The Work of Lagrange in Number Theory and Algebra

D P Patil, C R Pranesachar and Renuka Ravindran

(left) D P Patil got his Ph.D from the School of Mathematics, TIFR and joined IISc in 1992. His interests are commutative algebra, algebraic geometry and algebraic number theory.

(right) C R Pranesachar is at HBCSE, TIFR. His Ph.D is in combinatorics His interests are enumeration and triangle geometry.

(center) Renuka Ravindran was on the faculty of the Department of Mathematics, IISc, Bangalore. She was also Dean, Science Faculty at IISc. She has been a visiting Professor at various universities in USA and Germany.

Keywords
Primes, 4-square theorem, binary operations, groups, subgroups, equivalence relations, cosets.

Joseph Louis Lagrange, a French mathematician, worked on a variety of topics – Algebra (classical and abstract), Number Theory, Dynamics, Functions of several variables, and Astronomy to mention a few. Here we give proofs of four theorems, three in number theory and one in group theory.

It is said that post-Newtonian mathematics was dominated by two giants, Lagrange and Euler, in the eighteenth century. While Euler mainly contributed to pure mathematics, Lagrange contributed equally to mathematical physics and pure mathematics. Lagrange had special love for the theory of numbers and theory of polynomials.

1. Theorems of Wilson and Fermat

In this section we give Lagrange's proofs of Wilson's theorem and Fermat's little theorem.

Theorem 1.1 *Let p be a prime number. Then*

(1) (*Wilson*) *p divides $(p-1)!+1$.*

(2) (*Fermat*) *For every integer a which is coprime to p, we have p divides $a^{p-1}-1$.*

Proof. If $p = 2$ the assertions are trivial. Let p be an odd prime.Consider the polynomial $(x-1)(x-2)\cdots(x-p+1)$ of degree $p-1$ in x. When expanded

$$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - A_1x^{p-2} + A_2x^{p-3} - \cdots + A_{p-1}, \quad (1)$$

where $A_1, \quad , A_{p-1}$ are positive integers. In fact, for $r = 1, \quad , p-1$, the coefficient A_r is the sum of products of $1, 2, \quad , p-1$ taken r at a time. Multiplying equation (1) by x and then replacing x by $x-1$, we get

$$\begin{aligned} & (x-1)^p - A_1(x-1)^{p-1} + \quad + A_{p-1}(x-1) \\ = \; & (x-1)(x-2) \quad (x-p) \\ = \; & (x-p)(x^{p-1} - A_1 x^{p-2} + \quad + A_{p-1}). \end{aligned}$$

Equating coefficients of like powers of x, we have

$$\binom{p}{1} + A_1 = p + A_1$$

$$\binom{p}{2} + \binom{p-1}{1} A_1 + A_2 = pA_1 + A_2,$$

$$\binom{p}{3} + \binom{p-1}{2} A_1 + \binom{p-2}{1} A_2 + A_3 = pA_2 + A_3$$

Here the first relation is an identity. The others successively give us

$$A_1 = \binom{p}{2}, 2A_2 = \binom{p}{3} + \binom{p-1}{2} A_1,$$

$$3A_3 = \binom{p}{4} + \binom{p-1}{3} A_1 + \binom{p-2}{2} A_2,$$

$$(p-1)A_{p-1} = 1 + A_1 + A_2 + \quad + A_{p-2}.$$

Therefore we infer in succession that $p|A_1$, $p|A_2$, ., $p|A_{p-2}$ and finally $(p-1)A_{p-1} \equiv 1 \pmod{p}$. Since $A_{p-1} = (p-1)!$, we get $(p-1)! \equiv -1 \pmod{p}$. This proves Wilson's theorem.

Further, if we susbsitute $x = a$ which is not a multiple of p in equation (1) and read it modulo p, we conclude that $0 \equiv a^{p-1} - 1 \pmod{p}$, since $p|A_r$ for every $r = 1, \quad , p-2$ and $A_{p-1} \equiv -1 \pmod{p}$. This proves Fermat's theorem.

A positive integer p greater than 1 is called a prime if its only divisors are 1 and itself. The sequence of primes begins with 2,3,5,7,11,.... There are 25 primes less than 100.

If a and b are two integers and m is a positive integer, we say a is congruent to b modulo, and write $a \equiv b \pmod{m}$ if m divides $a-b$.

