a subgroup of* $\mathrm{Sym}(n)$.

Proof. Let A be the set of all even permutations in $\mathrm{Sym}(n)$. We must show that A satisfies (SG1), (SG2) and (SG3).

Let σ and τ be arbitrary elements of A. Then $\varepsilon(\sigma) = \varepsilon(\tau) = 1$, and by Eq. (1),

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = 1.$$

So $\varepsilon(\sigma\tau) \in A$ whenever $\sigma, \tau \in A$. That is, (SG1) holds.

The identity permutation $\mathrm{id} \in \mathrm{Sym}(n)$ can be represented bythe diagram in which each dot is joined to the one below it by a vertical line. This diagram has no crossings, and since zero is an even number it follows that $\varepsilon(\mathrm{id}) = 1$. So $\mathrm{id} \in A$; that is, (SG2) holds.

Let $\sigma \in A$ be arbitrary. Then $\varepsilon(\sigma) = 1$, and so

$$\varepsilon(\sigma^{-1}) = \varepsilon(\sigma^{-1})\varepsilon(\sigma) = \varepsilon(\sigma^{-1}\sigma) = \varepsilon(\mathrm{id}) = 1.$$

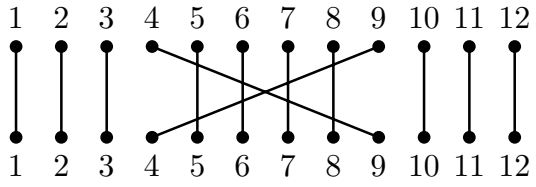
Hence $\sigma^{-1} \in A$ whenever $\sigma \in A$; that is, (SG3) holds. □

Although in the above proof we chose to appeal to the definition of the function ε to prove that $\varepsilon(\mathrm{id}) = 1$, it is also not hard to deduce this as a consequence of Eq. (1). In fact, the theorem we have just proved is a special case of the following important general theorem, which we shall prove later.

Let G and H be groups, and $\phi\colon G \to H$ a function satisfying $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Let e_H be the identity element of H. Then $\{\, x \in G \mid \phi(x) = e_H \,\}$ is a subgroup of G.

We temporarily defer further discussion of this, and return to our investigation of parity of permutations.

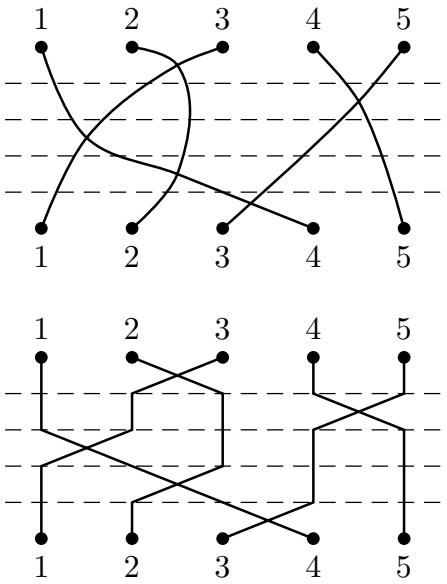
It is easy to see that a transposition (i, j) has to be odd: its diagram can be drawn so that the number of crossings is $2|i - j| - 1$. The diagram below illustrates this for $(4, 9)$.



The two diagonal lines cross exactly the same vertical lines as each other, namely the ones between i and j. There are $|i - j| - 1$ of these, making $2|i - j| - 2$ crossings. And the diagonal lines cross each other, making the total number of crossings $2|i - j| - 1$, which is odd.

Proposition. *Every permutation can be written as a product of transpositions. In fact, every permutation can be written as a product of transpositions that interchange adjacent numbers.*

For ease of discussion, we shall call a transposition (i, j) a *simple transposition* if i and j are adjacent numbers. That is, (i, j) is simple if $|i - j| = 1$. Clearly the simple transpositions are those associated with diagrams that have just one crossing. The diagram below indicates why the proposition is true: the diagram associated with any permutation can be split into layers that each correspond to simple transpositions.



The top diagram here is associated with the permutation $\sigma = (1, 4, 5, 3)$, and the other diagram illustrates that $\sigma = (2, 3)(4, 5)((1, 2)(2, 3)(3, 4)$.

We shall not give a formal proof of the proposition. However, assuming that our given permutation diagram is drawn in such a way that the lines from the top row of dots to the bottom row of dots descend continually, never bending back upwards, then the highest crossing in the diagram gives the first simple transposition in the factorization that we seek, the next highest gives the next simple transposition, and so on. In this way each crossing is viewed as a crossing of adjacent lines, and we obtain a factorization of the given permutation as a product of N simple transpositions, where N is the number of crossings in the original diagram.

