If G is a group and x, $y \in G$ then it is not necessarily true that $xy = yx$. If x and y do satisfy this condition we say that they *commute*. For example, the elements $(1,2)$ and $(1,3)$ in the group Sym(3) do not commute, whereas the elements $(1,2)(3,4)$ and $(1,3)(2,4)$ in the group Sym(4) do commute:

$$(1,2)(1,3) = (1,2,3), \qquad (1,3)(1,2) = (1,3,2);$$
$$((1,2)(3,4))((1,3)(2,4)) = (1,4)(2,3) = ((1,3)(2,4))((1,2)(3,4)).$$

Similarly, in the group of all 2×2 invertible matrices over $\mathbb{R}$, it is easily checked that

$$\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix},$$

and by contrast

$$\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}.$$

Definition. A group G is said to be *Abelian* (or *commutative*) if $xy = yx$ for all x, $y \in G$.

Let G be a group with n elements, x_1, x_2, …, x_n, and form the multiplication table in which the rows and columns correspond to x_1, x_2, …, x_n, taken in that order. Then the (i,j)-entry of the table—that is, the entry in row i and column j—is the product $x_i x_j$, while the (j,i)-entry contains the product $x_j x_i$. We conclude that the group is Abelian if and only if the (i,j) and (j,i) entries of the multiplication table are equal for all values of i and j. Thinking of the table as an $n \times n$ matrix, the condition that the (i,j) and (j,i) entries are always equal says that the matrix is symmetric. So finite Abelian groups can be characterized in the following way.

A finite group is Abelian if and only if its multiplication table (thought of as a matrix) is symmetric.

(This characterization assumes that the same ordering of the elements of G is used for the rows of the table as for the columns of the table.)

Example. Let $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ and $c = (1,4)(2,3)$, elements of Sym(4). We noted above that $ab = c$ and $ba = c$. It is very easy to check that $a^2 = b^2 = c^2 = \mathrm{id}$. It follows without further computation that $ac = a(ab) = (aa)b = \mathrm{id}\, b = b$. Similarly, $bc = b(ba) = (bb)a = \mathrm{id}\, a = a$. Similarly also, $ca = ba^2 = b$ and $cb = ab^2 = a$. So we can now fill in a multiplication table for the set $H = \{\mathrm{id}, a, b, c\}$.

	id	a	b	c
id	id	a	b	c
a	a	id	c	b
b	b	c	id	a
c	c	b	a	id

In particular, we find that the product of any two elements in H is also in H; so H is closed under multiplication. The identity element is in the set H, and our calculations have also shown that the inverse of every element of H. Indeed, each of the four elements

of H has the property that its square is the identity, and this implies that each of these elements is its own inverse. (Recall that y is called an inverse of x if $xy = yx = \mathrm{id}$, and in a group every element has a unique inverse. If $x^2 = \mathrm{id}$ then $xy = yx = \mathrm{id}$ holds with $y = x$; so we can say that $x = x^{-1}$ whenever $x^2 = \mathrm{id}$.)

Since H is closed under multiplication, contains the identity and contains the inverses of all its elements, it is a subgroup of Sym(4). It is Abelian: the table is symmetric about the diagonal from the upper left corner to the lower right.

It is a familiar fact that the inverse of a product of two invertible matrices is the product of the inverses, in the reverse order. The same is easily shown to be true also for elements of arbitrary groups.

Proposition. *Let G be a group and x, $y \in G$. Then $(xy)^{-1} = x^{-1}y^{-1}$.*

Proof. Let e be the identity element of G. By associativity,

$$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e,$$

and similarly

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}((x^{-1}x)y) = y^{-1}(ey) = y^{-1}y = e.$$

This shows that $y^{-1}x^{-1}$ is an inverse of xy. But inverses are unique; so it is the inverse of xy. □

As noted in a previous lecture, it follows from associativity of multiplication that, in any group G, all possible bracketings of a product of several factors yield the same element. This result, which is sometimes called the *Generalized Associative Law*, means that there is no ambiguity involved in omitting the brackets from extended products. Adopting this convention, it is clear that the above result about inverses extends to products involving more than two factors: $(x_1x_2\cdots x_n)^{-1} = x_n^{-1}x_{n-1}^{-1}\cdots x_1^{-1}$ for all $n \geq 0$ and x_1, x_2, …, $x_n \in G$.