Examples 1.2. (1) Taking $p = 7$ we see that $(7-1)!+1 = 721$ which is divisible by 7. This demonstrates Wilson's theorem. □

(2) Taking $p = 7$ and $a = 3$ we see that $3^6 - 1 = 728$ which is divisible by 7. This verifies Fermat's theorem.

Remark 1.3. If $n > 1$ and n divides $(n-1)!+1$, then it is an easy exercise to see that n is a prime. Therefore the converse of Wilson's theorem is also true. On the other hand, the converse of Fermat's theorem is not true, i.e., *if n is a positive integer and $a^{n-1} \equiv 1 \pmod{n}$ for every integer a, coprime to n, then n need not be a prime*! For example, one can verify that $n = 561 = 3 \cdot 11 \cdot 17$ is such a number. Such composite numbers are called *Carmichael numbers.*

2. Lagrange's Four-Square Theorem

In this section we shall prove one of the most famous theorems in Number Theory, which states: *Every positive integer is a sum of at most four square integers.* This statement was known to mathematicians such as Euler before Lagrange, but it was Lagrange who gave the first complete proof.

For example, $7 = 2^2 + 1^2 + 1^2 + 1^2$, $66 = 8^2 + 1^2 + 1^2$. It is an interesting exercise to prove that numbers of the form $4^k(8n + 7)$, $k \geq 0$, $n \geq 0$ cannot be expressed as sums of less than 4 squares.

Before proving the theorem, we digress a little bit. There is a two-square theorem attributed to another French mathematician Pierre de Fermat (1601-1665), which states that *a prime of the form $4k+1$ is a sum of two square integers in a unique way.*

For example, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $29 = 2^2 + 5^2$, $97 = 4^2 + 9^2$. The proof of Fermat's two-square theorem is not easy. But it is much easier to prove that a prime (or for that matter any positive integer) of the

form $4k+3$ is never a sum of two square integers. Of course the only even prime 2 is also a sum of two square integers: $2 = 1^2+1^2$. Such theorems belong to the realm of 'additive' number theory. Another famous theorem due to Gauss is that *an integer that is not of the form* $4^k(8n+7)$, $k \geq 0$, $n \geq 0$ *is a sum of at most three square integers.* For example, $11 = 1^2+1^2+3^2$, $19 = 1^2+3^2+3^2$. Waring's problem concerns expresing any positive integer as a sum of a minimum but fixed number of kth powers. This fixed number is denoted by $g(k)$. Thus Lagrange's 4-square theorem asserts that: $g(2) = 4$. The value of $g(3)$ is known to be 9.

We shall go through a few lemmas to prove our main theorem of this section.

Lemma 2.1. *A product of two expressions each of the form* $a^2+b^2+c^2+d^2$ *is again of the same form.*

Proof. Clearly,

$$(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) =$$

$$(ap+bq+cr+ds)^2+(aq-bp+cs-dr)^2+$$
$$(ar-cp-bs+dp)^2+(as-dp+br-cq)^2.$$

One can prove this by taking the determinants on both sides of the matrix identity

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} =$$

$$\begin{pmatrix} z_1z_2 - w_1\overline{w_2} & z_1w_2 + w_1\overline{z_2} \\ -\overline{z_1w_2} - z_2\overline{w_1} & \overline{z_1z_2} - \overline{w_1}w_2 \end{pmatrix}$$

where $z_1 = a+ib$, $w_1 = c+id$, $z_2 = p-iq$ and $w_2 = -r-is$ are complex numbers.

Note that all the three matrices involved are of the form $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$, whose determinant is $|z|^2+|w|^2$, z, w being complex numbers. □

In view of the above lemma, it is enough to prove our theorem for odd primes only as any positive integer is a product of primes and $2 = 1^2 + 1^2$.

