COUNTING PRINCIPLE

Theorem 3.32. (Lagrange's theorem) Let G be a finite group of order n and H be any subgroup of G. Then the order of H divides the order of G.

Proof. Let $|H| = m$ and $[G : H] = r$.

Then the number of distinct left cosets of H in G is r.

By theorem 3.30, these r left cosets are mutually disjoint, they have the same number of elements namely m and their union is G.

$\therefore \quad n = rm$. Hence m divides n.

Corollary. $[G : H] = \dfrac{|G|}{|H|}$

Note 1. Lagrange's theorem has many important applications in group theory. For example, a group G of order 8 cannot have subgroups of order 3, 5, 6 or 7. In fact any proper subgroup of G must be of order 2 or 4.

Note 2. Any group of prime order has no proper subgroups.

Note 3. The converse of Lagrange's theorem is false. (i.e) If G is a group of order n and m divides n, then G need not have a subgroup of order m.

For example A_4 is a group of order 12 and it does not have a subgroup of order 6.

However there are groups in which the converse of Lagrange's theorem is true.

For example, consider S_3. This is a group of order 6. $\{e, p_4\}$ is a subgroup of order 2 and $\{e, p_1, p_2\}$ is a subgroup of order 3. Hence for every divisor m of 6, there is a subgroup of S_3 of order m.

Exercises

1. Can a group of order 12 contain a subgroup of order 8?
2. Show that the converse of Lagrange's theorem is true in V_4.
3. Show that the converse of Lagrange's theorem is true in any finite cyclic group.

If G is a finite gp $a \in G$, then $o(a) / o(G)$

Theorem 3.33. The order of any element of a finite group G divides the order of G.

Proof. Let G be a group of order n. Let $a \in G$ be an element of order m. Then the order of a is the same as the order of the cyclic group $\langle a \rangle$.

Now, by Lagrange's theorem the order of the subgroup $\langle a \rangle$ divides the order of G. Hence $m|n$.

Theorem 3.34. Every group of prime order is cyclic.

Proof. Let G be a group of order p where p is prime. Let $a \in G$ and $a \neq e$.

By Theorem 3.33 order of a divides p.

$\therefore$ Order of a is 1 or p.

Since $a \neq e$ order of a is p.

Hence $G = \langle a \rangle$ so that G is cyclic.

If G is a finite gp and $a \in G$ then $a^{o(G)} = e$.

Theorem 3.35. Let G be a group of order n. Let $a \in G$ then $a^n = e$.

Proof. Let the order of a be m. Then m divides n.

Hence $n = mq$.

$\therefore \quad a^n = a^{mq} = (a^m)^q = e^q = e.$

Theorem 3.36 (Euler's theorem) If n is any integer and $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

($\phi(n)$ is the number of positive integers less than n relatively prime to n)

Proof. Let $G = \{m / m < n \text{ and } (m, n) = 1\}$. G is a group under multiplication modulo n. (Refer example 24 of section 3.2). This group is of order $\phi(n)$.

Now, let $(a, n) = 1$.

Let $a = qn + r; 0 \leq r < n$ so that $a \equiv r (\text{mod } n)$.

Since $(a, n) = 1$ we have $(n, r) = 1$ so that $r \in G$.

$\therefore \quad r^{\phi(n)} = 1$ (by Theorem 3.35).

$\therefore \quad r^{\phi(n)} \equiv 1 (\text{mod } n)$.

Also $a^{\phi(n)} \equiv r^{\phi(n)} (\text{mod } n)$ so that

$a^{\phi(n)} \equiv 1 (\text{mod } n)$ (since '$\equiv$' is transitive).

Theorem 3.37 (Fermat's theorem) Let p be a prime number and a be any integer relatively prime to p. Then $a^{p-1} \equiv 1 (\text{mod } p)$.

Proof. Since p is prime, $\phi(p) = p - 1$ and hence the result follows from Euler's theorem.

Theorem 3.38. A group G has no proper subgroups if it is a cyclic group of prime order.

Proof. Suppose G is a group of prime order. Then it follows from Lagrange's theorem that G has no proper subgroups.

Conversely, let G be a group having no proper subgroup. First we shall prove that G is cyclic.

Suppose G is not cyclic. Let $a \in G$ and $a \neq e$.

Then the cyclic group $\langle a \rangle$ is a proper subgroup of G which is a contradiction. Hence G is cyclic.

Also G cannot be infinite, for, an infinite cyclic group contains a proper subgroup $\langle a^2 \rangle$. Hence G must be of finite order, say, n.

We claim that n is prime. If possible let n be a composite number. Let $n = pq$ where $p, q > 1$.

Let $a \in G$ be a generator of the group.

Then $\langle a^p \rangle$ is a subgroup of order q and hence is a proper subgroup of G which is a contradiction.

Hence n is prime.

$\therefore \quad G$ is a cyclic group of prime order.