In the example given above, once we had shown that $ab = ba$, we were able to deduce readily that all elements of H commute with each other. This is because the elements a and b generate H, in the sense that all the elements of H can be expressed in terms of these two elements. It is a general fact that if a group is generated by a set of elements that commute with each other then the group is Abelian.

Let us make more precise what it means to say that a set of elements in a group generates that group.

Definition. Let $S = \{g_1, g_2, \ldots, g_k\}$ be a subset of a group G. We define $\langle S\rangle$, or $\langle g_1, g_2, \ldots, g_k\rangle$, to be the set of all elements of G of the form $x_1x_2\cdots x_n$, where n is a nonnegative integer and each factor x_i is either an element of S or the inverse of an element of S. That is, $g \in \langle g_1, g_2, \ldots, g_k\rangle$ if and only if there exists an integer $n \geq 0$ such that $g = g_{i_1}^{\varepsilon_1}g_{i_2}^{\varepsilon_2}\cdots g_{i_n}^{\varepsilon_n}$ for some i_1, i_2, …, $i_n \in \{1, 2, \ldots, k\}$ and ε_1, ε_2, …, $\varepsilon_n \in \{1, -1\}$. We say that S generates G, or g_1, g_2, …, g_k generate G, if $\langle g_1, g_2, \ldots, g_k\rangle = G$.

Thus if a, b, $c \in G$, where G is a group, then $\langle a, b, c\rangle$ is the subset of G consisting of all elements that can be expressed in terms of a, b and c. It contains, for example, the elements ab, $c^{-1}ab^{-1}c$ and $(ab)^{17}(ca)^2$, and also the identity element of G.

In the case that S consists of a single element x, we see that $\langle S\rangle = \langle x\rangle$ consists of all the powers of x; it is the subgroup generated by the element x, as defined in a previous lecture.

It is, indeed, a fact that $\langle S\rangle$ is always a subgroup of G, for any subset S of the group G. A formal proof of this will be given below, but it is helpful to first observe that $\langle a, b, c\rangle$ (as described above) is closed under multiplication. It is immediately apparent that this is true: if g, $h \in G$ can both be expressed in terms of a, b and c, then so can gh. For example, the product of $c^{-1}ab^{-1}c$ and $(ab)^{17}(ca)^2$, namely $c^{-1}ab^{-1}c(ab)^{17}(ca)^2$, is just as obviously an element of $\langle a, b, c\rangle$ as the the separate factors are.

It will be convenient to use the following notation: if S is a subset of a group G, let $S^{-1} = \{\, g^{-1} \mid g \in S \,\}$. Using this, the definition of $\langle S\rangle$ can be stated as

$$\langle S\rangle = \{\, x_1x_2\cdots x_n \mid n \geq 0 \text{ and } x_i \in S \cup S^{-1} \text{ for all } i \in \{1, 2, \ldots, n\} \,\}.$$

Proposition. *Let S be a subset of a group G. Then $\langle S\rangle$ is a subgroup of G.*

Proof. Let g, $h \in \langle S\rangle$. Then there exist nonnegative integers n and m, and elements x_1, x_2, $\ldots x_n$ and y_1, y_2, $\ldots$, y_m in $S\cup S^{-1}$ such that $g = x_1x_2\cdots x_n$ and $h = y_1y_2\cdots y_m$. We see that $gh = (x_1x_2\cdots x_n)(y_1y_2\cdots y_m)$ is an element of $\langle S\rangle$, since every factor in this expression for gh lies in the set $S \cup S^{-1}$. So the product gh is in $\langle S\rangle$ whenever g and h are both in $\langle S\rangle$; that is, $\langle S\rangle$ is closed under multiplication.