Of course, just as the diagram associated with a permutation is not uniquely determined, so the factorization of a permutation as a product of simple transpositions is not unique.

The following result is trivial, but extremely useful.

Proposition. *A cycle of length n can be expressed as a product of $n - 1$ transpositions.*

It is straightforward to simply write down such a factorization: it is left to the reader to check first that

$$(1, 2, 3, 4, 5, 6, 7) = (1, 2)(1, 3)(1, 4)(1, 5)(1, 6)(1, 7),$$

and then that

$$(i_1, i_2, \ldots, i_n) = (i_1, i_2)(i_1, i_3) \cdots (i_1, i_n)$$

for any cycle $(i_1, i_2, \ldots, i_n)$.

Thus it turns out—perhaps unfortunately—that cycles of even length (such as transpositions) are odd, while cycles of odd length are even. This makes it easy to tell the parity of a permutation from its expression as a product of disjoint cycles: if there are an odd number of cycles of even length then the permutation is odd, otherwise it is even. For example, $(1, 2, 3)$ is even, $(1, 4, 5, 2)$ is odd, $(1, 4, 5, 7, 3)(2, 6, 8)(9, 12)$ is odd.

Indeed, you do not have to obtain the standard expression for a permutation as a product of disjoint cycles to apply this rule: even if the cycles are not disjoint then the permutation is odd if and only if it has an expression as a product of cycles such that the number of even length cycles is odd. So, for example, $(1, 2, 4, 5)(1, 2, 4)(1, 2, 4, 5)(4, 3)$ is odd.

Recall that the group of all permutations of the set $\{1, 2, \ldots, n\}$ is known as the *symmetric group*, $\mathrm{Sym}(n)$. The subgroup consisting of the even permutations also has a name.

Definition. The group of all even permutations of the set $\{1, 2, \ldots, n\}$ is known as the *alternating group*, $\mathrm{Alt}(n)$.

Equivalence relations

Suppose that $\sim$ is a relation on a set X. This just means that $x \sim y$ is a proposition that makes sense for every pair of elements $x, y \in X$; in particular, either $x \sim y$ is true or $x \sim y$ is false. For every pair of elements of the set, the relation either holds or does not hold. We write $x \sim y$ if it holds, $x \not\sim y$ if it does not.

For example, suppose that X is a collection of medals, some made of gold, some of silver and some of bronze. Let $\sim$ be the relation "is made of the same metal as". If $x, y \in X$, then $x \sim y$ if x is made of the same metal as y, and $x \not\sim y$ if x is not made of the same metal as y. Given that every the medal in the set X is made of one of the three metals, it is always meaningful to enquire of a pair of medals from X whether or not the relation holds.

Of course, there are numerous mathematical examples of relations. Thus $>$ is a relation on $\mathbb{R}$, the set of all real numbers: given $x, y \in \mathbb{R}$, either $x > y$ or $x \not> y$. We could define a relation $\equiv$ on the set of all positive integers as follows: $x \equiv y$ if and only if the final digits of x and y (in the usual base 10 representation) are the same. This would give $21 \equiv 101$, and $7 \not\equiv 13$.

At present we are interested in the following three properties, which any given relation may or may not possess.

Definition. Let $\sim$ be a relation on the set X.
(a) We say that $\sim$ is *reflexive* if $x \sim x$ for all $x \in X$.
(b) We say that $\sim$ is *symmetric* if for all $x, y \in X$, if $x \sim y$ then $y \sim x$.
(c) We say that $\sim$ is *transitive* if for all $x, y, z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

The relation $>$ on $\mathbb{R}$ is clearly transitive: if x, y and z are real numbers with $x > y$ and $y > z$ then it follows that $x > z$. However, it is not reflexive since there exist real numbers x that do not satisfy $x > x$. (Of course, there are in fact no real numbers x for which $x > x$, but all we need is one example, like $x = 0$, to show that $>$ is not reflexive.) On the other hand, the "is made of the same metal as" relation is reflexive, symmetric and transitive, and so is the "has the same final digit as" relation.

Definition. We say that a relation $\sim$ on a set X is an *equivalence relation* if it is reflexive, symmetric and transitive.

It should be emphasized that this is nothing more nor less than the ordinary everyday concept of equivalence. In any context in which things may or may not be equivalent, we would always say that everything is equivalent to itself, that equivalence of A and B is the same as equivalence of B and A, and that two things that are both equivalent to a third are equivalent to each other. If any of these were not true we would not have a genuine case of equivalence.

