# LECTURE 20

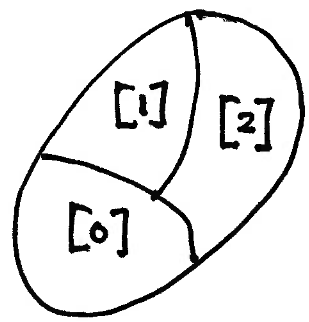
(Monday Nov. 18, 2019)

REMINDER: $(\mathbb{Z}, +)$ additive group. Fix $N > 0$.
For $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod N \iff b - a \in N\mathbb{Z}.$$

gives equivalence relation on $\mathbb{Z}$, whose classes are residue classes:

$N = 3$:




$$[a] = \{ b \in \mathbb{Z} : b \equiv a \pmod N \}$$
$$= \{ a + Nq : q \in \mathbb{Z} \}$$
$$= a + N\mathbb{Z}.$$

Partition $\mathbb{Z}$ into $N$ "boxes of numbers"

$$\mathbb{Z}_N = \{ [0], [1], \ldots, [N-1] \}$$ (has addition & multiplication).

Also, $[a] = [b] \iff a \equiv b \pmod N$.

—— GOAL is to generalize this to any group $G$ with a subgroup $H \leq G$.
(above: $G = \mathbb{Z}$ and $H = N\mathbb{Z}$)

Def. For $a, b \in G$,

$$a \sim b \iff a^{-1} * b \in H.$$

– This defines an equivalence relation on $G$:

(1) Reflexive: $a \sim a$

(indeed $a^{-1} * a = e \in H$)

(2) Symmetric: $a \sim b \implies b \sim a$

(knowing $a^{-1} * b \in H$ implies its inverse lies in $H$:

$$(a^{-1} * b)^{-1} = b^{-1} * a)$$

(3) Transitive: $a \sim b$ and $b \sim c \implies a \sim c$.

(we're assuming $a^{-1} * b \in H$ and $b^{-1} * c \in H$.

Since $H$ is closed under $*$, their composition still lies in $H$:

$$(a^{-1} * b) * (b^{-1} * c) = a^{-1} * c.)$$

Def. The equivalence class of $a \in G$ is the subset

$$[a] = \{b \in G : b \sim a\}$$
$$= \{a * h : h \in H\}$$
$$= a * H$$

– This is known as the (left) "COSET" containing $a$.

NOTE: $[e] = e * H = H$.

Remark: $a \equiv b \iff a*b^{-1} \in H$
also def. an equivalence relation on $G$, with classes $[a] = \{h*a : h \in H\} = H*a$
— the right coset containing $a$.

— Usually we take left cosets unless othw. specified.

Lemma: For $a, b \in G$,

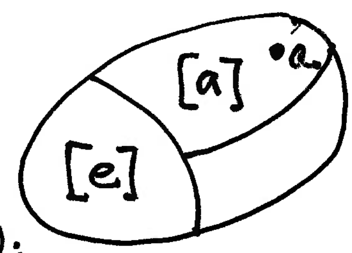
(i) $[a] = [b] \iff a \sim b$.

(ii) $[a] \cap [b] \neq \emptyset \implies [a] = [b]$.

PF. Standard argument (omit), cf. congruences mod $N$. $\square$

— In particular the cosets $[a]$ form a partition of $G$.

Remark: $[a] = a*H$ is not a subgroup unless $a \in H$.
$(e \in [a] \iff a \sim e \iff a \in H)$




(i): $a*H = b*H \iff a^{-1}*b \in H$.

Def:

$G/H = \{a*H : a \in G\}$

family of all left cosets.

— The index of $H$ in $G$ is the number of cosets:

• EX $\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_N$

equality! (not just isomorphic)

Index:

$$[G:H] \overset{\text{definition}}{=\!=} |G/H|. \qquad (\leq \infty).$$

LAGRANGE'S Theorem: ("index formula") Suppose $|G| < \infty$.

Let $H \leqslant G$ be any subgroup. Then $|H|$ divides $|G|$, and

$$\frac{|G|}{|H|} = [G:H].$$

know this for cyclic $G$.

PROOF. First observe that all cosets have the same size, namely $|H|$:

$$\begin{aligned} H &\longrightarrow a*H \\ h &\longmapsto a*h \end{aligned}$$

is a bijection (surjective by very def. of $a*H$, injective by the cancellation law:

$$a*h_1 = a*h_2 \Rightarrow h_1 = h_2)$$

- Follows that the sets must have the same cardinality: $|H| = |a*H|$.

NOW, decompose $G$ into (disjoint) cosets.

$$G = a_1*H \cup a_2*H \cup \cdots \cup a_N*H$$

(compare to $\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [N-1]$.)

Here $N = \#\text{cosets} = |G/H| = [G:H]$ (index)

Count:

$$|G| = \sum_{i=1}^{N} |a_i * H| \underset{\substack{\uparrow \\ 1^{st}\text{ obs.}}}{=} \sum_{i=1}^{N} |H| = N \cdot |H|.$$

- verifies that $|H|$ divides $|G|$, and

$|G| = [G:H] \cdot |H|$. $\square$

EX. $G = \mathbb{R}^2$ with (vector) addition. Fix $v \neq 0$

$H = \text{span}(v)$ line.

For $a \in \mathbb{R}^2$, its coset

$[a] = a + \text{span}(v)$

is the "line through a parallel to H".

(they partition the plane into parallel lines)