The identity element of G lies in the set $\langle S\rangle$, since by definition the product $x_1x_2\cdots x_n$ equals the identity if $n = 0$. (Empty products, like x^0, are always defined to be the identity element. This ensures that equations like $(x_1x_2\cdots x_n)(x_{n+1}x_{n+2}\cdots x_m) = x_1x_2\cdots x_m$ remain valid in the case $n = 0$. But if you do not like this then you can always regard it as a special definition that the identity element is in the set $\langle S\rangle$. This applies even if the set S itself is empty.)

In the previous two paragraphs we have shown that (SG1) and (SG2) are satisfied by $\langle S\rangle$, and so it remains to show that (SG3) is satisfied also. Now if $g \in \langle S\rangle$ then $g = x_1x_2\cdots x_n$ for some $n \geq 0$ and some $x_i \in S \cup S^{-1}$. Since $g = x_1x_2\cdots x_n$ gives $g^{-1} = x_n^{-1}x_{n-1}^{-1}\cdots x_1^{-1}$, and since $x_i \in S \cup S^{-1}$ gives $x_i^{-1} \in S \cup S^{-1}$ also, it follows that $g^{-1} \in \langle S\rangle$. So $\langle S\rangle$ contains the inverses of all of its elements, as required. □

In view of the above proposition, we shall henceforth refer to $\langle S\rangle$ as the *subgroup generated by S*.

In the syntax of MAGMA, if a group `G` and elements `a`, `b` and `c` have been defined, then `sub < G | a,b,c >` constructs the subgroup of `G` generated by `a`, `b` and `c`. Similarly, if `S` is a subset of `G` then `sub < G | S >` constructs the subgroup generated by `S`. For example, in the following MAGMA session we construct a certain subgroup of Sym(11) and find out how many elements it has of various orders.

```
> G := Sym(11);
> M := sub< G | (1,10)(2,8)(3,11)(5,7), (1,4,7,6)(2,11,10,9)>;
> #M;
7920
> S11 := { g : g in M | Order(g) eq 11 };
> #S11;
1440
```

```
> S8 := { g : g in M | Order(g) eq 8 };
> #S8;
1980
> S6 := { g : g in M | Order(g) eq 6 };
> #S6;
1320
> S5 := { g : g in M | Order(g) eq 5 };
> #S5;
1584
> S4 := { g : g in M | Order(g) eq 4 };
> #S4;
990
> S3 := { g : g in M | Order(g) eq 3 };
> #S3;
440
> S2 := { g : g in M | Order(g) eq 2 };
> #S2;
165
> S1 := { g : g in M | Order(g) eq 1 };
> #S1;
1
> #S1+#S2+#S3+#S4+#S5+#S6+#S8+#S11;
7920
```

The translates of a subset of a group

Let G be a group and W a subset of G. If $x \in G$ define

$$Wx = \{\, wx \mid w \in W \,\}$$

and

$$xW = \{\, xw \mid w \in W \,\}.$$

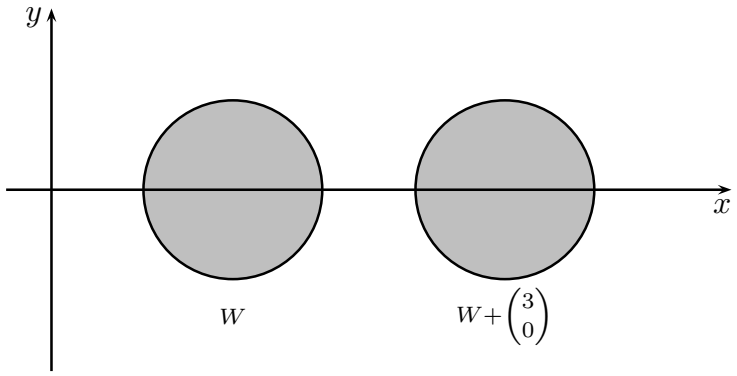
Thus Wx is the set of all elements of G obtained by multiplying elements of W by x, on the right hand side. The set Wx is called the *right translate* of W by x. Similarly, xW is called a *left translate* of W. Note that when G is Abelian, the right translates and left translates of W are the same; however, when G is not Abelian they need not be.

