First lecture

[Home][PDF]

Topics: Groups, Cyclic Groups

Disclaimer: There may be errors her, please report them to me, and if the equations look to terrible, check out the PDF.

Groups we already know

$\mathbb{N}$ = {1,2,3,...} Natural numbers

$\mathbb{Z}$ = {...,-2,-1,0,1,2,...} all integers positive and negative

$\mathbb{Q}$ = { $\frac{p}{q}$: $p, q \in \mathbb{Z}$ }

$\mathbb{R}$ = {0.1, 0.0 , 0.11, $\sqrt{1}, \pi$ }

Relations: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Operations

Addidtion $+$ and substraction $-$ Multiplication $\cdot$ divivsion $\div$

$$a - b = a + (-b)$$

$$a \div b = a * \frac{1}{b}$$

Properties

Commutativity

We have for addition $a + b = b + a$ and multiplication $a \cdot b = b \cdot a$ and is called commutativity when $\forall a, b$

Associative

We have for addition $a + (b + c) = (a + b) + c$ and for multiplication $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Distributivity

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

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

Binary Operations

Let $\mathbb{S}$ be a set of elements, with the binary operation $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

Then we have that:

$$\varphi(a, b) = c$$

$$a, b, c \in \mathbb{S}$$

Ternary Operations

$$\varphi : \mathbb{S} \times \mathbb{S} \times \mathbb{S} \rightarrow \mathbb{S}$$

$$\varphi(a, b, c) = d$$

$$a, b, c, d \in \mathbb{S}$$

This can be extended to a n-ary operation

$$\varphi : \mathbb{S}_\mathbf{1} \times \mathbb{S}_\mathbf{2} \times \ldots \times \mathbb{S}_\mathbf{n}$$

$$n \in \mathbb{N}$$

Algebraic System / Structure $< S, P >$

Algebraic system with the symbol $*$ as a binary operation. Here S is called the groupoid.

$$< S, * >$$

S a groupoid where the assosiative laws holds, is called a semigroupoid.

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

$$\forall a, b, c$$

S is a semigroup with $e \in S$ s.t $e \times a = a \times e = a, \forall a$ is called a monoide.

e is called an identity element.

If S is a monoid and $\forall a \in S, \exists a^{-1} \in S$ s.t $a \times a^{-1} \wedge a^{-1} \times a = e$ Then S is called a group.

a^{-1} is called the inverse element of a.

Definition of a group

$\langle G, * \rangle$ with a binary operation $*$, is called a group if the following holds:

i) $\forall a, b, c \in G$ we have that $a * (b * c) = (a * b) * c$

ii) $\forall a \in G, \exists e \in G$ we have that $e * a = a * e = a$

iii) $\forall a \in G, \exists a^{-1}$ such that $a * a^{-1} = a^{-1} * a = e$

If a groups is also commutative, then it is called an abelian group. Then this also applies to the group.

iv) $a * b = b * a$

Proof: Identity element of a group is unique

The identity element e of a group G is unique.

$$\exists e_1, e_2 \in G$$

$$e_1 \times a = a \times e_1$$

$$e_2 \times a = a \times e_2$$

$$\implies e_1 = e_1 \times e_2 = e_2$$

$$\square$$

The inverse element is unique $\forall a \in G$ in group G.

Proof: Inverse element $\forall a \in G$ is unique

Let a be an element in G, $a \in G$,

Assume we have to inverse elements a^{-1} and a_1^{-1}, for a^{-1} and a_1^{-1} the following holds.

$$(a^{-1} \times a = a \times a^{-1} = e$$

$$a_1^{-1} \times a = a \times a_1^{-1} = e$$

To show that a only has one inverse element.

$$a^{-1} \times a = e$$

$$(a^{-1} \times a) \times a_1^{-1} = e \times a_1^{-1}$$

$$a^{-1} \times (a \times a_1^{-1}) = a_1^{-1}$$

$$a^{-1} \times e = a_1^{-1}$$

$$a^{-1} = a_1^{-1}$$

$$\square$$

If there is two inverse elements, they are the same element.

