Group Theory

Lecture 3, Sunday November 6, 2022
Ari Feiglin

Note:

I was not present at this lecture, and so this summary was written based off of someone else's who was.

From now on, instead of writing $a \circ b$, I will simply write ab for a group's operation.

Definition 2.0.1:

G is an **abelian group** (or G is abelian) if G is a group and for every $a, b \in G$, $ab = ba$.

Thus $\mathbb{Z}$, $\mathbb{Z}_n$, and $\mathrm{Euler}(n)$ are all examples of abelian groups.
We will further define exponentiation in groups. For $a \in G$, we define $a^0 = e$ (where $e \in G$ is the identity) and for $n \in \mathbb{N}$: $a^{n+1} = a^n a$. Thus $a^n = \underbrace{a \cdots a}_{n \text{ times}}$. We further define $a^{-n} = \left(a^{-1}\right)^n$. The ordinary rules for exponentiation hold here:

$$\left(a^n\right)^m = a^{nm} \qquad a^n a^m = a^{n+m}$$

Moreso, in an abelian group $(ab)^n = a^n b^n$.

Proposition 2.0.2:

Let G be a group then for every $a, b \in G$, $(ab)^2 = a^2 b^2$ if and only if G is abelian.

Proof:

If G is abelian, then this is trivial. Let's show the converse. Let $a, b \in G$ then $(ab)^2 = abab$ and so:

$$abab = a^2 b^2$$

So multiplying the left by a^{-1} and the right by b^{-1} gives

$$ba = ab$$

As required.

■

Definition 2.0.3:

The **order** of an element $a \in G$ is the minimum integer $n > 0$ such that $a^n = e$. If such a number does not exist, then the order is defined to be ∞. The order of a is denoted by $o(a)$, and sometimes $|a|$.

For example:
- $o(7) = \infty$ in $\mathbb{Z}$.
- $o(7) = 2$ in $\mathrm{Euler}(8)$ (since $7^2 = 49 \equiv 1 \pmod 8$)
- $o(1) = n$ in $\mathbb{Z}_n$ (since $1 + \cdots + 1 = n$)

Proposition 2.0.4:

Suppose $g \in G$ is of finite order, then $g^m = e$ if and only if $o(g) \mid m$.

Proof:

Let $o = o(g)$. Suppose $g^m = e$, then by the quotient rule $m = qo + r$ for some q and $0 \leq r < o$, then:

$$g^m = (g^o)^q g^r = e^q g^r = g^r$$

Since $0 \leq r < o$, and o is the minimum number such that $g^o = e$, this can equal e only if $r = 0$, and thus o divides m. To prove the converse, suppose $o \mid m$, so $m = qo$. And so:

$$g^m = g^{qo} = (g^o)^q = e$$

As required.

■