Example 1. Let $G = \mathbb{R}^2$, considered as a group under addition, and let

$$W = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \;\middle|\; (x-2)^2 + y^2 < 1 \right\}.$$

The diagram below shows the set W and the set $W + \begin{pmatrix} 3 \\ 0 \end{pmatrix}$, where we have identified $\mathbb{R}^2$

with the Euclidean plane in the usual way. The set $W + \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ is obtained by moving, or translating, W three units to the right.



Example 2. Let $G = \mathbb{R}^2$ again, and this time let W be the y-axis: the set of all points with zero x-coordinate. Then

$$W + \begin{pmatrix} a \\ b \end{pmatrix} = \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix} \;\middle|\; y \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} a \\ y' \end{pmatrix} \;\middle|\; y' \in \mathbb{R} \right\},$$

a line parallel to the y-axis. Observe that in this case no two distinct right translates of W have any points in common. We shall show later that the translates of a subgroup always have this property, whereas distinct translates of other subsets can have points in common.

Example 3. Let $G = \mathrm{Sym}(4)$ and let H be the subset of G consisting of all permutations $\sigma \in G$ such that $4^\sigma = 4$. It is easy to find all the elements of H; indeed,

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

The right translate $H(1,4) = \{\, h(1,4) \mid h \in H \,\}$ is found to be

$$\{(1,4), (1,2,4), (1,3,4), (1,4)(2,3), (1,2,3,4), (1,3,2,4)\}.$$

Proposition. *Let W be a finite subset of the group G, and let x be any element of G. Then the sets W and Wx have the same number of elements.*

Proof. Consider the function $\Phi\colon W \to Wx$ defined by $\Phi(w) = wx$ for all $w \in W$. It is immediate from the definition of Wx that Φ is onto: if z is an arbitrary element of Wx then $z = wx = \Phi(w)$ for some $w \in W$. Furthermore, Φ is also one-to-one. To see this, suppose that w_1, $w_2 \in W$ satisfy $\Phi(w_1) = \Phi(w_2)$. Then $w_1 x = w_2 x$. Multiplying both sides of this equation on the right by x^{-1} gives $w_1 x x^{-1} = w_2 x x^{-1}$, and so

$$w_1 = w_1 e = w_1 x x^{-1} = w_2 x x^{-1} = w_2 e = w_2.$$

Thus we have shown that for all w_1, $w_2 \in W$, if $\Phi(w_1) = \Phi(w_2)$ then $w_1 = w_2$; that is, Φ is one-to-one, as claimed.

Since the function Φ is one-to-one and onto it establishes a one-to-one correspondence between the sets W and Wx. So the sets W and Wx have the same number of elements. □

We remark that for infinite sets A and B it is usual to intepret the statement that A and B have the same number of elements as meaning that it is possible to find a one-to-one correspondence between the two sets. Thus in the proposition above the assumption that W is finite is unnecessary: the proof as given applies equally well when W is infinite. However, in this course we do not wish to become involved with the theory of infinite numbers, and so most of the time we shall consider only finite groups.

Let G be a finite group. We shall investigate the following question: given a fixed subset W of G, how many distinct right translates of W are there?

Example. Let G and H be as in Example 3 above. It turns out that there are exactly four distinct sets of the form Hx, where $x \in G$. There are 24 possible choices for the element x, since G has 24 elements, but the corresponding sets Hx are not all distinct from one another. Indeed, each of the four translates occurs for six different values of x, as indicated in the table below. In each row of the table the elements of Wx are listed in the order $\mathrm{id}\,x$, $(1,2)x$, $(1,3)x$, $(2,3)x$, $(1,2,3)x$, $(1,3,2)x$. But a set is not altered by re-ordering its elements, and it can be seen that the first six values of x below give the same set Wx, as do the next six, and so on.