The identity e of a group G is unique, The inverse element is unique $\forall a \in G$ in group G

Then $\forall a, b$ we have the following

$$(a \times b)^{-1} = b^{-1} \times a^{-1}$$

We can then show that:

$$(a \times b)^{-1} \times (a \times b) = e$$

$$(b^{-1} \times a^{-1}) \times (a \times b) = b^{-1} \times (a^{-1} \times a) \times b^{-1}$$

$$RHS = b^{-1} \times e \times b$$

$$= b^{-1} \times b$$

$$(b^{-1} \times a^{-1}) \times (a \times b) = e$$

$$\square$$

$*$ Operator

The $*$ operator will be replaced by either $+$ or $\cdot$ for their repective operation, $\cdot$ => multiplication, and $+$ for addition.

Multiplicative notation

$$* := \cdot$$

$$e = 1 \text{ (the identity element)}$$

$$a^{-1} \text{ (the inverse element)}$$

$$a \cdot b = ab$$

$$a_1 a_2 \cdot \ldots \cdot a_n$$

$$a \cdot a \cdot \ldots \cdot a = a^n$$

$$(-a) \cdot (-a) \cdot \ldots \cdot (-a) = (-a)^n$$

$$(-a^{-1}) \cdot (-a^{-1}) \cdot \ldots \cdot (-a^{-1}) = (-a)^{-n}$$

$$a^0 = e$$

$$a^n, n \in \mathbb{Z}$$

$$\forall n, m \in \mathbb{Z} \text{ we haven } a^n \cdot a^m + a^{a+m}$$

$$(a^n)^m = a^{n \cdot m}$$

$$n \cdot (m \cdot a) = (n \cdot m) \cdot a$$

Additive notation

$$* := +$$

$$e = 0 \text{ (the identity element)}$$

$$-a \text{ (the inverse element)}$$

$$0 \cdot a = 0$$

$$a_1 + a_2 + \ldots + a_n$$

$$a_1 + a_2 + \ldots + a_n = n \cdot a$$

$$n \cdot a + m \cdot a = (n + m) \cdot a$$

Example: $\mathbb{Z}$

$\langle \mathbb{Z}, + \rangle$ is a group, it must fulfil the group definition.

i) $\forall a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$ //OK

ii) $e = 0$ for addetive groups $a + e = a \iff e = 0$ //OK

iii) If a is an element in $\mathbb{Z}$, $a \in \mathbb{Z}$ then it has an inverse s.t the following holds:

$$a^{-1} + a = e$$

$$(-a) + a = 0$$

All tree rules holds, it is a group.

Example: Trivial Group

In a trivial group, the identity element must exists.

$$G = e$$

$$e * e = e$$

Example: $\mathbb{Q}$

Is $\langle \mathbb{Q}, + \rangle$ a group? All three rules holds for this group, so yeas this is a group.

Is $\langle \mathbb{Q}, \cdot \rangle$ a group? Associative property holds Identity property $e = 1$ for multiplicative groups.

Inverse Element: For $\mathbb{Q}$ we have that $a = \frac{p}{p}$ then the inverse element is $a^{-1} = \frac{q}{p}$. If $p = 0$ then a^{-1} is not a number ($p = 0 \rightarrow \frac{q}{0} = NaN$), and hence $\langle \mathbb{Q}, \cdot \rangle$ cannot be a group.

Example: G with 6 elements

Let G be the set of remainders of all the integers on division by 6, this group contains of 6 elements and is:

$$G = 0, 1, 2, 3, 4, 5$$

Not sure why this got noted:

An element $m \in \mathbb{Z}$ is defined as follows:

$m = g \cdot q + r$ where $q \in \mathbb{Z} \text{ and } 0 \leq r \leq 5$