Lemma 2.2. *If p is an odd prime, then there exist integers x, y such that p divides $1 + x^2 + y^2$. Moreover, we may choose x, y so that if $1 + x^2 + y^2 = mp$, then $0 < m < p$.*

Proof. Consider the numbers of the form $1 + x^2$, where x takes the values $0, 1, \quad (p-1)/2$. We claim that the remainders obtained when all these $(p+1)/2$ numbers are divided by p are distinct. For, if $1 + x^2 \equiv 1 + x_1^2 \pmod{p}$ for two such distinct values x and x_1, then p divides $(x - x_1)(x + x_1)$. But $x + x_1 < p$, so either $x + x_1 = 0$ or else $x = x_1$. Neither case is possible. This proves the claim. Similarly, the $(p+1)/2$ numbers of the form $-y^2$, where y takes the values $0, 1, \quad (p-1)/2$, also leave distinct remainders when divided by p. But altogether there are $p + 1$ remainders from both the collections:

$$1 + x^2, \qquad x = 0, 1, 2, \qquad (p-1)/2 \quad \text{and}$$

$$-y^2 \qquad y = 0, 1, 2, \qquad (p-1)/2.$$

Since only p distinct remainders are possible, some remainder is common to both of these collections, say corresponding to $x = x_1$ and $y = y_1$. Therefore $1 + x_1^2 + y_1^2$ is divisible by p. Further, for this pair, if $1 + x_1^2 + y_1^2 = mp$, then

$$0 < 1 + x_1^2 + y_1^2 \leq 1 + ((p-1)/2)^2 + ((p-1)/2)^2$$

$$< p^2/4 + p^2/4 < p^2.$$

This means that $0 < mp < p^2$, whence $0 < m < p$. This proves the lemma. □

Example 2.3. Let $p = 11$. Then the numbers

$$1 + 0^2 \;\; 1 + 1^2, 1 + 2^2 \;\; 1 + 3^2, 1 + 4^2, 1 + 5^2$$

when divided by 11 leave respectively $(11+1)/2 = 6$ distinct remainders

$$1, 2, 5, 10, 6, 4.$$

Similarly, the numbers

$$-0^2, -1^2, -2^2, -3^2, -4^2, -5^2$$

upon division by 11 leave the remainders (note that remainders are by definition non-negative)

$$0, 10, 7, 2, 6, 3.$$

Hence we may take the pair (x, y) to be any one of the three: $(1,3), (3,1), (4,4)$. But the first two pairs are essentially the same and hence we have two possibilities $(1,3), (4,4)$. In both cases 11 divides $1 + x^2 + y^2$ and the quotients are strictly less than 11 as asserted in lemma 2.2.

We shall need one more lemma before the final assault.

Lemma 2.4. *If p is an odd prime and m is an even positive integer such that mp is a sum of four squares, then $(m/2)p$ is also a sum of four squares.*

Proof. If $mp = a^2 + b^2 + c^2 + d^2$, then as m is even, the following three cases arise:

(i) a, b, c, d are all even; or (ii) a, b, c, d are all odd; or (iii) two of a, b, c, d are even and the other two are odd: say a, b are even and c, d are odd.

Thus in all cases $a+b, a-b, c+d, c-d$ are all even. and hence

$$\frac{mp}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

proving our assertion. □

Remark 2.5. If further $m/2$ is also even then from the above lemma we see that $(m/4)p$ is also a sum of

four squares, and so on. Hence, in general, if $m = 2^k m_1$, where m_1 is odd, we can conclude by iteration that $m_1 p$ is a sum of four squares.

We now come to the proof of Lagrange's four-square theorem. The proof is by 'descent', a common method used to prove several results especially in number theory.

Theorem 2.6. *(Lagrange's Four-square Theorem) Every positive integer is a sum of at most four square integers.*

Proof. Let p be an odd prime. then by Lemma 2.2 we may assume that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2, \tag{2}$$

where $0 < m < p$. (If a number is a sum of three squares, then it is a sum of four squares as well!) Let m be the least such positive number for which (2) holds. Then by Lemma 2.4, we may further assume that m is odd. If $m = 1$, then there is nothing to prove. So assume that $1 < m < p$. Since $m \geq 3$ and not all of x_1, x_2, x_3, x_4 are divisible by p (why?), we may assume by the division algorithm that

$$x_j = mb_j + y_j, \qquad j = 1, 2, 3, 4,$$

where $|y_j| < m/2$ and $y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$. Then $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(m/2)^2 = m^2$, and $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}$.