Wx						x
{ id	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$ }	id
{ $(1,2)$	id	$(1,3,2)$	$(1,2,3)$	$(1,3)$	$(2,3)$ }	$(1,2)$
{ $(1,3)$	$(1,2,3)$	id	$(1,3,2)$	$(1,2)$	$(2,3)$ }	$(1,3)$
{ $(2,3)$	$(1,3,2)$	$(1,2,3)$	id	$(1,3)$	$(1,2)$ }	$(2,3)$
{ $(1,2,3)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	id }	$(1,2,3)$
{ $(1,3,2)$	$(2,3)$	$(1,2)$	$(1,3)$	id	$(1,2,3)$ }	$(1,3,2)$
{ $(1,4)$	$(1,2,4)$	$(1,3,4)$	$(1,4)(2,3)$	$(1,2,3,4)$	$(1,3,2,4)$ }	$(1,4)$
{ $(1,2,4)$	$(1,4)$	$(1,3,2,4)$	$(1,2,3,4)$	$(1,4)(2,3)$	$(1,3,4)$ }	$(1,2,4)$
{ $(1,3,4)$	$(1,2,3,4)$	$(1,4)$	$(1,3,2,4)$	$(1,2,4)$	$(1,4)(2,3)$}	$(1,3,4)$
{$(1,4)(2,3)$	$(1,3,2,4)$	$(1,2,3,4)$	$(1,4)$	$(1,3,4)$	$(1,2,4)$ }	$(1,4)(2,3)$
{ $(1,2,3,4)$	$(1,3,4)$	$(1,4)(2,3)$	$(1,2,4)$	$(1,3,2,4)$	$(1,4)$ }	$(1,2,3,4)$
{ $(1,3,2,4)$	$(1,4)(2,3)$	$(1,2,4)$	$(1,3,4)$	$(1,4)$	$(1,2,3,4)$ }	$(1,3,2,4)$
{ $(2,4)$	$(1,4,2)$	$(1,3)(2,4)$	$(2,3,4)$	$(1,4,2,3)$	$(1,3,4,2)$ }	$(2,4)$
{ $(1,4,2)$	$(2,4)$	$(1,3,4,2)$	$(1,4,2,3)$	$(2,3,4)$	$(1,3)(2,4)$}	$(1,4,2)$
{$(1,3)(2,4)$	$(1,4,2,3)$	$(2,4)$	$(1,3,4,2)$	$(1,4,2)$	$(2,3,4)$ }	$(1,3)(2,4)$
{ $(2,3,4)$	$(1,3,4,2)$	$(1,4,2,3)$	$(2,4)$	$(1,3)(2,4)$	$(1,4,2)$ }	$(2,3,4)$
{ $(1,4,2,3)$	$(1,3)(2,4)$	$(2,3,4)$	$(1,4,2)$	$(1,3,4,2)$	$(2,4)$ }	$(1,4,2,3)$
{ $(1,3,4,2)$	$(2,3,4)$	$(1,4,2)$	$(1,3)(2,4)$	$(2,4)$	$(1,4,2,3)$ }	$(1,3,4,2)$
{ $(3,4)$	$(1,2)(3,4)$	$(1,4,3)$	$(2,4,3)$	$(1,2,4,3)$	$(1,4,3,2)$ }	$(3,4)$
{$(1,2)(3,4)$	$(3,4)$	$(1,4,3,2)$	$(1,2,4,3)$	$(2,4,3)$	$(1,4,3)$ }	$(1,2)(3,4)$
{ $(1,4,3)$	$(1,2,4,3)$	$(3,4)$	$(1,4,3,2)$	$(1,2)(3,4)$	$(2,4,3)$ }	$(1,4,3)$
{ $(2,4,3)$	$(1,4,3,2)$	$(1,2,4,3)$	$(3,4)$	$(1,4,3)$	$(1,2)(3,4)$}	$(2,4,3)$
{ $(1,2,4,3)$	$(1,4,3)$	$(2,4,3)$	$(1,2)(3,4)$	$(1,4,3,2)$	$(3,4)$ }	$(1,2,4,3)$
{ $(1,4,3,2)$	$(2,4,3)$	$(1,2)(3,4)$	$(1,4,3)$	$(3,4)$	$(1,2,4,3)$ }	$(1,4,3,2)$

