UNIT 2:

Permutation, Combination and Algebraic System

Permutation and combination are explained here elaborately, along with the difference between them. We will discuss both the topics here with their formulas, real-life examples and solved questions. Students can also work on Permutation And Combination Worksheet to enhance their knowledge in this area along with getting tricks to solve more questions.

What is Permutation?

In mathematics, **permutation relates to the act of arranging all the members of a set into some sequence or order.** In other words, if the set is already ordered, then the rearranging of its elements is called the process of permuting. Permutations occur, in more or less prominent ways, in almost every area of mathematics. They often arise when different orderings on certain finite sets are considered.

Click here to learn more about Permutation in maths.

What is a Combination?

The **combination is a way of selecting items from a collection, such that (unlike permutations) the order of selection does not matter**. In smaller cases, it is possible to count the number of combinations. Combination refers to the combination of n things taken k at a time without repetition. To refer to combinations in which repetition is allowed, the terms k-selection or k-combination with repetition are often used. Permutation and Combination Class 11 is one of the important topics which helps in scoring well in Board Exams.

Click here to get more information about Combination.

Permutation and Combination Formulas

There are many formulas involved in permutation and combination concepts. The two key formulas are:

Permutation Formula

A permutation is the choice of r things from a set of n things without replacement and where the order matters.

${}^{n}P_{r}$ = (n!) / (n-r)!

Combination Formula

A combination is the choice of r things from a set of n things without replacement and where order does not matter.

$$ {}_nC_r = \binom{n}{r} = \frac{{}_nP_r}{r!} = \frac{n!}{r!(n-r)!} $$

Learn how to calculate the factorial of numbers here.

Difference Between Permutation and Combination

Go through the differences between permutation and combination given below.

Permutation	Combination
Arranging people, digits, numbers, alphabets, letters, and colours	Selection of menu, food, clothes, subjects, team.
Picking a team captain, pitcher and shortstop from a group.	Picking three team members from a group.
Picking two favourite colours, in order, from a colour brochure.	Picking two colours from a colour brochure.

Permutation	Combination
Picking first, second and third place winners.	Picking three winners.

Uses of Permutation and Combination

A permutation is used for the list of data (where the order of the data matters) and the combination is used for a group of data (where the order of data doesn't matter).

Sum and Product Rules

Example 1: In New Hampshire, license plates consisted of two letters followed by 3 digits. How many possible license plates are there?

Answer: 26 choices for the first letter, 26 for the second, 10 choices for the first number, the second number, and the third number:

$26^2 \times 10^3 = 676{,}000$

Example 2: A traveling salesman wants to do a tour of all 50 state capitals. How many ways can he do this?

Answer: 50 choices for the first place to visit, 49 for the second, ...: 50! altogether.

Chapter 4 gives general techniques for solving counting problems like this. Two of the most important are:

The Sum Rule: If there are n(A) ways to do A and, distinct from them, n(B) ways to do B, then the number of ways to do A or B is n(A) + n(B).

- This rule generalizes: there are n(A) + n(B) + n(C) ways to do A or B or C
- In Section 4.8, we'll see what happens if the ways of doing A and B aren't distinct.

The Product Rule: If there are n(A) ways to do A and n(B) ways to do B, then the number of ways to do A and B is n(A) × n(B). This is true if the number of ways of doing A and B are independent; the number of choices for doing B is the same regardless of which choice you made for A.

- Again, this generalizes. There are n(A)×n(B)×n(C) ways to do A and B and C

Binary Operations

The binary operation can be understood as an operation which is performed on the two elements p & q from the set X. Thus, the binary operation performed on operands p and q is symbolized as p*q. The function is given by *:AAA. The result of the operation on p and q is another element from the same set X.

Note: We can denote a binary operation using any symbol (!, @ , * , $ etc.)

Example: Show that subtraction and division are not binary operations on N.

