Lagrange's theorem

Lagrange's theorem relates the size of a subgroup of a group to the size of the group itself. It states that the order og a subgroup of a group must divide the order of the group. In more formal language

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

In symbols

If H is a subgoup of the finite group G, then $|H| \, \big| \, |G|$.

The symbol $|G|$ stands for the order of the group *G*, which is the number of distinct elements in the group *G*.

<u>Example (1)</u>

A group, *G*, has order 10. Show that all its non-trivial subgroups are cyclic.

Solution

By Lagrange's theorem the order of the possible subgroups of *G* are 1, 2, 5 and 10. The non-trivial subgroups of *G* are 2 and 5. Both 2 and 5 are prime numbers. All groups whose order is prime are cyclic. Therefore, all the non-trivial subgroups of *G* are cyclic.

<u>Example (2)</u>

Show that if *G* is a group with order *p*, where *p* is prime, then *G* cannot have any non-trivial subgroups.

Solution

By Lagrange's theorem, the order of a subgroup *H* of *G* must divide the order of *G*. Since *p* is prime, the only possible orders of *H* are 1 and *p*, which can not be orders of a proper subgroup of *G*. That is, there are no non-trivial subgroups of *G*.

© blacksacademy.net

Cosets and a Proof of Lagrange's Theorem

In order to prove Lagrange's theorem we need to define an object called a coset of *H* in *G*. We do this as follows

Let *G* be a group and *H* be a subgroup of *G*.

We write $H \leq G$ to signify that *H* is a subgroup of *G*.

For each element $g \in G$ and for each $h \in H$, form the element

$$gh$$

which is an element of G (by closure).

Let

$$gH = \{gh : h \in H\}$$

That is, let gH represent the set of every element in G formed by taking a fixed element g of G and combining it systematically with every distinct element $h \in H$.

This set is called a (left) coset of H in G.

Each element $g \in G$ gives rise to a coset gH in G.

Example (3)

Let S_3 denote the group of permutations of $\{1,2,3\}$. Let H be the subgroup consisting of the permutations

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

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

Find all the cosets of H in S_3.

Solution

© blacksacademy.net

The elements of S_3 are

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \textit{identity}$$

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \textit{cyclic permutation}$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \textit{cyclic permutation}$$

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \textit{swops } 2 \textit{ and } 3$$

$$q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \textit{swops } 1 \textit{ and } 2$$

$$q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \textit{swops } 1 \textit{ and } 2$$

The group table for this group is

	e	*a*	*b*	*p*	*q*	*r*
e	*e*	*a*	*b*	*p*	*q*	*r*
a	*a*	*b*	*e*	*q*	*r*	*p*
b	*b*	*e*	*a*	*r*	*p*	*q*
p	*p*	*r*	*q*	*e*	*b*	*a*
q	*q*	*p*	*r*	*a*	*e*	*b*
r	*r*	*q*	*p*	*b*	*a*	*e*

To illustrate the construction of this table, consider the element *pb*. This means *b* followed by *p*. Under *b*

© blacksacademy.net

$$1 \longrightarrow 3$$
$$2 \longrightarrow 1$$
$$3 \longrightarrow 2$$

Under p

$$1 \longrightarrow 1$$
$$2 \longrightarrow 3$$
$$3 \longrightarrow 2$$

Therefore, for pb we have

$$1 \xrightarrow{b} 3 \xrightarrow{p} 2$$
$$2 \xrightarrow{b} 1 \xrightarrow{p} 1$$
$$3 \xrightarrow{b} 2 \xrightarrow{p} 3$$

That is

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

which is q. That is

$$q = pb$$

The other entries are found similarly.

Now we find the cosets of H in S_3.

We have

$gH = \{gh : h \in H\}$ for all $g \in G$

and

$$H = \{e, p\}$$

© blacksacademy.net

For e $eH = \{ee, ep\} = \{e, p\} = H$

For a $aH = \{ae, ap\} = \{a, q\}$

For b $bH = \{be, bp\} = \{b, r\}$

For p $pH = \{pe, pp\} = \{p, e\}$

For q $qH = \{qe, qp\} = \{q, a\}$

For r $rH = \{re, rp\} = \{r, b\}$

Since

$\{\text{a,q}\} = \{q, a\}$

and

$\{b, r\} = \{r, b\}$

we have just three cosets of H in S_3 :

$H = \{e, p\}$

$L = \{a, q\}$

$M = \{b, r\}$

This illustrates that if x, y are distinct elements of G and H is a subgroup of G, then the cosets xH and yH are not necessarily distinct. We need a criterion for demonstrating when $xH = yH$.