The subset H in this example is in fact a subgroup of G. So if $x \in H$ then it follows from the fact that H is closed under multiplication that $hx \in H$ for all $h \in H$. Thus the set $Hx = \{\, hx \mid h \in H \,\}$ must be a subset of H. But the proposition we proved earlier tells us that Hx has the same number of elements as H, which in this case is 6. So $Hx = H$ whenever $x \in H$. The first six rows of the table confirm this.

More generally, it can be checked from the table that $Hy = Hx$ whenever $y \in Hx$. Thus, for example, the six elements of $H(1,4)$ are $(1,4)$, $(1,2,4)$, $(1,3,4)$, $(1,4)(2,3)$, $(1,2,3,4)$ and $(1,3,2,4)$, and the table indicates that

$$H(1,4) = H(1,2,4) = H(1,3,4) = H(1,4)(2,3) = H(1,2,3,4) = H(1,3,2,4).$$

We shall show later that this property ($Hy = Hx$ whenever $y \in Hx$) holds in general whenever H is a subgroup of G.

If W is a nonempty subset of a group G we define the *right-stabilizer* of W to be the set $\mathrm{Stab}(W) = \{\, g \in G \mid Wg = W \,\}$.

Proposition. *Let G be a group, and let W be a nonempty subset of G. Then* $\mathrm{Stab}(W)$ *is a subgroup of G.*

Proof. Let e be the identity element of G. Obviously $We = \{\, we \mid w \in W \,\} = W$; so $e \in \mathrm{Stab}(W)$. Thus (SG2) holds for $\mathrm{Stab}(W)$.

Let x, $y \in \mathrm{Stab}(W)$ be arbitrary. Then $Wx = W$ and $Wy = W$. It follows easily from associativity of multiplication that $W(xy) = (Wx)y$; so

$$W(xy) = (Wx)y = Wy = W,$$

and we conclude that $xy \in \mathrm{Stab}(W)$. We have shown that the product of any pair of elements of $\mathrm{Stab}(W)$ is always an element of $\mathrm{Stab}(W)$; that is, (SG1) holds.

Let $x \in \mathrm{Stab}(W)$ be arbitrary. Then $W = Wx$, and so

$$Wx^{-1} = (Wx)x^{-1} = W(xx^{-1}) = We = W.$$

Thus $x^{-1} \in \mathrm{Stab}(W)$. Since this holds for all $x \in \mathrm{Stab}(W)$, we have shown that (SG3) holds.

Since (SG1), (SG2) and (SG3) all hold, $\mathrm{Stab}(W)$ is a subgroup of G, as required. □

Example. Let G be a cyclic group of order 6, generated by t. Thus $G = \{e, t, t^2, t^3, t^4, t^5\}$, with $t^6 = t^0 = e$. Let $W = \{t, t^3, t^4, t^5\}$. Multiplying on the right by t we find that

$$\begin{aligned} We &= \{t, t^2, t^4, t^5\}, \\ Wt &= \{t^2, t^3, t^5, e\}, \\ Wt^2 &= \{t^3, t^4, e, t\}, \\ Wt^3 &= \{t^4, t^5, t, t^2\}, \\ Wt^4 &= \{t^5, e, t^2, t^3\}, \\ Wt^5 &= \{e, t, t^3, t^4\}. \end{aligned}$$

Thus we see that $\mathrm{Stab}(W) = \{e, t^3\}$. It is trivial to confirm directly that this is a subgroup of G, the principal point being that $t^3 t^3 = e$.

We need a notation for the number of elements in a set, and for convenience we shall adopt MAGMA's notation.

Notation. If S is a finite set then $\#S$ denotes the number of elements of S.