Solution:

- : ℕℕℕ, given by (a, b) a – b, is not binary operation, as the image of (2, 7) under '-' is 2-7 =-5 ℕ. Similarly, : ℕℕℕ, given by (a, b) a ÷ b is not a binary operation, as the image of (2, 7) under '' is 2 ÷ 7 =2/7 ℕ.

Example:Show that addition, subtraction and multiplication are binary operations on R , but division is not a binary operation on R . Further, show that division is binary operation on the set R of non-zero real numbers.

Solution

+: R × R → R is given by +(a,b) → a+b
-: R × R → R is given by -(a,b) → a-b
: R × R → R is given by (a,b) → ab

Since +,- and are functions, they are binary operations on R .

But : R × R → R , given by (a,b)a/b is not a function and hence not a binary operation, as for b=0, a/b is not defined.
However, : R × R → R is given by (a,b)a/b is a function and hence a binary operation on set R of non zero real numbers.

Example:Let M be the set of all subsets of a given set A. Show that : M × MM given by (P, Q)PQ and : M × MM given by (P, Q)PQ are binary operations on the set M.

Solution

Proving for Union

Since M is the set of all the subsets of the given set A and P, Q are in set M we can say that P and Q are also the subsets of A.

If we calculate PQ then it will also be a subset of A as the union of subsets is also a subset

Hence, PQ will also be in set M i.e. is a binary operation.

Proving for Intersection

Since M is the set of all the subsets of the given set A and P, Q are in set M we can say that P and Q are also the subsets of A

If we calculate PQ then it will also be a subset of A as the intersection of subsets is also a subset.Hence, PQ will also be in set M i.e. is a binary operation.

Example :Show that the operation : R× R→ R given by (p, q) max {p, q} and the operation
: R× R → R given by (p, q)min {p, q} are binary operations.

Solution:

Since, pq=max of p and q; p,qR

pq will give output as either p or q.

Hence, pq R. Therefore, is a binary operation.

Also, pq=min of p and q, p,qR

pq will give output as either p or q.

Hence, pq R. Therefore, is a binary operation.

Note:

- Addition, subtraction and multiplication are also the binary operations on each of the sets of integers, rational numbers, real numbers
- Addition,subtraction and multiplication are not binary operations on the set of irrational numbers.
- Division is not a binary operation on the set of natural numbers, integers, rational numbers, real numbers and complex numbers.

Properties of Binary Operations

1. Commutative:

A binary operation * is commutative on the set X, if a*b=b*a for every a,bX.

Example: Addition and multiplication are commutative binary operations but subtraction and division are not.

2. Associative:

A binary operation on set X is associative if for every a,b,cX, a*(b*c)=(a*b)*c

Example: Addition and multiplication are associative binary operations on the set of real numbers but subtraction and division are not.

3. Identity element:

An element eX is called the identity of the operation *: XXX, if

a*e=a=e*a, for every element aX.

Example: 0 and 1 are the identities for addition and multiplication operation on the set of

real numbers. There is no identity for subtraction and division operations on $\mathbb{R}$.

4. Inverse of an element:

For a binary operation * on a non-empty set X, let e be the identity element. If aX, then a is invertible if there exists an element bX such that a*b=b*a=e.

Example: 1/a is the inverse of a0 of the multiplication operation() on $\mathbb{R}$ but it's not an inverse of X on the set of natural numbers $\mathbb{N}$.

Number of Binary Operations on a Set

Let *:AAA be a binary operation on set A and n(A)=p

Now, n(AA)=n(A)n(A)=pp=p2

Hence, number of functions from AAA will be pp2

(Since, number of functions from AB where n(A)=a, n(B)=b is ba)

The total number of binary operations on a set consisting of n elements is given by pp2.

Types of Binary Operations

Commutative

A binary operation * on a set A is commutative if a * b = b * a, for all (a, b) ∈ A (non-empty set). Let addition be the operating binary operation for a = 8 and b = 9, a + b = 17 = b + a.

