Further Pure 3 Notes

Jacob Santry

June 28, 2017

Contents

Group Theory **1**
1.1 Background Work 1
1.2 Modulo Arithmetic 2

Group Theory

1.1 Background Work

Set Notation

$$A = \{\text{Colours of the rainbow}\}$$

$$\mathit{Red} \underset{\substack{\uparrow \\ \text{Is an element of.}}}{\in} A$$

$$\text{or } B\{2, 5, 11, 17\}$$

$$\text{or } C = \{x \underset{\substack{\uparrow \\ \text{Such that.}}}{:} x > 2\}$$

Special sets

$\mathbb{R}$={Real numbers}
$\mathbb{C}$={Complex numbers}
$\mathbb{Z}$={Integers}
$\mathbb{Z}^+$={Real numbers}
$\big[$ also N={Natural numbers} $\big]$
$\mathbb{Q}$={Rational numbers}

Binary Operations

The operation, * , acts on the two elements of a set to produce a unique "product" (i.e. outcome).

Properties of Binary Operations

1. Commutivity: an operation, *, is communative iff

$$x * y = y * x \quad \forall x, y.$$

2. Associativity: operation, *, is associative iff

$$x * (y * z) = (x * y) * z \quad \forall x, y, z$$

3. Distributive property: operation, *, is distributive over operation $\circ$, iff

$$x * (y \circ z) = (x * y) \circ (x * z) \quad \forall x, y, z$$

1.2 Modulo Arithmetic

Aritmetic modulo n returns the remainder after division by n.

e.g.

$$3 +_6 5 = 2$$

$$3 \times_6 5 = 3$$

both of these calculations are restricted to the set $\mathbb{Z}_6$ = {0,1,2,3,4,5}
so $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Definitions of a group

A group, G, consist of a set, S, together with an operation,x.
The following criteria must be satisfied

1. Closed: i.e.
$$x * y \in S \quad \forall x, y \in S.$$
2. Associative: i.e.
$$x * (y * z) = (x * y) * z \quad \forall x, y, z \in S.$$
3. Identity: i.e.
$$\exists e \in S \quad \text{st. } x * e = e * x = x \quad x \in S.$$
4. Inverse: i.e.
$$\forall x \in S \quad \exists x^{-1} \quad \text{st. } x * x^{-1} = x^{-1} * x = e.$$

If, in addition, a group is commutative it is known as an Abelion group.

Finite groups

e.g. To show that $\mathbb{Z}_4$ together with $+_4$ form a group.

$+_4$	0	1	2	3
0	0	2	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1. Closed ✓by inspection
2. Associative ✓because addition of integers if associative.
3. Identity ✓e=0
4. Inverse

$$0^{-1} = 0$$
$$1^{-1} = 3$$
$$2^{-1} = \underset{\uparrow}{2}$$

2 is a self-inverse element.

$$3^{-1} = 1$$

$\therefore$ (Z_4,$+_4$) is a group. This group is also commuattive- it has a symetry about the leading diagonal. An operation table like this is known as a Cayley Table and if it represents a group it must exhibit the properties of a Latin Square (i.e. each of the elements exactly once in every row and column).

Order of a group

The order of a group os the number of elements it contains.