Recall that we are seeking a general method of determining the number of right translates that there are for a given nonempty subset W of a finite group G. For every $x \in G$ there is a right translate, Wx, but we have seen by example that the number of distinct sets Wx is not necessarily the same as the number of choices for x, since repetitions can occur. To obtain the correct answer for the number of distinct sets Wx we need to determine precisely how much repetition there is.

Let x, $y \in G$. If $Wx = Wy$ then right-multiplying by x^{-1} gives $Wxx^{-1} = Wyx^{-1}$, and thus

$$W = We = Wxx^{-1} = Wyx^{-1}.$$

Conversely, if $W = Wyx^{-1}$ then right-multiplying by x gives

$$Wx = Wyx^{-1}x = Wye = Wy.$$

So $Wx = Wy$ if and only if $Wyx^{-1} = W$. Since $\mathrm{Stab}(W)$ is the set of all elements s such that $Ws = W$, we see that $Wx = Wy$ if and only if $yx^{-1} = s$ for some $s \in \mathrm{Stab}(W)$. But $yx^{-1} = s$ implies $y = sx$ (right-multiplying by x), and conversely $y = sx$ implies $yx^{-1} = s$ (right-multiplying by x^{-1}). So we have proved the following fact, valid for all x, $y \in G$:

$$Wy = Wx \text{ if and only if } y = sx \text{ for some } s \in \mathrm{Stab}(W). \tag{1}$$

If x is fixed then the number of distinct elements of G of the form sx for some $s \in \mathrm{Stab}(W)$ is precisely $\#\mathrm{Stab}(W)$, since if $s_1x = s_2x$ then right-multiplying by x^{-1} gives $s_1 = s_2$. So it follows from (1) above that for each $x \in G$ there are precisely $\#\mathrm{Stab}(W)$ elements $y \in G$ such that $Wy = Wx$. So now we know precisely how much repetition there is: as x runs through all the elements of G, each distinct set Wx occurs $\#\mathrm{Stab}(W)$ times. So the number of such sets is $\#G$, the number of choices for x, divided by $\#\mathrm{Stab}(W)$, the number of times each separate translate is obtained. Thus we have proved the following theorem.

Theorem. *If W is a nonempty subset of the finite group G, then the number of right translates of W in G is $\#G/\#\mathrm{Stab}(W)$, where $\mathrm{Stab}(W)$ is the right-stabilizer of W in G.*

Example 1. In the last example above, we had $G = \{e, t, t^2, t^3, t^4, t^5\}$, so that $\#G = 6$, and we found (for the set W under discussion) that $\mathrm{Stab}(W) = \{e, t^3\}$, so that $\#\mathrm{Stab}(W) = 2$. According to the above theorem we should find that $\#W$ has exactly $6/2 = 3$ right translates. Our calculations above do indeed confirm this: the three distinct translates of W are

$$\begin{aligned} We = Wt^3 &= \{t, t^2, t^4, t^5\}, \\ Wt = Wt^4 &= \{e, t^2, t^3, t^5\}, \\ Wt^2 = Wt^5 &= \{e, t, t^3, t^4\}. \end{aligned}$$

Example 2. With G as above, let $W = \{e, t^2, t^4\}$. We find that

$$\begin{aligned} We &= \{e, t^2, t^4\}, \\ Wt &= \{t, t^3, t^5\}, \\ Wt^2 &= \{t^2, t^4, e\} = We, \\ Wt^3 &= Wet = Wt, \\ Wt^4 &= Wt^2 = We, \\ Wt^5 &= Wet = Wt. \end{aligned}$$

Thus $\mathrm{Stab}(W) = \{e, t^2, t^4\}$ has three elements, and $\#G/\#\mathrm{Stab}(W) = 6/3 = 2$. So according to the theorem there should be exactly two right translates of W, and indeed the calculations show that this is the case, the translates being $\{e, t^2, t^4\}$ and $\{t, t^3, t^5\}$.

In the second of these two examples we again had a situation in which the subset whose translates were being considered was in fact a subgroup. Examination of this example, as well as the earlier example dealing with the right translates of a subgroup of Sym(4), will confirm the following.