Associative

The associative property of binary operations hold if, for a non-empty set A, we can write (a * b) *c = a*(b * c). Suppose **N** be the set of natural numbers and multiplication be the binary operation. Let a = 4, b = 5 c = 6. We can write (a × b) × c = 120 = a × (b × c).

Distributive

Let * and o be two binary operations defined on a non-empty set A. The binary operations are distributive if a*(b o c) = (a * b) o (a * c) or (b o c)*a = (b * a) o (c * a). Consider * to be multiplication and o be subtraction. And a = 2, b = 5, c = 4. Then, a*(b o c) = a × (b − c) = 2 × (5 − 4) = 2. And (a * b) o (a * c) = (a × b) − (a × c) = (2 × 5) − (2 × 4) = 10 − 6 = 2.

Identity

If A be the non-empty set and * be the binary operation on A. An element e is the identity element of a ∈ A, if a * e = a = e * a. If the binary operation is addition(+), e = 0 and for * is multiplication(×), e = 1.

Inverse

If a binary operation * on a set A which satisfies a * b = b * a = e, for all a, b ∈ A. a^{-1} is invertible if for a * b = b * a= e, a^{-1} = b. 1 is invertible when * is multiplication.

The Very Basics of Groups, Rings, and Fields

Groups, rings, and fields are familiar objects to us, we just haven't used those terms. Roughly, these are all sets of elements with additional structure (that is, various ways of combining elements to produce an element of the set). Studying this finer structure is the key to many deep facts in number theory.

Informal Definitions A GROUP is a set in which you can perform one operation (usually addition or multiplication mod *n* for us) with some nice properties. A RING is a set equipped with two operations, called addition and multiplication. A RING is a GROUP under addition and satisfies some of the properties of a group for multiplication. A FIELD is a GROUP under both addition and multiplication.

Definition 1. *A* **GROUP** *is a set G which is CLOSED under an operation* $*$ *(that is, for any* $x,y \in G$, $x * y \in G$*) and satisfies the following properties:*

(1) *Identity – There is an element e in G, such that for every* $x \in G$, $e * x = x * e = x$.
(2) *Inverse – For every x in G there is an element* $y \in G$ *such that* $x * y = y * x = e$, *where again e is the identity.*
(3) *Associativity – The following identity holds for every* $x,y,z \in G$:

$x * (y * z) = (x * y) * z$

Examples:

(1) $\mathbb{Z}/n\mathbb{Z}$, fancy notation for the integers mod *n* under addition. Let's see how this satisfies the axioms:
   (a) CLOSURE: Given any two integers mod *n*, their sum (via addition modulo *n*) is an integer mod *n* by definition. (Again, to be clear, the operation $*$ described above is addition modulo *n*.)
   (b) IDENTITY: 0 mod *n* is the identity element, since $a * 0$ means $a + 0$ mod *n*, which is clearly *a* mod *n*.
   (c) INVERSE: Given any *a* (mod *n*), we must find an inverse *b* so that $a * b = e$ in the group, i.e. $a + b \equiv 0 \pmod{n}$. The inverse to any *a* in this case is $n - a$.
   (d) ASSOCIATIVITY: The integers are associative, by basic rules of addition, sothe integers mod *n* are also associative. That is, since

$a + (b + c) = (a + b) + c$, then it follows that $a + (b + c) \equiv (a + b) + c \ (n)$

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$, more fancy notation for the integers mod n under multiplication. IMPORTANT: the elements of this set are NOT all integers mod n, but rather all integers RELATIVELY PRIME to n. See if you can show how these relatively prime elements

form a group mod n and why including all integers mod n would not be a group (i.e. fails one or more of the axioms).

(3) $\mathbb{Z}$, the integers under addition. Groups don't have to be finite. Also note that you can't make the integers into a group under multiplication, since elements like 2 don't have a multiplicative inverse (i.e. an element y such that $2y = 1$, since 1/2 isn't in the integers). But in Math 152, we mainly only care about examples of the type above.

