Mathematical Structures: Groups, Rings, and Fields

Presented By:- Shilpa
AP in Maths

☪$_6$ – Our first group

- We begin with a set of six numbers

  ☪$_6$ = { 0, 1, 2, 3, 4, 5 }

- We define an operation on the set which we call addition and denote by +
- This is similar to, but not really the same as, the usual operation of addition
- To see this, let's add 1 to each element of ☪$_6$

Add 1 to each element of ☪$_6$

0 + 1 = 1

1 + 1 = 2

2 + 1 = 3

3 + 1 = 4

4 + 1 = 5

5 + 1 = ?

- What is 5 + 1?
- Usually it's 6, but there is no 6 in our set
- What to do?

Add 2 to each element of ☪$_6$

0 + 2 = 2

1 + 2 = 3

2 + 2 = 4

3 + 2 = 5

4 + 2 = 0

5 + 2 = 1

- Now we seem to have two strange results, but keep thinking about clock arithmetic

Addition table for $☪_6$

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

- Pick an element x in the left column and an element y in the top row
- Where the row and column meet is x + y

Examples of addition

3 + 2 = 5

3 + 3 = 6, so 6 - 6 = 0 is the sum

3 + 4 = 7, so 7 - 6 = 1 is the sum

4 + 1 = 5

4 + 4 = 8, so 8 - 6 = 2 is the sum

5 + 5 = 10, so 10 - 6 = 4 is the sum

Note how similar this is to clock arithmetic

0 is an identity

$$0 + 0 = 0$$
$$1 + 0 = 1$$
$$2 + 0 = 2$$
$$3 + 0 = 3$$
$$4 + 0 = 4$$
$$5 + 0 = 5$$

- So $x + 0 = x$ for every x
- We say 0 is an **identity** element for +

Every element has an inverse

$$0 + 0 = 0$$

$$1 + 5 = 0$$

$$2 + 4 = 0$$

$$3 + 3 = 0$$

$$4 + 2 = 0$$

$$5 + 1 = 0$$

- Every element x has an **inverse** element x' such that

$$x + x' = 0$$

Be associative

- How to compute 5 + 4 + 2 ?

$$(5 + 4) + 2 = (3) + 2 = 5$$

$$5 + (4 + 2) = 5 + (0) = 5$$

- For any three elements x, y, z of ☪$_6$ we have

$$(x + y) + z = x + (y + z)$$

- Another way to say this: Addition is **associative**

Where are we?

- We have a set of six elements

  ☪$_6 = \{ 0, 1, 2, 3, 4, 5 \}$

- We have an operation + defined on the set which takes any two elements of the set and combines them to produce another element of the set
- The operation is **associative**, so for any three elements x, y, and z we have

  $$(x + y) + z = x + (y + z)$$

Groups

- Note that the word “group” is being used here in a highly technical sense
- A group is a non-empty set with a binary operation defined on it such that the operation is associative, an identity element exists, and every element has an inverse
- The group is one of the most fundamental structures in mathematics
- Groups sprout like weeds in modern math

Examples of groups

- Let ☪$_n$ = { 0, 1, 2, ..., n-1 } for any integer n > 0, and define + in analogy with + for ☪$_{6}$⌛
- ☪$_n$ is a group
- ☪$_n$ is called the **cyclic** group of n elements
- Note that for every positive integer n there exists at least one group with n elements
- So we don't have to worry about running out of groups

Some groups go on forever ...

- Now consider ☪ = { ..., -2, -1, 0, 1, 2, ... }, the set of all integers, and let + be the usual addition of integers
- Is <☪,+> a group?
- Is + a binary operation on ☪?
- Is + associative?
- Which element is the identity?
- For x an integer, what is its inverse?

☪ is indeed a group

- + on integers is a binary operation
- It is associative
- 0 is the identity element
- For any integer x, its inverse is -x
- ☪ is an **infinite** group, the first such we have seen

Is <☪,*> a group?

- Now consider ☪ and the operation *, the usual multiplication of integers
- Is <☪,*> a group?
- Is * a binary operation on ☪?
- Is * associative?
- Which element is the identity?
- For x an integer, what is its inverse?

<☪,*> is NOT a group

- * on integers is a binary operation
- It is associative
- 1 is the identity element
- For any integer x, its inverse is 1/x
- Whoops! 1/x is not an integer (except when x = -1 or x = +1), so the vast majority of integers have no multiplicative inverses

Is <☼$^{+}$,*> a group?

- Let ☼$^{+}$ denote the set of all positive real numbers, and let * be the usual multiplication of real numbers
- Is <☼$^{+}$,*> a group?
- Is * a binary operation on ☼$^{+}$?
- Is * associative?
- Which element is the identity?
- For x a positive real, what is its inverse?

<☼$^+$,*> is a group

- * on real numbers is a binary operation
- It is associative
- 1 is the identity element
- For any real x, its inverse is 1/x
- <☼$^+$,*> is an **infinite** group, the second such we have seen
- [It's *way* more infinite than <☪,+>, but that's the subject of another talk.]

<$☪_6$,+> is isomorphic to <H,*>

- When two mathematical objects are isomorphic, they have the same structure
- When a statement is proved true about one structure, the equivalent statement is true about the other structure
- Sometimes one structure is easier to work with than another
- Addition in $☪_6$ may be easier than rotating cardboard hexagons

S_3 is a group

- An **identity** element R_0 exists so that for any element x we have

$$x * R_0 = x$$

- Every element x has an **inverse** element x' so that

$$x * x' = R_0$$

- In short, S_3 is a group!