If W is a subgroup of G then

1) $\mathrm{Stab}(W) = W$,
2) *no two distinct right translates of W have any elements in common, and*
3) *every element of G lies in exactly one right translate of W.*

We shall prove later that this is true in all cases.

Cosets

The translates of a subgroup, being somewhat special, are given another name.

Definition. If W is a subgroup of the group G then the right trnslates of W by elements of G are called the *right cosets* of W in G. Similarly, the left translates of W by elements of G are called the *left cosets* of W in G.

Example. Let $G = \mathrm{Sym}(3)$. It is trivial to check that the set $K = \{\mathrm{id}, (1,2)\}$ is a subgroup of G. We determine the right cosets of K in G.

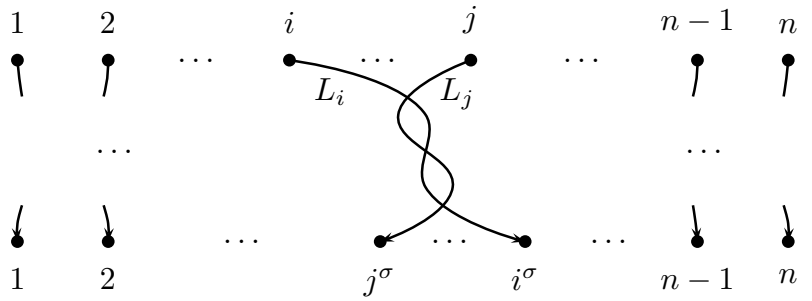
$$\begin{aligned} K = K\,\mathrm{id} &= \{\mathrm{id}, (1,2)\}, \\ K(1,3) &= \{\mathrm{id}\,(1,3),\ (1,2)(1,3) = \{(1,3),\ (1,2,3)\}, \\ K(2,3) &= \{\mathrm{id}\,(2,3),\ (1,2)(2,3) = \{(2,3),\ (1,3,2)\}. \end{aligned}$$

There are three cosets, with two elements each, accounting for all six elements of G.

The parity of a permutation

It is sometimes convenient to represent a permutation σ of $\{1, 2, \ldots, n\}$ by means of a diagram, constructed as follows: draw two rows of dots labelled 1, 2, ..., n, and for each i draw a line from the dot in the upper row labelled i to the dot in the lower row labelled i^σ.

Let us consider the number of times that lines in this diagram may cross. Consider, in particular, the lines that start at the points labelled i and j, where $i < j$. There are essentially two different situations that may arise: either $i^\sigma < j^\sigma$, or $j^\sigma < i^\sigma$. The following diagram illustrates the latter case.



The initial and final points of the line L_j joining j to j^σ are on opposite sides of the line L_i joining i to i^σ. Consequently L_i and L_j must cross each other an odd number of times. By altering the way the diagram is drawn it is possible to arrange that they only cross once, or that they cross 3 times, as in the diagram, or some larger odd number of times, but since their initial and final points are determined, the number of times they cross is inevitably odd. (The lines are not allowed to go outside the horizontal strip between the two rows of dots.)

A similar situation would arise if $i^\sigma < j^\sigma$, but in that case the number of times L_i and L_j cross would have to be even (possibly zero).

It follows that no matter how one redraws the diagram, the total number of times that lines cross each other can only be varied by an even number. If the total number of crossings is even, it remains even, and if the total number is odd it remains odd, no matter how one attempts to redraw the diagram.

Definition. We say that a permutation σ of $\{1, 2, \ldots, n\}$ is *even* if an associated diagram has an even number of line crossings, or *odd* if an associated diagram has an odd number of crossings. We define $\varepsilon(\sigma) = 1$ if σ is even, $\varepsilon(\sigma) = -1$ if σ is odd.

It is not hard to see that the following statement is equivalent to the definition given: σ is even if the total number of pairs (i, j) such that $i < j$ and $i^\sigma > j^\sigma$ is even, while σ is odd if the total number of such pairs is odd.