Group Theory , Explained I

March 19, 2013

Group Theory is the simplest part of *abstract algebra*. Different from *tangible algebra* , abstract algebra deal with algebraic structrue, which is very abstract. But abstract algebra is very useful. Thus it is worth to spend efforts to learn it.

In formal abstract algebra text books, the text is full of mathematical definitions, people who get used to applied mathematics can hardly get what it means.

These definitions are very important , and not useless / stupid . They hold certain important meaning. In this short notes, I try to give some suggestions that why those definitions are necessary and why they are defined in such way.

1 Close

Definition 1. For a set S, an operation $\circ$, the set S is said to be *close* on operation $\circ$ if $\forall a, b \in S \implies a \circ b \in S$

Explanation

A set S is a collection of something, for example, number.

If we have a set S with its element , and that's it, it will be very boring.

Then why don't we include some *operation* on the set ?

There are lots of operation (e.g.$+$, $-$, $\surd$, $!$). Some of them works on only ONE object (e.g. $4! = 4 \cdot 3 \cdot 2 \cdot 1$, $\sqrt{8} = 2\sqrt{2}$), they are called *uniary operation*.

Some operation involve TWO object , thet are called *binary operation*.

Then for a binary operation , there are so many binary operation (e.g. $+$, $-$, $\cdot$, *mod* , *GCD*, log) , we just use a symbol $\circ$ to denote them.

Then, it seems natural that if the result after operation is still inside the set, that operation is "good".

Example 2. Consider the set of positive number $\mathbb{R}^+$, for the operation $\times$, it is so obvious that $\mathbb{R}^+$ is close in operation $\times$. Can you find 2 number , both are positive, that their product is negative (thus outside the set $\mathbb{R}^+$) ?

Example 3. Another example, $\mathbb{R}^-$ is not close in operation $\times$. ($(-a) \times (-b) = +ab \notin \mathbb{R}^-$!)

Example 4. Real number is not close in operation $\log_a b$: $\log_e(-3) = \ln|-3| + 2\pi i \notin \mathbb{R}$

2 Associative

Definition 5. For a set S , S is associative on operation $\circ$ if $\forall a, b, c \in S$, $(a \circ b) \circ c = a \circ (b \circ c)$

Explanation

One we have the operation on 2 elements in a set , what about operation on 3 elements ? It is natural to think that $a \circ b \circ c$ can be calculated in any order such as calculate the first pair of element $a \circ b \circ c = (a \circ b) \circ c$ or calculate the last pair of element first $a \circ b \circ c = a \circ (b \circ c)$

If this does not hold, then $a \circ a \circ a =$? Since this time $(a \circ a) \circ a \neq a \circ (a \circ a)$.

Thus this is important that the operation $\circ$ is accosicative.

3 Semi-Group

Definition 6. For a set S, if S is associative and close on operation $\circ$, S is a semi-group.

Explanation

This is just giving name for the sets that fulfill the 2 requirements.

4 Identitity Element and Inverse

Definition 7. For a set S that if there is an element , denoted as e , such that $e \circ a = a \circ e = a$ $\forall a \in S$, then such element is called the *identity*.

Definition 8. For a set S that $\forall a \in S$, there is always an element $b \in S$ such that $a \circ b = b \circ a = e$, then b is called the *inverse* of a, and usually denoted as a^{-1}

Explanation

1. e is fix, unique, never change.
2. Different a has different inverse, and a^{-1} is not necessary means $\frac{1}{a}$!
3. The inverse has to be also inside the set S , thus for some operations that is not close in the set, there is no inverse.

Example 9. The set of real number and operation + : ($\mathbb{R}$, +) has identity element as 0 : $0 + a = a + 0 = a$.

Example 10. For set of integer and operation $\times$: $(\mathbb{Z}, \times)$, it has identity element as 1

Example 11. For set of positive integer and operation $-$: $(\mathbb{Z}^+, -)$, there is no inverse. $-a \in \mathbb{Z}^+$. Since $\mathbb{Z}^-$ is not close on operation $-$.

5 Group

Definition 12. A set G and a operation $*$, denoted as $(G, *)$ is a group if

1. Close : $\forall a, b \in G$, $a * b \in G$
2. Associative : $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$
3. $\exists e \in G$ *s.t.* $g * e = e * g = g$, $\forall g \in G$
4. $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $g * g^{-1} = g^{-1} * g = e$

Example 13. For set of positive integer and operation $\times$: $(\mathbb{Z}^+, -)$

1. It is close on $\times$
2. It is associative on $\times$
3. There is identity element , whihc is 1
4. There is no inverse, for example, the inverse of 4 is not inside the set

6 Commutative

$a * b = b * a$ is not required in Group Definition.

Definition 14. The set S , operation $*$, is *commutative* if $\forall a, b \in S$, $a * b = b * a$

Definition 15. For the group that is commutative on its operation, the group is called *abelian group*

7 Order

A group is a set and a operation. The number of element inside the set is the order of the group. If the set is finite, the group is a finite group.

Definition 16. For group with n element, the order of the group is n , denoted as $|G| = n$.

8 Some corollaries

1. Identity element is unique
2. Inverse is unique
3. $(a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$
5. $\forall a, b \in G$, $ax = b$ and $ya = b$ both has unique solution.

$-END-$