An Introduction to Group Theory

Tarik Adnan Moon, Bangladesh.

November 22, 2008

Abstract

In this article I'll discuss some topics on Group theory which is a very important topic in mathematics.

Let's see what a group actually is. We start with formal definition.
Group:
A Group is a set G with a binary operation (defined by $*$) which satisfies the following axioms:

1. **Closure:** if $g, h \in G$ then $g * h \in G$,
2. **Associativity:** $f * (g * h) = (f * g) * h \quad \forall \quad f, g, h \in G$
3. **Identity:** There is an element $e \in G$ such that, $g * e = g = e * g$
4. **Inverses:** For each $g \in G$ there is an element $h \in G$ such that $g * h = e = h * g$
   [note that: this doesn't say that this group is abelian i.e. it commutes]

Now lets prove something with this. We start with a classical exercise.

Exercise 1: We denote the set of all the units in Z_n by U_n. Prove that, U_n forms a group under multiplication $\mod n$ with identity [1].

Solution: Here the binary operation is simple multiplication. It is enough to show that U_n satisfies all 4 axioms of being a group.
For **closure:** we see that, the product of two units $[a], [b]$ is also a unit. So, $[a][b] = [ab]$ is also a unit. Now, we know that, $[a], [b]$ has inverses $[u], [v]$ such that,

$$[a][u] \equiv 1 \mod n \quad \text{and} \quad [b][v] \equiv 1 \mod n$$

Joining these results we get,

$$[ab][uv] = [abuv] = [aubv] = [au][bv] = [1]^2 = [1]$$

So, $[ab]$ has inverse $[uv]$ so it is also a unit. i.e. $[ab] \in U_n$ (We are doing all these stupid looking calculation because we have to do everything using axioms. As we can't directly say that, $x * y = y * x$ etc.)
Here **Associativity** is easily seen, $[a]([b][c]) = ([a][b])[c] \iff [a(bc)] = [(ab)c]$ for all units $[a], [b], [c] \in U_n$ and the **identity** is [1], and it follows from,

$$[a][1] = [a] = [1][a]$$

Now the last one, existence **inverse**. And we know that for all $[a] \in U_n$ there exists some $[u] \in Z_n$ such that, $[a][u] = [1]$ and we know that $[a] \in U_n$. So we are done at last.

We can simply write the products $g * h = gh$ and $g * g * \cdots * g$ (where there are i gs) we can write it g^i. (Here $i \in N$) And the inverse is often denoted as $h = g^{-1}$. The **order of a group**

G is the number of elements of the set G which is denoted as $|G|$. If the order of a group is finite we call it **finite group.**

Now we study more specific groups.

Commutative groups (abelian group): We call a group abelian if all the elements of commutes i.e. it satisfies,

$$gh = hg \equiv 1 \mod n \quad \forall \quad g, h \in G$$

Exercise 2: Prove that, U_n is an abelian group.

Solution: For $[x], [y] \in U_n$ we have,

$$[x][y] = [xy] \quad \text{ and } \quad [y][x] = [yx] = [xy]$$

So, $[x][y] = [y][x]$ that is U_n is abelian.

Now we should discuss some more points on group theory. Like subsets, in group theory we have **Sub groups**.

Subgroup is a subset G and H which itself is a group with respect to the same binary operation as G and it is equivalent to satisfying the conditions:

1. If $g, h \in H$ then $gh \in H$
2. $1 \in H$
3. If $g \in H$ then $g^{-1} \in H$

Here we can write $H \leq G$ and say that H is a subgroup of G. Now we define two things, **right cosets** and **left cosets**. If $H \leq G$ and $g \in G$, then the right coset of H containing g is the subset, $Hg = \{hg \mid h \in H\}$. So, each right coset of H contains $|H|$ elements. Right cosets Hg_1 and hg_2 are either equal or disjoint, so they partition G into disjoint subsets. The number of disjoint right cosets of H in G is called the index $|G : H|$ of H in G. If G is finite then, we can write, $|G| = |G : H|.|H| \cdots\cdots (*)$

Similarly, we can define left cosets, $gH = \{gh \mid h \in H\}$

Surprisingly enough, we have already proved one of the most useful theorem of group theory named **Lagange's Theorem**

Lagrange's theorem says: *For any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.*

Which follows from $(*)$

Application of **Lagrange's Theorem**:

The order of an element $g \in G$ is the least integer $n > 1$ such that, $g^n = 1$ (provided that such an integer n exists, if it does not then g has infinite order. Why? just remember the closure axiom) If G is finite then every elment g has finite order n for some integer n. the powers $g, g^2 \cdots, g^{n-1}, g^n (= 1)$ forms a subgroup of G.

So, n divides $|G|$ by Lagrange's theorem.

Now, lets see some some more examples which are probably a bit "olympiad oriented"

Exercise 3 (Euler's Function):

If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \mod n$

Solution: We have already showed that, U_n is a group under multiplication. Since the group has order $\phi(n)$ i.e. $|U_n| = \phi(n)$, by Lagrange's theorem,

$$[a]^{\phi(n)} \equiv [1] \mod n$$

Now a more Olympiad oriented problem.

Exercise 4 : If $(a, b) = 1$ then $2^a - 1$ and $2^b - 1$ are coprimes as well.

Solution: Let n be the highest common factor of $2^a - 1$ and $2^b - 1$. As n is odd 2 is a unit $\in Z_n$. Let $ord_n = k$; and $n|2^a - 1$ which implies that, $2^a = 1$ in U_n and it implies that, $k|a$ and similar argument shows that $k|b$. So, $n|\gcd(a, b) = 1$ so, $k = 1$ and $2^1 \equiv 1 \mod (n)$ so, $n = 1$ as required.

References

[1] A. Jones and Mary Jones, *Elementary Number Theory.*

[2] W. Ledermann, *Introduction to Group theory.*

[3] Wikipedia.