Definition. If $\sim$ is an equivalence relation on a set X, and if $x \in X$, we define the *equivalence class* of x to be the set $\mathcal{E}(x, \sim)$ consisting of all elements of X that are equivalent to x. That is, $\mathcal{E}(x, \sim) = \{\, y \in X \mid y \sim x \,\}$.

The crucial thing about equivalence relations, in mathematics as in everyday life, is that an equivalence relation on a set of things divides that set up into subsets consisting of things that are all equivalent to one another. These are the equivalence classes of the above definition. Two things are in the same class if and only if they are equivalent to each other. Things from different classes are definitely not equivalent. The equivalence classes do not overlap, and together they cover the whole set of things under discussion.

We can state these properties more formally, as follows.

Proposition. *Let $\sim$ be an equivalence relation on a set X. If x and y are arbitrary elements of X then*

a) $\mathcal{E}(x, \sim) = \mathcal{E}(y, \sim)$ *if* $x \sim y$, *and*

b) $\mathcal{E}(x, \sim) \cap \mathcal{E}(y, \sim) = \emptyset$ *if* $x \not\sim y$.

Furthermore, every element of X lies in some equivalence class.

The next step in this process is to focus attention not on the objects of X themselves, but rather on the equivalence classes. This is really the whole point, for it simplifies the context in which we are working, enabling us to deal with many things at a time instead of treating every object individually.

Definition. Let $\sim$ be an equivalence relation on a set X. The set of all equivalence classes of X with respect to $\sim$ is called the *quotient* of X by $\sim$, and it is often denoted by $X/\!\sim$.

Observe that in the situation of the definition, $X/\!\sim$ is a set whose elements are sets. This can take a little getting used to. In the medals example above, we do not know how many elements the set X has: we were not told the total number of medals. But the set $X/\!\sim$ has three elements: the set of all gold medals, the set of all silver medals and the set of all bronze medals. This is a little abstract. However, sets whose elements are themselves sets are extremely commonplace in modern mathematics. Furthermore, there is no reason to stop at this level. It is perfectly acceptable, and common, to deal with sets whose elements are sets whose elements are sets, not to mention sets whose elements are sets whose elements are sets whose elements are sets, and so on.

Permutation groups and their orbits

This section has not yet been dealt with in lectures. However, the topic is investigated in Computer Tutorial 9.

Let G be a subgroup of $\mathrm{Sym}(n)$. We can use G to define a relation $\sim$ on the set $\{1, 2, \ldots, n\}$, as follows: for all $i, j \in \{1, 2, \ldots, n\}$ we say that $i \sim j$ if and only if there exists a permutation $\sigma \in G$ such that $i^\sigma = j$. It turns out that this relation is always an equivalence relation, given that G is a group.

For example, the following set G is a subgroup of $\mathrm{Sym}(5)$:

$$G = \{\, \mathrm{id},\ (3,4,5),\ (3,5,4),\ (1,2),\ (1,2)(3,4,5),\ (1,2)(3,5,4) \,\}.$$

We omit the verification that G is a subgroup of $\mathrm{Sym}(5)$. But it is easy to check that it gives rise to an equivalence relation on $\{1, 2, 3, 4, 5\}$, with two equivalence classes, namely $\{1, 2\}$ and $\{3, 4, 5\}$. There are permutations in G that take 1 to 2 and permutations in G that take 2 to 1. There are also permutations in G that take 3 to 4, that take 3 to 5, that take 4 to 5, that take 4 to 3, and so forth. But there are none that take 1 or 2 to 3, 4 or 5, or vice versa.

More generally, let G be a subgroup of $\mathrm{Sym}(n)$, and define $\mathcal{P}_k$ to be the set of all k-element subsets of $\{1, 2, \ldots, n\}$. Define a relation $\sim$ on $\mathcal{P}_k$ as follows: if $X, Y \in \mathcal{P}_k$, then $X \sim Y$ if and only if there exists $\sigma \in G$ such that $Y = X^\sigma$, where by definition $X^\sigma = \{\, x^\sigma \mid x \in X \,\}$. It can be shown that this is an equivalence relation; the equivalence classes are known as *orbits*.

