Sets and Groups: Part 2

At the end of this lecture you should be able to:

- solve problems using set algebra;
- distinguish between **natural numbers**, **integers**, **rational numbers**, **real numbers** and **complex** numbers;
- distinguish between **discrete** and **continuous** values;
- determine whether an operation is **commutative** and/or **associative**;
- perform simple algebra using complex numbers;
- define the meaning of the term **group** and state the criteria that determine whether a set is a group under a particular operation;
- use the above criteria to decide whether a set and an operation constitute a group;
- explain the meaning of the term **Abelian group**;
- explain the terms **semigroup** and **monoid**.

The Algebra of Sets

There are a number of laws that follow directly from the definitions that we covered in the last lecture:

Idempotent Laws

$A \cup A = A$

$A \cap A = A$

Identity Laws

$A \cap \varnothing = \varnothing$

$A \cap U = A$

$A \cup \varnothing = A$

$A \cup U = U$

Complement Laws

$A \cup \overline{A} = U$

$A \cap \overline{A} = \varnothing$

$\overline{\varnothing} = U$

$\overline{U} = \varnothing$

Two other laws which are not quite so obvious are:

Distributive law

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan's law

$\overline{A \cup B} = \overline{A} \cap \overline{B}$

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

It can be seen that the above pairs are duals of each other. This is a fact of set algebra called **the principle of duality**.

Worked examples

1. Show that:

$$A \cap (\overline{A} \cup B) = A \cap B$$

<u>Solution</u>

$A \cap (\overline{A} \cup B)$

$= (A \cap \overline{A}) \cup (A \cap B)$ Distributive Law

$= \varnothing \cup (A \cap B)$ Complement Law

$= A \cap B$ Identity Law

2. Show that:

$(A \cap B) \cup (A \cap \overline{B}) = A$

<u>Solution</u>

$(A \cap B) \cup (A \cap \overline{B})$

$= A \cap (B \cup \overline{B})$ Distributive Law

$= A \cap U$ Complement Law

$= A$ Identity Law

Number Types

Natural Numbers

Natural numbers are the numbers that we use for counting. That is to say, whole numbers from 0 to infinity:

Examples of natural numbers are:

3, 10, 289, 1098

Integers

Integers include the natural numbers, but also include the numbers less than zero (negative numbers).

Integers are therefore whole numbers from minus infinity to plus infinity:

Examples of integers are:

-1, 34, -235, 0, 195

Rational numbers

- **Rational numbers** are numbers that can be expressed as: $\frac{p}{q}$

  where p and q are integers.

- Some numbers occur naturally in nature but cannot be expressed as rational numbers – they are *irrational* numbers (also called **surds**);

- examples of irrational numbers are:

  - $\sqrt{2}$

  - π (the number of times the diameter of a circle goes into the circumference)

  - Euler's number, e, which is a very important mathematical constant.

Real Numbers

Real numbers are numbers that have a fractional part;

They include rational numbers but also include irrational numbers;

They also include integers (and therefore natural numbers) because integers can be expressed as, for example, 2.0, 3.0, -5.0 and so on.

Examples of real numbers are:

-3.127, 34.987, 0.001, -108.7, 3.0

Complex numbers

- **complex numbers** are used in advanced mathematics and consist of a *real* part and an *imaginary* part;

- the imaginary part contains a special number i, which is defined as:

$$\sqrt{-1}$$

- of course there is no real number that gives -1 when squared, which is why we use the term imaginary number.

- a typical complex number might look like this: 3 + 2i

  - the set of complex numbers also contains real numbers (the coefficient of i is 0).

Worked example

Consider the following numbers: -4.82 33 -262 45.987 0.3

Which of these numbers are:

a) Real numbers b) Integers c) Natural numbers

Solution

a) All of them are real numbers.

b) 33 and -262 are integers (as well as being real numbers)

c) 33 is a natural number (as well as being an integer and a real number).

Working with complex numbers

Addition

We add the two parts separately.

For example

$(3 + 2i) + (4 – i) = 7 + i$

Multiplication

We do a normal binomial multiplication.

For example $(3 + 2i)(4 – 2i) = 12 - 6i + 8i – 4i^2$

$= 12 + 2i – 4i^2$

BUT $i^2 = -1$

so our final answer is $12 + 2i + 4$ or $\underline{16 + 2i}$

Division

Consider the following example: $\frac{3+i}{1-3i}$

- we need to find a way to remove the imaginary part from the denominator;
- we can do this by multiplying both numerator and denominator by (1 + 3i).

$$\frac{3+i}{1\ -3i} = \frac{(3+i)(1+3i)}{(1-3i)(1+3i)}$$

$$= \frac{3+9i+i+3i^2}{1+3i-3i-9i^2}$$

$$= \frac{3+10i+3i^2}{1-9i^2}$$

But i^2 = -1

$$= \frac{3+10i-3}{10}$$

$$= \frac{10i}{10}$$

$$= i$$

Application to computing

In most programming languages we have to declare the type of a variable before we use it.

This is because different number types are stored in different ways in memory.

It takes up a lot more memory to store a real number than an integer for example.