Therefore

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m, \tag{3}$$

where $0 < m_1 < m$. Multipling equations (2) and (3), and using Lemma 2.1 we get

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m^2 m_1 p,$$

for some suitable numbers z_1, z_2, z_3, z_4, given by $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, etc. But then $z_1 = \sum_{i=1}^4 x_i y_i =$

$\sum_{i=1}^{4} x_i(x_i - b_i m) \equiv 0 \pmod{m}$; and likewise z_2, z_3, z_4 are each divisible by m. Hence writing $z_i = mt_i$, we get

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p.$$

As $0 < m_1 < m$, we have a contradiction to the minimality of m. This proves that $m = 1$, and the theorem is proved. □

The reader may pause for a while here and debate on the point whether the proof given above is existential or constructive! Essentially a proof along similar lines yields Fermat's two-square theorem stated in Section 2. For a proof of this, the reader may go through the following steps:

(i) A sum of two squares times another sum of two squares is again a sum of two squares.

(ii) If p is a prime of the form $4k + 1$, then p divides $1 + x^2$ for some integer x. Further, we may choose x so that if $1 + x^2 = mp$, then $0 < m < p$. To prove this one has to use judiciously Wilson's theorem proved in Section 1. For instance, try $x = ((p-1)/2)!$.

(iii) If $x^2 + y^2 = mp$, where p is a prime and $1 < m < p$, then $x_1^2 + y_1^2 = m_1 p$, with x_1, y_1 integers and $0 < m_1 < m$.

It may be remarked here that both Lagrange's four-square theorem and Fermat's two-square theorem have several proofs. One may find as many as four proofs of the latter and three proofs of the former in [1].

3. Lagrange's Theorem in Group Theory

In this section we shall prove a well-known theorem in elementary group theory which is generally attributed to Lagrange. He was led to the assertion of this theorem after being inspired by the study of roots of polynomial equations. The modern formulation with proof is presented here.

A fundamental algebraic concept is that of a binary operation on a set. A *binary operation* on a set X is a map $X \times X \to X$ usually denoted either by $(x, y) \mapsto xy$ in the multiplicative notation or by $(x, y) \mapsto x + y$ in the additive notation. The other notations $x * y$, $x \circ y$, $x \sqcap y$, $x \sqcup y$, are also used. For example, on the sets $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$, $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}$, $\mathbb{R}$ and $\mathbb{C}$ of natural numbers, integers, rational numbers, real numbers and complex numbers respectively, the usual addition $+$ and the usual multiplication are binary operations. On the power set $\mathfrak{P}(X) = \{A \mid A \subseteq X\}$ of a set X the union $\cup$, the intersection $\cap$ and the symmetric difference Δ are binary operations. On the sets X^X of maps from X into itself and the set $\mathfrak{S}(X) = \{f \in X^X \mid f \text{ is bijective}\}$ of permutations of X the composition $\circ$ of maps is a binary operation.

With the above examples in mind, we abstract and make the following definitions.

A binary operation $G \times G \to G$, $(x, y) \mapsto xy$, is *commutative* or *abelian* if $xy = yx$ for all $x, y \in G$. The operation is *associative* if $(xy)z = x(yz)$ for all $x, y, z \in G$.

Definitions 3.1. Let G be a set with a binary operation $G \times G \to G$. We shall use the multiplicative notation, i.e., use $(x, y) \mapsto xy$ to denote the given binary operation.

(1) An element $e \in G$ is called a *identity (*or *neutral) element* if $ex = xe = x$ for all $x \in G$. (If neutral element exists, then it is unique: $e = ee' = e'$.)

(2) G is called a *monoid* if the binary operation of G is associative and has a neutral element.

(3) Suppose that G is a monoid with neutral element e. An element $x' \in G$ is called an *inverse* of $x \in G$ if $xx' = x'x = e$. For example, e is an inverse of e. If the

element $x \in G$ has an inverse in G, then it is unique: if x' and x'' are inverses of x, then $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$. If the inverse of $x \in G$ exists, then in the multiplication notation it is denoted by x^{-1} and in the additive notation it is denoted by $-x$. Similarly, the neutral element $e \in G$ is denoted by 1_G or simply 1 in the multiplicative notation and by 0_G or simply by 0 in the additive notation. Therefore $xx^{-1} = x^{-1}x = 1$ in the multiplicative notation and $x+(-x) = (-x)+x = 0$ in the additive notation.

(4) An element of a monoid G is called *invertible* or an *unit* if x has an inverse in G. If $x, y \in G$ are two invertible elements in a monoid G, then x^{-1} and xy are also invertible in G. Moreover, $(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1}x^{-1}$. Therefore, the binary operation of the monoid G induces a binary operation on the subset $G^\times = \{x \in G \mid x \text{ is invertible}\}$ of all invertible elements in G; therefore $G^\times \times G^\times \to G^\times$ is an associative binary operation on $G^\times$, the neutral element $e \in G^\times$ and every element in $G^\times$ has an inverse in $G^\times$.