Consider, for example, the group of symmetries of a square, identified with permutations of $\{1, 2, 3, 4\}$ as described in an earlier lecture. Then

$$G = \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,2)(3,4), (2,4), (1,4)(2,3)\}.$$

The set $\mathcal{P}_2$ of all 2-element subsets of $\{1, 2, 3, 4\}$ has $\binom{4}{2} = 6$ elements,

$$\mathcal{P}_2 = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\},$$

and the equivalence relation described above splits $\mathcal{P}_2$ into two orbits, one with 2 elements and one with 4 elements:

$$\mathcal{P}_2 = \{\{1,3\}, \{2,4\}\} \cup \{\{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}\}.$$

The idea here is that a symmetry of the square can take any pair of adjacent vertices to any pair of adjacent vertices, and can take any pair of opposite vertices to any pair of opposite vertices. But no symmetry can take adjacent vertices to opposite vertices, or vice versa. There are 4 pairs of adjacent vertices, 2 pairs of opposite vertices.

Here is a MAGMA session dealing with this example.

```
> S:=Sym(4);
> a:=S!(1,2,3,4);
> b:=S!(1,3);
> G:=sub<S | a,b>;
> Set(G);
```

```
{
    (1, 3)(2, 4),
    Id(G),
    (1, 2, 3, 4),
    (1, 4, 3, 2),
    (2, 4),
    (1, 3),
    (1, 4)(2, 3),
    (1, 2)(3, 4)
}
> X:={1,2};
> C1:={ X^g : g in G};
> C1;
{
    { 1, 4 },
    { 2, 3 },
    { 1, 2 },
    { 3, 4 }
}
> Y:={1,3};
> C2:={ Y^g : g in G};
> C2;
{
    { 1, 3 },
    { 2, 4 }
}
> for A in C1 do
for> for B in C1 do
for|for> exists{g : g in G | A^g eq B};
for|for> end for;
for> end for;
true
true
... 13 similar lines omitted ...
true
> for A in C2 do
for> for B in C2 do
for|for> exists{g : g in G | A^g eq B};
for|for> end for;
for> end for;
true
true
true
true
```

One advantage of using MAGMA is that it is able to do much larger examples than the above without any difficulty. The disadvantage is that rushing too quickly to computer calculations can deprive one of important theoretical insights. It is quite possible to

understand very large examples without any calculation whatever, just by theoretical considerations. The moral is that computer calculations should always be accompanied by human thought processes.

Here is another MAGMA example, this time with a group of order 110.

```
> S:=Sym(11);
> a:=S!(1,2,3,4,5,6,7,8,9,10,11);
> b:=S!(2,3,5,9,6,11,10,8,4,7);
> G:=sub<S | a,b>;
> #G;
110
> X1:={1,2};
> C1:={X1^g : g in G};
> #C1;
55
> (11*10)/(2*1);
55
> Y1:={1,2,3};
> D1:={Y1^g : g in G};
> #D1;
55
> Y2:={1,2,4};
> D2:={Y2^g : g in G};
> #D2;
110
> C2 meet C3;
{}
> (11*10*9)/(3*2*1);
165
> Z1:={1,2,3,4};
> E1:={Z1^g : g in G};
> #E1;
55
> Z2:={1,2,3,5};
> E2:={Z2^g : g in G};
> #E2;
110
> Z3:={1,2,3,6};
> E3:={Z3^g : g in G};
> #E3;
110
> #(E3 meet E2);
0
> Z4:={1,3,4,6};
> E4:={Z4^g : g in G};
> #E4;
55
```

```
> E4 eq E1;
false
> #(E1 join E2 join E3 join E4);
330
> (11*10*9*8)/(4*3*2*1);
330
```

For each k, let $\mathcal{P}_k$ be the set of k-element subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. The group G in the above example has just one orbit on $\mathcal{P}_2$, which has $\binom{11}{2} = 55$ elements. On $\mathcal{P}_3$, with $\binom{11}{3} = 165$ elements, there are two orbits, one with 55 elements and the other with 110. On $\mathcal{P}_4$, with $\binom{11}{4} = 330$ elements, there are 4 orbits, two with 55 elements and two with 110 elements.

Cosets as equivalence classes

Let G be a group and H a subgroup of G. Recall that this means that H satisfies
(SG1): $xy \in H$ whenever x, $y \in H$,
(SG2): $e \in H$ (where e is the identity element of G),
(SG3): $x^{-1} \in H$ whenever $x \in H$.

Define a relation $\equiv$ on G as follows: if x, $y \in G$ then $x \equiv y$ if and only if $x = hy$ for some $h \in H$.

The relation $\equiv$ is reflexive.

Proof. Let $x \in G$. Then $x = ex$, since e is the identity. It follows that $x = hx$ for some $h \in H$, since $e \in H$ by (SG2). Hence $x \equiv x$. Since this holds for all $x \in G$, we have shown that $\equiv$ is reflexive. □

The relation $\equiv$ is symmetric.