The available types for Java are shown on the next slide.

Java type	Range of values	Allows for
byte	very small integers	–128 to 127
short	small integers	–32 768 to 32 767
int	big integers	–2 147 483 648 to 2 147 483 647
long	very big integers	–9 223 372 036 854 775 808 to 9 223 372 036 854 775 807
float	real numbers	+/– 1.4 * 10^{-45} to 3.4 * 10^{38}
double	very big real numbers	+/– 4.9 * 10^{-324} to 1.8 * 10^{308}

Number sets

It is common to refer to the sets of numbers by the following letters:

$\mathbb{N}$ is the set of natural numbers

$\mathbb{Z}$ is the set of integers

$\mathbb{Q}$ is the set of rational numbers

$\mathbb{R}$ is the set of real numbers;

$\mathbb{C}$ is the set of complex numbers.

We see that: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Discrete versus continuous values

Imagine turning on a tap just enough so that the tap drips. You can count the individual drops of water that come out of the tap.

Imagine you turn the tap further, so that the water comes in a continuous stream. Now it is not possible to count anything.

Discrete values are like the drops of water. They come in separate packets, and you can count them.

Natural numbers and integers are discrete. You can count how many integers there are between, say, 1 and 10.

Continuous values are like the stream of water coming from the tap. There are no separate items that you can count.

Real numbers are continuous. It is not possible to say how many items there are between, say 2.1 and 2.2.

Countable and non-countable sets

Consider the set of positive numbers greater than or equal to 5 and less than or equal to 10. This set would contain 6 numbers – we can count them from 5 up to 10.

But what if we put no upper limit on the set? We could still count the members – the only thing is that we would never finish counting, because the number of elements is infinite. A set like this is said to be *countable* and *infinite*.

Now consider the set of real numbers form 5 to 10. How could we count these? If we started with 5.0, then counted 5.1, what about 5.01, 5.02 etc? And what about the numbers between 5.01 and 5.02?

You can see we can never count real numbers – and in fact it can be mathematically proven that if we take any two real numbers, there is always another number in between.

The set of real numbers, $\mathbb{R}$, is *non-countable* and infinite – whereas the set of natural numbers, $\mathbb{N}$, and the set of integers, $\mathbb{Z}$, are *countable* and infinite.

So you can see that there are in fact two types of infinity – countable infinity and non-countable infinity!

Operations

In mathematics, an **operation** is a calculation from a number of input values (called **operands**) to an output value.

The basic arithmetic operations are:

- Addition (+)
- Subtraction (-)
- Multiplication (x or *)
- Division (÷ or /)

Commutative Operations

When we perform an operation on two terms, the operation is **commutative** if it doesn’t matter which of the terms is placed first and which one is placed second.

In arithmetic the following operations are commutative:

Addition

$$x + y = y + x$$

For example: 2 + 3 = 3 + 2 = 5

Multiplication

$$x \times y = y \times x$$

For example: 2 x 3 = 3 x 2 = 6

The following arithmetic operations are *not* commutative:

Subtraction

$x - y \neq y - x$

For example: 10 – 3 = 7 3 – 10 = -7

10 - 3 $\neq$ 3 – 10

Division

$x \div y \neq y \div x$

For example: 10 $\div$ 5 = 2 5 $\div$ 10 = 0.5

10 $\div$ 5 $\neq$ 5 $\div$ 10

Associative Operations

When we perform an operation on more than two terms, the operation is **associative** if it doesn’t matter how we group the terms.

In arithmetic the following operations are associative:

Addition

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

For example: 2 + (3 + 4) = (2 + 3) + 4 = 9

Multiplication

$$x\times(y\times z)=(x\times y)\times z$$

For example: 2 x (3 x 4) = (2 x 3) x 4 = 24

The following arithmetic operations are *not* associative:

Subtraction

$$x-(y-z)\neq(x-y)-z$$

For example: 12 – (6 – 2) = 8 but (12 – 6) – 2 = 4

12 – (6 – 2) ≠ (12 – 6) – 2

Division

$$x\div(y\div z)\neq(x\div y)\div z$$

For example: 12 ÷ (6 ÷ 2) = 4 but (12 ÷ 6) ÷ 2 = 1

12 ÷ (6 ÷ 2) ≠ (12 ÷ 6) ÷ 2

In set theory the following operations are commutative:

Union

$$A \cup B = B \cup A$$

Intersection

$$A \cap B = B \cap A$$

The following operations are *not* commutative:

Difference

$$A \setminus B \neq B \setminus A$$

Cartesian product

$$A \text{ x } B \neq B \text{ x } A$$

The following set operations are associative:

Union

$$(A \cup B) \cup C = A \cup (B \cup C)$$

Intersection

$$(A \cap B) \cap C = A \cap (B \cap C)$$

The following set operation is *not* associative:

Difference

$$(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$$

Is Cartesian product is associative?