This is given by,

if $x^{-1}y \in H$ then $xH = yH$

An equivalent to this is given by

if $y^{-1}x \in H$ then $xH = yH$

We will firstly show that

if $x^{-1}y \in H$ then $y^{-1}x \in H$

Let $x^{-1}y \in H$

then $\left(x^{-1}y\right)^{-1} \in H$ (by the existence of inverses, since H is a group)

then $y^{-1}\left(x^{-1}\right)^{-1} \in H$

then $y^{-1}x \in H$

© blacksacademy.net

We will also illustrate the meaning of this criterion for deciding when two cosets of a group are identical by looking again at our example.

Here,

$$aH = \{ae, ap\} = \{a, aa^{-1}q\} = \{a, q\}$$
$$qH = \{qe, ap\} = \{q, qq^{-1}a\} = \{q, a\}$$

The two cosets are identical because we can replace p by $a^{-1}q$ since $p = a^{-1}q$ in the first case, and p by $q^{-1}a$ since $p = q^{-1}a$ in the second case. This illustrates that if $x^{-1}y \in H$ then $xH = yH$.

We will now prove in general that

if $x^{-1}y \in H$ then $xH = yH$

Suppose $f \in xH$
then $f = xh$ for some $h \in H$
then $f = yy^{-1}xh$
but $y^{-1}x \in H$
that is $h' = y^{-1}x$
Therefore, $f = yh'h,$ where $h, h' \in H$
Therefore, $f \in yH$

Likewise, if $f \in yH$
then $f = yh,\ h \in H$
$f = xx^{-1}yh = xh''h,$ where $h, h'' \in H$
Therefore, $f \in xH$

This shows that if $x^{-1}y \in H$ then $xH \subseteq yH$ and $yH \subseteq xH$
Therefore, $xH = yH$.

The cosets of H in G form a partition of G. What this means is that if two cosets of H in G are not identical then they do not share any element in common. The proof of this is by contradiction. Thus, suppose

$xH \neq yH$

are two cosets of H in G, but that they share at least one element in common. Let this common element be t. That is

$t \in xH$ and $t \in yH$

Therefore,

$t = xh$ and $t = yh'$, where $h, h' \in H$.

Therefore,

$$xh = yh'$$
$$xh(h')^{-1} = y$$
$$h(h')^{-1} = x^{-1}y$$

That is,

$$x^{-1}y = h(h')^{-1}$$

Therefore,

$x^{-1}y \in H$ since $h(h')^{-1} \in H$

But we just showed that if $x^{-1}y \in H$ then $xH = yH$.

Hence, $xH = yH$
which contradicts $xH \neq yH$.

Thus, if two cosets of H in G share an element in common, then they must be completely identical. Hence, the cosets of H in G partition G. This means that every element of G is in one, and only one, coset of H in G.

The number of elements of each coset of H in G is the same. That is,

if xH is a coset of H in G then

$$|xH| = |H|$$

Their orders are the same.

This is because each coset is formed by taking an element g of G and combining it with each distinct element h of H. For each distinct h in H we get a different element gh in G. Indeed, if $g^{-1}(gh) = g^{-1}(gh')$ then $gh = gh'$ and thus $h = h'$ follows. Hence, there is a one-one correspondence between elements of H and elements of any coset xH of H in G.

© blacksacademy.net

Further, G is divided into a finite number of cosets xH of H in G.

Thus,

$$|G| = (\text{the number of cosets of } H \text{ in } G) \times |H|$$

(The order of G is equal to the product of the number of cosets of H in G, and the order of H.)

That is,

$$|H| \,\big|\, |G|$$

The order of H divides the order of G, which proves the theorem.

In summary, the outline of the proof is as follows

Let H be a subgroup of G. That is $H \leq G$

Then the cosets of H in G partition (divide up) G in such a way that

(1) each coset has exactly the same number of distinct elements as H.
(2) every element of G is in one and only one coset of H.

Hence,

$$|G| = (\text{the number of cosets of } H \text{ in } G) \times |H|$$

(The order of G is equal to the product of the number of cosets of H in G, and the order of H.)

which means that the order of any subgroup of G must divide the order of G.

© blacksacademy.net