Lecture 3: Mathematical preliminaries : Groups

A quick intro of groups

<u>Def 1</u>: A group $(G,+)$ is a set G and operation '+' that obey:

(i) For any $a,b \in G$, we have $a+b \in G$ (Closure)

(ii) For any $a,b,c \in G$, we have $(a+b)+c = a+(b+c)$ (Associativity)

(iii) $\exists$ an element $0 \in G$ s.t. $a+0 = 0+a = a, \forall a \in G$ (Existence of identity)

(iv) For each element $a \in G$, $\exists$ an element $(-a) \in G$ s.t $a+(-a) = (-a)+a = 0$ (Existence of inverse)

<u>Remark</u>: We will only consider <u>abelian</u> groups G that are <u>commutative</u>.

<u>Eg</u>: The set of integers $\mathbb{Z}$ (under +), the set of reals $\mathbb{R}$ (under +), the set of rationals $\mathbb{Q}$ (under +)

<u>Q</u>: Can these groups above be modified to also be groups under the standard multiplication operation?

<u>HW 1</u>: (i) Prove that the inverse $(-a)$ of an element a and the identity element 0 are <u>unique</u>.

(ii) Prove that the set

$$a+G \triangleq \{a+g : g \in G\}$$

equals G itself.

(iii) Consider a "cyclic group" G with a generator $g \in G$ such that any element $a \in G$ can be written as

$$a = \overbrace{\underbrace{g + g + \cdots + g}_{K \text{ times}}}^{\triangleq Kg}, \text{ for some } K.$$

Let n be the smallest integer such that $ng = 0$.

Show that $\{g, 2g, 3g, \ldots, ng = 0\}$ equals G.

[Eg: Given $\omega = e^{i2\pi/n}$, the set $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ is a cyclic group generated by ω under complex multiplication]

Def (Order): The order of a group $(G,+)$ equals $|G|$.

Def (Subgroup): A subgroup $(S,+)$ of the group $(G,+)$ is a group with $S \subseteq G$.

Eg: $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$, which in turn, is a subgroup of $(\mathbb{R},+)$.

Def (Coset): Let $(S,+)$ be a subgroup of $(G,+)$.

A coset (or translate) of the group $(S,+)$ is a set of the form

$$g + S \triangleq \{g + s : s \in S\},$$

for some $g \in G$.

Remark: If $g \in S$, then $g + S = S$.

Thm 1: Two cosets are either disjoint or identical

Proof: Consider cosets g_1+S and g_2+S, for some $g_1, g_2 \in G$.

Suppose that $g_1-g_2 \in S$. Then, $g_1 \in g_2+S$ and $g_2 \in g_1+S$ (Why?)

Thus, $g_1+S \subseteq g_2+S$ and $g_2+S \subseteq g_1+S$, giving rise to

$g_1+S = g_2+S$.

Else, suppose that $g_1-g_2 \notin S$. Then, if g_1+S and g_2+S have any element h in common, then $h-g_1 \in S$ and $h-g_2 \in S$

$$\Downarrow$$

$$g_1-g_2 \in S$$

[Contradiction!] ∎

Thm 2: If S is a subgroup of a finite group G, then $|S| \mid |G|$.

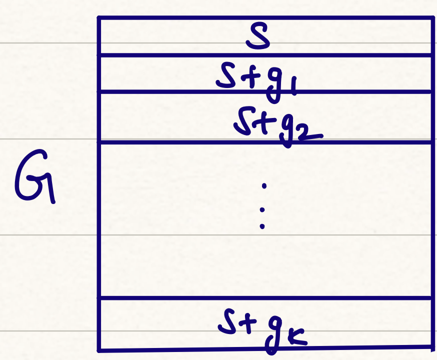
[Lagrange's Thm.]

Lemma 3: All cosets of S in G are of the same size.

Proof: HW / discussion.

Proof of Thm 2: Putting together Thm 1 and Lemma 3, we see that since

(picture)



, we must have $|S| \mid |G|$.

Example : Consider the group $\mathbb{Z}_n$ of integers modulo n. [Prove that this is a group!]

Note that $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Let S be a "cyclic subgroup" of $\mathbb{Z}_n$ with generator m, i.e (see HW above), $S = \{0, m, 2m, \ldots, (k-1)m\}$, where km is the least integer s.t. $km \equiv 0 \pmod{n}$, i.e., km is the LCM of m and n. k is also called the "order of m".

We know that $km = \frac{mn}{\gcd(m,n)} \equiv \boxed{|S| = k = \frac{n}{\gcd(m,n)}}$

HW : Within $\mathbb{Z}_{20}$, find subgroups of order 2, 4, and 5.

Def (Euler totient function): The Euler totient function $\phi : \mathbb{N} \to \mathbb{N}$ is such that $\phi(d)$ is the number of integers relatively prime to d.

Example. In $\mathbb{Z}_n$, let $d|n$. Consider the collection

$$S_d = \{e : e = \frac{ln}{d}, \text{ for some } l \in [d] \text{ relatively prime to } d\}.$$

S_d is the collection of elements of order d in $\mathbb{Z}_n$.

The number of elements in this collection is $|S_d| = \phi(n/d)$.

Since the coll^{n}s $(S_d : d \in [n], d|n)$ are pairwise disjoint (Why?) and their union is [n] (Why?), we must have

$$\boxed{n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)}$$

HW for a generic cyclic group G.

Def (coset leader): A coset leader / representative of a coset is any element of a coset.

Remark: 0 is a coset leader of a subgroup $S \subseteq G$.