(5) A monoid G is called a *group* if $G^\times = G$, i.e., if every element of G has an inverse in G.

(6) A group G is called *commutative* or *abelian* if the binary operation of G is commutative.

(7) A group G is called finite if the set G has finitely many elements. In this case the number of elements in G is called the *order* of G and is denoted by $\mathrm{ord}(G)$.

We now list some examples which illustrate the above concepts.

Examples 3.2. (1) The additive monoids $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are groups, but the monoids $(\mathbb{N}, +)$, $(\mathbb{N}^\times, \cdot)$, $(\mathbb{Z}, \cdot)$ are not groups; in fact $(\mathbb{N}, +)^\times = \{0\}$, $(\mathbb{N}^* \cdot)^\times = \{1\}$, $(\mathbb{Z}, \cdot)^\times = \{\pm 1\}$, where $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. However, the monoids $(\mathbb{Q}^* \cdot)$, $(\mathbb{R}^* \cdot)$, $(\mathbb{C}^*, \cdot)$, where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are groups.

(2) Let X be any set. Then the monoids $(X^X, \circ)$ and $(\mathfrak{S}(X), \circ)$ are not commutative if X has more than 2 elements. Moreover, the monoid $(X^X, \circ)$ is not a group and the group $(\mathfrak{S}(X), \circ) = (X^X, \circ)^\times$ of invertible elements of $(X^X, \circ)$ is called the *permutation group* of X; its elements are precisely the bijective maps from X onto itself and are called the *permutations* of X It is not difficult to prove that the permutation group $\mathfrak{S}(X)$ of a finite set X with n elements is a finite group of order $n!$.

We shall now introduce the most natural subsets of a group G which reflect the fact that G has an algebraic structure imposed on it.

Definition 3.3. A non-empty subset H of a group G is called a *subgroup* of G if under the binary operation of G, H itself forms a group. It is easy to check that a non-empty subset H of a group G is a subgroup G if and only if $xy \in H$ and $x^{-1} \in H$ whenever $x, y \in H$ In the special case of a finite group G the situation is nicer: a non-empty subset H of a finite group G is a subgroup of G if and only if H is closed under multiplication in G.

We give some examples of some subgroups in some groups. The whole group G and the singleton $\{e\}$ are clearly subgroups of a group G, these are called *trivial subgroups*. The non-trivial subgroups are the most interesting objects in the study of groups.

Examples 3.4. (1) In the additive group $(\mathbb{Z}, +)$, the subset $n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$ of all multiples of n is a subgroup of $(\mathbb{Z}, +)$ for every $n \in \mathbb{Z}$. More generally, in any group G, the subset $H(x) = \{x^r \mid r \in \mathbb{Z}\}$ of all integral powers of x forms a subgroup of G and is called the *cyclic subgroup generated by* x. This provides means of producing subgroups of G. If $G = \mathrm{H}(x)$ for some $x \in G$, then we say that G is a *cyclic group* and the

element x is called a *generator* of G. For example, the group $(\mathbb{Z}, +)$ is cyclic with a generator 1; note that -1 is also a generator, but the groups $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are not cyclic (why?). Cyclic groups are very special and play an important role in the theory of groups.

(2) Let X be any set and let $x_0 \in X$ Then in the permutation group $\mathfrak{S}(X)$, the subset $F(x_0) = \{\sigma \in \mathfrak{S}(X) \mid \sigma(x_0) = x_0\}$ of all permutations of X which fix x_0 is a subgroup of $\mathfrak{S}(X)$.

(3) In the multiplicative group $(\mathbb{C}^* \cdot)$ of non-zero complex numbers, the subset $\mathrm{S}^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$ is a subgroup; this subgroup is called the *unit-circle group.*

The main ingredient which goes into the proof of Lagrange's group theorem is that a subgroup in a group defines an equivalence relation. More precisely, let G be a group and let H be a subgroup. For $x, y \in G$, we say that x is *congruent to y modulo H* if $xy^{-1} \in H$ and this is denoted by $x \equiv y \bmod H$ or by $x \equiv_H y$.