If Cartesian product is associative then: $(A \text{ x } B) \text{ x } C = A \text{ x } (B \text{ x } C)$

Strictly speaking it is *not* associative:

Let $A = \{a, m, n\}$ $B = \{b, x, y\}$ $C = \{c, d, e, f, g\}$

The left hand side would give us:

$$\{((a, b), c), ((a, b), d), ((a, b), e) \text{ .... } \}$$

The right side would give as a set such as:

$$\{(a, (b, c)), (a, (b, d)), (a, (b, e)) \text{ .... } \}$$

However, we often assume that the Cartesian product of three sets just gives as triples.

In this case it *is* associative as both sides would gives us:

$$\{(a, b, c), (a, b, d), (a, b, e) \text{ .... } \}$$

Groups

- a group is a **set** combined with an **operation**;

For example

the *set* of integers with the *operation* addition

- however, a set and an operation do not constitute a group unless it satisfies the following criteria:

1. The group contains an **identity.**
2. The group contains **inverses.**
3. The operation is **associative.**
4. The group is **closed** under the operation.

- we will now explore each of these in turn.

A group must contain an identity

- if the operation is applied to any element and the identity, the element will be unchanged

<u>For example</u>

For the set of *integers* and *addition*, the identity is 0:

$5 + 0 = 5$	$0 + 5 = 5$	
$7 + 0 = 7$	$0 + 7 = 7$	
$-5 + 0 = -5$	$-5 + 0 = -5$	etc

- the identity element must be an element of the set;
- there is only one identity element for every group;
- the symbol that is usually used for the identity element is *e.*

Formally:

For a set G under the operation *:

There exists an e in G, such that $a * e = a$ and $e * a = a$, for all elements a in G

A group must contain inverses

- for every element of the group, there's another element of the group such that when we use the operator on both of them, we get *e*, the identity.

For example

For the *integers* and *addition*, the inverse of 5 is -5 (because 5 + -5 = 0)
the inverse of -5 is 5
etc

- if a is the inverse of b, then it must be that b is the inverse of a;
- inverses are unique – for example, there is no other x, apart from -5, such that 5 + x = 0;

Notation

- the inverse of a is written as a^{-1}; in the above example, $a^{-1} = b$.

Formally:

For all a in G, there exists a b in G, such that $a * b = e$ and $b * a = e$.

A group must be associative

- we already know the meaning of this.

For example

For the set of integers, addition is an associative operation.

Formally:

For all a, b, and c in G, a * (b * c) = (a * b) * c

A group must be closed under the operation

- if there are two elements in the group, a and b, and * represents the operation, then it must be the case that $a * b$ is also in the group.

- we say that the group is **closed** under the operation.

For example

With integers and addition, then the group is closed because whatever the value of and a and b, $a + b$ is always an integer.

Formally:

For all a, b in G, $a * b$ is in G

We see that the group integers with addition is formally a group because it has all of the required properties.

Notation and terminology

You will often see a group written like this: $(G, *)$

where G represents the set, and * the operation.

For example:

The set of integers with addition: $(\mathbb{Z}, +)$

The set {1} with multiplication: ({1}, x)

Note

1. Sometimes you will see the symbol $\circ$ used instead of *.

2. If a group is also commutative, it is referred to as an **abelian** group.

3. A group that has associativity and closure only is called a **semigroup**.

4. A semigroup that has an identity element is called a **monoid**.

Worked examples

1. Is the set {-1, 1} under multiplication a group?

Solution

Is there an identity element?

The identity element is 1 because 1 x 1 = 1 and -1 x 1 = -1.

Are there inverses?

1 x 1 = 1 and -1 x -1 = 1, so there is an inverse for each element.

Is the operation associative?

We already know that multiplication is associative with any integers.

Is there closure?

It is closed because the results of all of the following are in the group:

1 x 1   -1 x -1   1 x -1   -1 x 1

Therefore the set {-1, 1} under multiplication is a group.

2. Is the set {-1, 0, 1} under addition a group?

Solution

Is there an identity element?

The identity element is 0.

Are there inverses?

-1 + 1 = 0, 1 + -1 = 0 and 0 + 0 = 0, so there is an inverse for each element.

Is the operation associative?

We already know that addition is associative with any integers.

Is there closure?

It is not closed because the result of adding -1 to itself is not in the group, neither is the result of adding 1 to itself.

Therefore the set {-1, 0, 1} under addition is not a group.

3. Is the set of integers under multiplication a group?

Solution

Is there an identity element?

The identity element is 1.

Are there inverses?

If you take an integer such as 7, there is no integer that will result in 1 if multiplied by 7.

This applies to all integers except 1.

So it does not satisfy the inverse property

The set of integers under multiplication is therefore not a group.

4. Is the set of rational numbers excluding zero under multiplication a group?

Solution

Is there an identity element?

The identity element is 1.

Are there inverses?

We can find an inverse for every element.

For example: The inverse of $\frac{5}{7}$ is $\frac{7}{5}$ because $\frac{5}{7} \times \frac{7}{5} = 1.$

The same applies to every rational number (excluding zero)

Is the operation associative?

We already know that addition is associative with all numbers.

Is there closure?

It is closed because the result of any possible multiplication always results in another rational number:

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Therefore the set of rational numbers excluding zero under multiplication is a group.

But notice that if we include zero, it is not a group because there is no inverse for zero.