S_3 is noncommutative

- Many operations in mathematics are **commutative**, i.e., the order of the operands does not matter:

$$15 + 6 = 6 + 15 = 21$$

$$15 * 6 = 6 * 15 = 90$$

- But composition on S_3 is **noncommutative**:

$$R_1 * F_2 \neq F_2 * R_1$$

- Be careful not to assume commutativity

S_3 is nonabelian

- When a group is commutative, it is said to be **abelian**
- When a group is noncommutative, it is said to be **nonabelian**
- The term *abelian* is derived from the name of the Norwegian mathematician, Niels Henrik Abel (1802-1829), who did significant mathematics before dying at a young age of tuberculosis

What about multiplication?

- A group has only one operation, usually called addition (but, as we have seen, it is not necessarily the usual addition we are used to)
- In many cases of interest there are two operations: addition and **multiplication**
- Let's return to our favorite structure, $☪_6$, and see if we can define multiplication for it

Multiplication made easy

- Denote multiplication by *
- For x and y in $\text{☪}_{\text{⌛}}$, we define x * y like this:
- Multiply x times y in the usual way as if they were ordinary whole numbers to get a product z

  If z < 6, then z is the product

  If z ≥ 6, then subtract 6 from z repeatedly until a number < 6 results; it is the product

Examples of multiplication

2 * 2 = 4

2 * 3 = 6, so 6 - 6 = 0 is the product

3 * 3 = 9, so 9 - 6 = 3 is the product

3 * 4 = 12, so 12 - 6 - 6 = 0 is the product

1 * 5 = 5

4 * 4 = 16, so 16 - 6 - 6 = 4 is the product

5 * 5 = 25, so 25 - 6 - 6 - 6 - 6 = 1 is the product

Multiplication table for ☪$_6$

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1 is a unity

0 * 1 = 0

1 * 1 = 1

2 * 1 = 2

3 * 1 = 3

4 * 1 = 4

5 * 1 = 5

- So x * 1 = x for every x
- We say 1 is a **unity** for *

Definition of a ring

- A **ring** <R,+,*> is a non-empty set R together with two operations + and *, called addition and multiplication, such that
- <R,+> is an abelian group
- Multiplication is associative
- Multiplication distributes over addition
- A **commutative ring with unity** is a ring in which multiplication is commutative and there exists a unity element

<☪$_6$,+,*> is a commutative ring with unity

- We have seen that <☪$_6$,+> is an abelian group (remember *abelian* means + is commutative)
- * is associative
- * distributes over +
- * is commutative
- 1 is a unity
- <☪$_6$,+,*> is a commutative ring with unity

Examples of Rings

- Let ☪$_n$ = { 0, 1, 2, ..., n-1 } for any integer n > 0, and define + and * in analogy with + and * for ☪$_6$
- <☪$_n$,+,*>□ is a commutative ring with unity
- So there are an infinite number of such rings
- There are also infinite rings, e.g., ☪ with the usual addition and multiplication

A ring divided ...

- In order to divide by an element x, we must have an element x' such that x * x' = 1, i.e., we need a multiplicative inverse for x
- Then, to divide by x, we simply multiply by the multiplicative inverse x'
- Looking back at the multiplication table for ☪$_6$, we see that only 1 and 5 have multiplicative inverses
- So division in ☪$_6$ is just not going to work

If $☪_6$ doesn't work, try $☪_5$

- Let's look at <$☪_5$,+,*>, a commutative ring with unity consisting of 5 elements 0, 1, 2, 3, and 4
- We can add and multiply in this ring much like we did in $☪_6$: When a value is greater than or equal to 5, we subtract 5 repeatedly until we get 0, 1, 2, 3, or 4
- Let's look at the multiplication table for $☪_5$

Multiplication table for ☪$_5$

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

How is this different from the multiplication table for ☪$_6$?

Unity at last

- In every row of the table except the first, we see that the multiplicative unity 1 appears
- This means that every element except 0 has a multiplicative inverse:

$$1 * 1 = 1$$

$$2 * 3 = 1$$

$$3 * 2 = 1$$

$$4 * 4 = 1$$

What's your field?

- Given a non-zero element x of a ring, if there exists an element x^{-1} such that $x * x^{-1} = 1$, then x^{-1} is the **multiplicative inverse** of x
- A **field** is a commutative ring with unity in which every non-zero element has a multiplicative inverse
- In a field we can not only add, subtract, and multiply, we can also divide

Examples of fields

- ☪$_5$ is a field
- ☪$_p$ is a field for every prime p, so there are an infinite number of finite fields
- Is ☪, the set of all integers, a field?
- Is ✈, the set of all rational numbers, a field?
- Is ☼, the set of all real numbers, a field?
- Is 👍, the set of all complex numbers, a field?

A subset of the real numbers

- Consider the set S = { a+b√2 | a,b □ ✈ }
- Some elements of S: 2+√2, ½ +3√2, 5
- Note that S is bigger than ✈ and smaller than ☼: ✈   ② S   ② ☼
- Define addition and multiplication on S as the usual operations on the real numbers
- Is S a field?
- What are the requirements on a set in order for it to be a field?

You do the third one

- 1. $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$

- 2. $(a+b\sqrt{2}) * (c+d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd\sqrt{2}\sqrt{2} = (ac+2bd) + (ad+bc)\sqrt{2}$

- 3. The multiplicative inverse of $a+b\sqrt{2}$ is $a/d - (b/d)\sqrt{2}$, where $d = a^2 - 2b^2$

Thanks