Lemma 3.5. *Let G be a group and let H be a subgroup. Then the relation $\equiv_H$ is an equivalence relation on G. Moreover, for $x \in G$, $Hx = \{hx \mid h \in H\}$ is the equivalence class of x.*

Proof. To prove that $\equiv_H$ is an equivalence relation on G, we must verify the following three conditions: For all $x, y, z \in G$,

(1) (*reflexivity*) $x \equiv x \bmod H$;

(2) (*symmetry*) $x \equiv y \bmod H$ implies that $y \equiv x \bmod H$;

(3) (*transitivity*) $x \equiv y \bmod H$ and $y \equiv z \bmod H$ implies that $x \equiv z \bmod H$

Let us verify each of these in turn.

(1) Since H is a subgroup of G, $xx^{-1} = e \in H$ and hence $x \equiv x \bmod H$

(2) If $x \equiv y \bmod H$, i.e., $xy^{-1} \in H$ and hence $yx^{-1} = (y^{-1})^{-1}x^{-1} = (xy^{-1})^{-1} \in H$ since H is a subgroup of G. Therefore $y \equiv x \bmod H$

(3) If $x \equiv y \bmod H$ and $y \equiv z \bmod H$, i.e., $xy^{-1} \in H$ and $yz^{-1} \in H$ Therefore, since H is a subgroup of G, we have $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xez^{-1} = xz^{-1} \in H$ and hence $x \equiv z \bmod H$

Now let $[x]$ denote the equivalence class of $x \in G$ under the equivalence relation $\equiv_H$, i.e., $[x] = \{y \in G \mid x \equiv y \bmod H\}$. To show the equality $[x] = Hx$, we first show the inclusion $Hx \subseteq [x]$. For, if $h \in H$ then $x(hx)^{-1} = x(x^{-1}h^{-1}) = (xx^{-1})h^{-1} = eh^{-1} = h^{-1} \in H$ since H is a subgroup of G. This means $x \equiv hx \bmod H$ and hence $hx \in [x]$. Therefore $Hx \subseteq [x]$. To prove the other inclusion $[x] \subseteq Hx$, let $y \in [x]$. Then $xy^{-1} \in H$ and hence $(xy^{-1})^{-1} = yx^{-1} \in H$ Therefore $yx^{-1} = h$ for some $h \in H$ Then, multiplying both sides on the right by x, we get $y = hx \in Hx$. This proves the inclusion $[x] \subseteq Hx$. □

In the additive group $(\mathbb{Z}, +)$ of integers, the congruence relation modulo the subgroup $n\mathbb{Z}$ of all multiples of n is precisely the usual number theoretic relation of congruence modulo n. Therefore the relation on an arbitrary group G defined by using a subgroup H is the natural generalisation of a familiar relation in a familiar group.

The equivalence relation $\equiv_H$ on a group G defined by a subgroup H yields equivalence classes and hence a decomposition of G into mutually disjoint subsets. Therefore *any two right cosets of H in G either are identical or disjoint.*. We now claim that:

Lemma 3.6. *Let G be a group and let H be a subgroup. Then for each $x \in G$, there is a bijection between the right cosets H and Hx.*

Proof. It is easy to verify that the map $H \to Hx$

defined by $h \mapsto hx$ is bijective. □

The above Lemma 3.6 is of most interest when H is a finite subgroup, for, then each right coset of H in G has exactly as many elements as that in H, i.e., $|Hx| = \text{ord}(H)$ for every $x \in G$. Moreover, if G is finite and if k represents the number of distinct right cosets of H in G, then we must have $\text{ord}(G) = k \ \text{ord}(H)$. Note that k is the number of subsets in the decomposition of G given by the equivalence relation $\equiv_H$ on G, i.e., $k = |G/\equiv_H|$, where $G/\equiv_H$ denotes the quotient set of G by the equivalence relation $\equiv_H$. The number k is also called the *index* of H in G and is denoted by $[G : H]$. Therefore we have proved that: $\text{ord}(G) = \text{ord}(H) \ [G : H]$. In particular, we have proved the famous Lagrange's group theorem:

Theorem 3.7. (*Lagrange's group theorem*) *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G,* i.e., *ord*$(H) \mid \text{ord}(G)$.

Lagrange's group theorem has several very important corollaries. Before we mention them let us recall that the *order* of an element x in a group G is the least positive integer m such that $x^m = \underbrace{x \ x \ \ldots \ x}_{m-\text{times}} = e$. If no such positive integer exists, then we say that x is of infinite order. We shall denote the order of x by $\text{ord}(x)$.