A group is said to be "abelian" if $x * y = y * x$ for every $x,y \in G$. All of the examples above are abelian groups. The set of symmetries of an equilateral triangle forms a group of size 6 under composition of symmetries. It is the smallest group which is NOT abelian.

Definition 2. *A* **RING** *is a set R which is CLOSED under two operations* + *and* × *and satisfying the following properties:*

(1) *R is an abelian group under* +.

(2) *Associativity of* × *– For every a,b,c* ∈ *R,*

$a \times (b \times c) = (a \times b) \times c$

(3) *Distributive Properties – For every a,b,c* ∈ *R the following identities hold:*

$a \times (b + c) = (a \times b) + (a \times c)$

and

$b + c) \times a = b \times a + c \times a.$

Examples:

(1) Both the examples $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ from before are also RINGS. Note that we don't require multiplicative inverses.

(2) $\mathbb{Z}[x]$, fancy notation for all polynomials with integer coefficients. Multiplication and addition is the usual multiplication and addition of polynomials.

Definition 3. *A* **FIELD** *is a set F which is closed under two operations* + *and* × *such that*

(1) *F is an abelian group under* + *and*

(2) $F - \{0\}$ *(the set F without the additive identity* 0*) is an abelian group under* ×.

Examples: $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is an additive group and $(\mathbb{Z}/p\mathbb{Z}) - \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication. Sometimes when we (or Cox) want to emphasize that $\mathbb{Z}/p\mathbb{Z}$ is a field, we use the notation $\mathbb{F}_p$. Other examples: R, the set of real numbers, and C, the set of complex numbers are both infinite fields. So is Q, the set of rational numbers, but not Z, the integers. (What fails?)

Another NON-Example: If n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field, since $(\mathbb{Z}/n\mathbb{Z}) - \{0\} 6= (\mathbb{Z}/n\mathbb{Z})^\times$. There are, in general, lots of other elements than 0 which are not relatively prime to n and hence have no inverse under multiplication.

The theory of these abstract structures is sometimes simpler than dealing with specific examples because we've pared down and listed all the essential properties that should be used in proofs. Here's a simple result from group theory (though we don't bother with the proof since there's already enough notation so far in this document):

Theorem 1 (Corollary to Lagrange's Theorem)**.** *If $x \in G$, a group of size N, then $x^N = e$.*

In particular when $G = (\mathbb{Z}/p\mathbb{Z})^\times$, the group of integers which are non-zero mod p under multiplication, this implies Fermat's Little Theorem. Indeed, there are $p-1$ elements in this group, so the above theorem implies that

$$x^{p-1} = e \qquad \text{for all elements } x \text{ in } G$$

What does this equality mean in the group? The identity element is given by 1 mod p, and equality in this group means two numbers are congruent mod p. So this statement translates to: $x^{p-1} \equiv 1\ (p)$for all elements x which are non-zero mod p

More generally, when $G = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of integers mod n which are relatively prime to n (NOTICE: this generalizes the definition we made when $n = p$), we get a special case of the above theorem known as Euler's theorem. We denote the size of G by the number $\varphi(n)$ and the statement

$x^N = e$

in the corollary to Lagrange's theorem similarly translates to (since e, the identity under multiplication, is 1 in this case) $x^{\varphi(n)} \equiv 1 \pmod{n}$.

You might try investigating the properties of $\varphi(n)$, the number of relatively prime integers to n mod n, by doing a few examples. Since divisibility is so important to us, this turns out to be a very important function.

Again, WHY do we ever need to consider groups?

Believe it or not, this added abstraction often makes problems easier. By reducing to a generic object defined by axioms, you can often see a clearer picture of what's going on (that is, what depends on what) and why. For example, working on arithmetic problems mod 11 all the time, you might be able to prove many things, and even guess a general picture, so working out these specific examples as we did for our proof of Fermat's Little Theorem is a good idea. However, you'll never see how far your theory extends unless you think about what makes the proof work and what axioms are essential to demonstrating its truth.