Proof. Let x, $y \in G$, and suppose that $x \sim y$. Then $x = hy$ for some $h \in H$. So $h^{-1}x = h^{-1}hy = ey = y$. And $h^{-1} \in H$, since $h \in H$ (by (SG3)). So $y = h'x$ for some $h' \in H$, namely $h' = h^{-1}$. Thus $y \sim x$. So we have shown that $y \sim x$ whenever $x \sim y$, as required. □

The relation $\equiv$ is transitive.

Proof. Let x, y, $z \in G$, and suppose that $x \sim y$ and $y \sim z$. Then $x = hy$ for some $h \in H$, and $y = h'z$ for some $h' \in H$. So $x = h(h'z) = (hh')z$. And $hh' \in H$, by (SG1), since $h \in H$ and $h' \in H$. So $x = h''z$ for some $h'' \in H$, namely $h'' = hh'$. Thus $x \sim z$. So we have shown that $x \sim z$ whenever $x \sim y$ and $y \sim z$, as required. □

It should be observed that we needed exactly one of the three subgroup properties (SG1), (SG2) and (SG3) in each of the above three proofs.

Since $\equiv$ is reflexive, symmetric and transitive, it is an equivalence relation on G, and hence it partitions G into equivalence classes. If $g \in G$ then the equivalence class containing g is the set

$$\{\, x \in G \mid x \equiv g \,\} = \{\, x \in G \mid x = hg \text{ for some } h \in H \,\} = \{\, hg \mid h \in H \,\} = Hg,$$

the right coset of H containing g. So the equivalence classes for $\equiv$ are exactly the right cosets of H in G. We conclude that every element of G lies in exactly one right coset of the subgroup H. So we can state the following result.

Proposition. *If H is a subgroup of G, then G is the disjoint union of the right cosets of H in G.*

As a corollary of this we obtain the following important result.

Lagrange's Theorem. *Let G be a finite group and H a subgroup of G. Then $\#H$ is a divisor of $\#G$.*

Proof. Let $\#G = n$ and $\#H = m$. Suppose that the number of distinct right cosets of H in G is k. Then G is the disjoint union of k sets of size m, since (as we proved in a previous lecture) all the cosets Hg have the same number of elements as H. Hence $n = km$, and, in particular, m is a divisor of n. □

For example, if $\#G = 100$ then G could have subgroups of any of the orders 1, 2, 4, 5, 10, 20, 25, 50 and 100, but it cannot have subgroups of any other orders. Note that there is no guarantee that there will be a subgroup of G whose order is a given divisor of $\#G$; all that is guaranteed is that a number that is not a divisor of $\#G$ is not the order of any subgroup.

Definition. The number of distinct right cosets of H in G is called the *index* in G of the subgroup H. It is denoted by $[G : H]$.

The above proof tells us that if G is a finite group and H a subgroup of G then $[G : H] = \#G/\#H$.

It turns out that the right cosets of subgroups of G are the only nonempty subsets of G with the property that they are disjoint from all their right translates.

Proposition. *Suppose that S is a nonempty subset of a group G, and suppose that no two distinct right translates of S have any elements in common. Then there exists a subgroup H of G and an element $g \in G$ such that $S = Hg$.*

Proof. Choose some fixed element $g \in S$—we can do this since $S \neq \emptyset$—and define $H = Sg^{-1}$. Note that $e = gg^{-1} \in Sg^{-1} = H$.

Recall that in an earlier lecture we made the definition

$$\mathrm{Stab}(W) = \{\, x \in G \mid Wx = W \,\},$$

whenever W is a subset of G, and we showed that $\mathrm{Stab}(W)$ is always a subgroup of G. We shall use this to prove that the set H above is a subgroup of G, by showing that $H = \mathrm{Stab}(H)$.

We show first that if x is any element of H then $Hx = H$. Since $e \in H$ we have that $ex \in Hx$; that is, $x \in Hx$. By assumption we know that $x \in H$. So the sets $Hx = Sg^{-1}x$ and $H = Sg^{-1}$ have the element x in common. Since our assumption is that distinct right translates of S have no common elements, we conclude that these right translates cannot be distinct. That is, $Hx = H$, as claimed.

The converse of the above statement is also true: if $Hx = H$ then $x \in H$. Indeed, this is trivial, since $x = ex \in Hx$ gives $x \in H$, when $Hx = H$.

We conclude from the above that H coincides with the set of all x in G such that $Hx = H$. That is, $H = \mathrm{Stab}(H)$, as claimed. Now since $H = Sg^{-1}$, it follows that $Hg = Sg^{-1}g = Se = S$, so that S is a right coset of the subgroup H, as required. □