Corollary 3.8. *Let G be a finite group and let $x \in G$. Then the order of x divides the order of G, i.e.,* $\text{ord}(x) \mid \text{ord}(G)$. *In particular,* $x^{\text{ord}(G)} = e$.

Proof. Let $H = \text{H}(x)$ be the cyclic subgroup generated by x. Then it is clear that $\text{ord}(x) = \text{ord}(H)$ and hence $\text{ord}(x) \mid \text{ord}(G)$ by the Lagrange's group theorem. □

A special case of the above corollary is of great interest: if $f : X \to X$ is a bijection from a finite set X onto itself, then f composed with itself sufficiently many times is

the identity map of the set X, i.e., $f^m = \mathrm{id}_X$ for some positive integer m (In fact, $m = n!$ will work, where n is the number of elements in X).

We mention another consequence of Lagrange's group theorem. For a positive integer n, let $\mathrm{U}_n := \{m \in \mathbb{N} \mid 1 \leq m \leq n,\ \gcd(m,n) = 1\}$. Then it can easily be proved that U_n is a group under multiplication modulo n and this group has order $\varphi(n)$, where φ denotes the Euler's totient function. We apply the above corollary to the group U_n to get the following famous theorem due to Euler which is a generalisation of the Fermat's little theorem proved in the theorem 1.1 (2).

Corollary 3.9. (*Euler*) *Let n be a positive integer and let a be an integer which is relatively prime to n. Then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corollary 3.10. *A finite group of prime order is cyclic.*

If n is a positive integer, the $\varphi(n)$ denotes the number of positive integers less than or equal to n and comprime to n. Here φ is called the Euler's totient function. For example, $\varphi(1) = \varphi(2) = 1$; $\varphi(p) = p - 1$, if p is a prime.

Proof. First note that G has no nontrivial subgroups H For, if H is a subgroup of G, then $\mathrm{ord}(H) \mid \mathrm{ord}(G) = p$ by the Lagrange's group theorem and hence (since p is prime) either $\mathrm{ord}(H) = 1$ or $\mathrm{ord}(H) = p$. Therefore either $H = \{e\}$ or $H = G$. Let $x \in G$, $x \neq e$ and let $H = H(x)$ be the cyclic subgroup generated by x. Then $H = G$ and hence G is cyclic and every element $x \in G$, $x \neq e$ is a generator of G. □

Remarks 3.11 It is important to note that the converse of Lagrange's theorem is false, i.e., *If G is a finite group of order n and d divides n, then G may not have a subgroup of order d.*

For example, it an easy exercise to show that the alternating group A_4 of order 12 has no subgroup of order 6.

However, *if G is a finite group of order n and a prime p divides n, then G has an element of order p.* (For an elegant, charming and short proof of this result, we refer

the reader to the article [2]). Consequently, G has a subgroup of order p. This interesting result was first proved by Cauchy. Moreover, the following stronger result was proved by a Norwegian mathematician Ludwig Sylow in 1872.

If G is a finite group of order n and a prime power p^r divides n, then G has a subgroup of order p^r

This is the most basic and widely used classic theorem in group theory.

4. Some Other Results

Lagrange is also known for the following results among others in pure mathematics. Besides putting Calculus on a firm footing, he is known for:

- the method of Multipliers for determining the extrema of functions of several variables under some constraints;
- determining a polynomial in x of degree n given values of the polynomial at $(n + 1)$ values of x (*Lagrange's Interpolation Formula*);
- determining the structure of prime divisors of expressions of the form $x^2 + 2y^2$, where x and y are coprime positive integers;
- giving a formula for the multiplicative inverse of a real power series; and
- determining extremal functions among functions satisfying certain conditions which is now a subject of Calculus of Variations.

Suggested Reading

[1] **G H Hardy and E M Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London, 5th edition, 1975.**

[2] **James H McKay, Another proof of Cauchy's group theorem, *American Mathematical Monthly*, Vol.66, p.119, 1959.**

Address for Correspondence
D P Patil, C R Pranesachar
and Renuka Ravindran
Department of Mathematics
Indian Institute of Science
Bangalore 560 012, India.
Email:patil@math.iisc.ernet.in
pran@math.iisc.ernet.in
renrav@math.iisc.erent.in