Solved problems

Problem 1. Let A and B be subgroups of a finite group G such that A is a subgroup of B. Show that

$$[G : A] = [G : B][B : A].$$

Solution. $[G : A] = \dfrac{|G|}{|A|}$ (by Lagrange's theorem)

$$[G : B] = \frac{|G|}{|B|}$$

$$\text{and } [B : A] = \frac{|B|}{|A|}$$

$$\therefore \quad [G : B][B : A] = \frac{|G|}{|B|}\frac{|B|}{|A|} = \frac{|G|}{|A|} = [G : A].$$

Problem 2. Let A and B be two finite subgroups of a group G such that $|A|$ and $|B|$ have no common divisors. Then show that $A \cap B = \{e\}$.

Solution. $A \cap B$ is a subgroup of A and B.

$\therefore$ By Lagrange's theorem, $|A \cap B|$ divides $|A|$ and $|B|$. But by hypothesis $|A|$ and $|B|$ have no common divisors.

$\therefore \quad |A \cap B| = 1$. Hence $A \cap B = \{e\}$.

Problem 3. Let H and K be two subgroups of G of finite index in G. Prove that $H \cap K$ is a subgroup of finite index in G.

Solution. By theorem 3.19 $H \cap K$ is a subgroup of G.

Let $[G : H] = m$ and $[G : K] = n$.

We claim that for any $a \in G$, $(H \cap K)a = Ha \cap Ka$.

Clearly, $H \cap K \subseteq H$ and K.

$\therefore \quad (H \cap K)a \subseteq Ha$ and Ka.

$\therefore \quad (H \cap K)a \subseteq Ha \cap Ka$. ... (1)

Now, let $x \in Ha \cap Ka$.

$\therefore \quad x \in Ha$ and $x \in Ka$

$\therefore \quad x = ha$ for some $h \in H$ and

$x = ka$ for some $k \in K$.

$\therefore \quad x = ha = ka$

$\therefore \quad h = k$

$\therefore \quad h \in H \cap K$.

$\therefore \quad x \in (H \cap K)a$.

$\therefore \quad Ha \cap Ka \subseteq (H \cap K)a$. ... (2)

From (1) and (2) we have

$$(H \cap K)a = Ha \cap Ka.$$

$\therefore$ Every right coset of $H \cap K$ in G is the intersection of a right coset of H and a right coset of K.

Also since $[G : H] = m$, the number of right cosets of H in G is m.

Similarly the number of right cosets of K in G is n.

Hence the number of right cosets of $H \cap K$ in G is atmost mn.

$\therefore \quad [G : H \cap K] \leq mn$.

$\therefore \quad H \cap K$ is a subgroup of finite index in G.

Problem 4. Let H and K be two finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Let $L = H \cap K$. Since H and K are subgroups of G, L is also a subgroup of G and $L \subseteq H$ and K.

Now, let $Lx_1, Lx_2, \ldots\ldots, Lx_m$ be the distinct right cosets of L in K so that

$$K = Lx_1 \cup Lx_2 \cup \ldots\ldots \cup Lx_m \quad \ldots (1)$$

and

$$m = [K : L] = \frac{|K|}{|L|} = \frac{|K|}{|H \cap K|} \quad \ldots (2)$$

From (1)

$$HK = HLx_1 \cup HLx_2 \cup \ldots\ldots \cup HLx_m$$

$$= Hx_1 \cup Hx_2 \cup \ldots\ldots \cup Hx_m \text{ (since } L \subseteq H) \quad \ldots (3)$$

We claim that the cosets $Hx_1, Hx_2, \ldots\ldots, Hx_m$ are distinct.

Suppose $Hx_i = Hx_j$.

$\therefore \quad x_i x_j^{-1} \in H$

Also $x_i, x_j \in K$ and hence $x_i x_j^{-1} \in K$.

$\therefore \quad x_i x_j^{-1} \in H \cap K = L$,

Hence $Lx_i = Lx_j$ which is a contradiction since the cosets $Lx_1, Lx_2, \ldots\ldots, Lx_m$ are distinct.

Thus from (3) we have

$$|HK| = |Hx_1| + |Hx_2| + \ldots\ldots + |Hx_m|$$

$$= m|H|$$

$$= \frac{|H||K|}{|H \cap K|} \text{ by (2).}$$

Problem 5. Let H and K be two subgroups of a finite group G such that $|H| > \sqrt{|G|}$ and $|K| > \sqrt{|G|}$. Then $H \cap K \neq \{e\}$.

Proof. Suppose $H \cap K = \{e\}$.

$\therefore \quad |H \cap K| = 1$

$\therefore \quad |HK| = \frac{|H||K|}{|H \cap K|}$ (by Problem 4)

$$= |H||K|$$

$$> \sqrt{|G|}\sqrt{|G|} = |G|.$$

$\therefore \quad |HK| > |G|$ which is a contradiction.

$\therefore \quad H \cap K \neq \{e\}$.

Exercises

1. Show that any group of order 17 is cyclic.
2. Show that any infinite group has proper subgroups.
3. Prove that in an infinite cyclic group all the subgroups other than $\{e\}$ are infinite.