Lecture 8 Abstract Nonsense (cont.)

$\pi \circ *$

" $*'' \circ \pi \times \pi$

Recall $G = D_{2n}$ Let the partition defined by $\sim$ be

$$I = \{\underbrace{\{1, r, r^2, \dots, r^{n-1}\}}_{= A}, \underbrace{\{s, rs, \dots, r^{n-1}s\}}_{= B}\}$$

$I = \{A, B\} \subseteq 2^G$ Then we have a group morphism

$$G \xrightarrow{\chi} \mathbb{Z}/2\mathbb{Z}$$

$G/\sim = I$

$A \mapsto \bar{0}$ $\quad A = \chi^{-1}(\bar{0})$

$B \mapsto \bar{1}$ $\quad B = \chi^{-1}(\bar{1})$

$$\begin{tikzcd} G \times G \arrow[r, "*"] \arrow[d, "\pi \times \pi"'] & G \arrow[d, "\pi"] \\ I \times I \arrow[r] & I \end{tikzcd}$$

In particular, $\Rightarrow$ implies that "$*$" exists

We have checked before that

if

$y \in$ \ $x \in$	A	B
A	$xy \in A$	$xy \in B$
B	$xy \in B$	$xy \in A$

$$I \times I = \{(A, A), (A, B), (B, A), (B, B)\}$$

$$\text{"}*\text{"} \downarrow \qquad (A,A) \mapsto A,\ (A,B) \mapsto B,\ (B,A) \mapsto B,\ (B,B) \mapsto A$$

well defined $\quad I$

The formation of I is completely analogous to the formation of $\mathbb{Z}/n\mathbb{Z}$

A general procedure of putting a partition on G

$(G, *) =$ a group $\quad H \leq G$ is a subgroup

Define a binary relation $\sim$ on G by

$$x \sim y \Leftrightarrow \exists h \in H, \text{ s.t. } hx = y$$

Check that this is an equivalence

(a) $x \sim x$ (true b/c $1 \in H$ $1 \cdot x = x$)

(b) $x \sim y \Leftrightarrow y \sim x$ ($hx = y \Leftrightarrow x = h^{-1} y$)

(c) $x \sim y$ $y \sim z \Rightarrow x \sim z$ ($hx = y$, $h' y = z \Rightarrow h' h x = z$)

($\equiv \bmod n$) as an equivalence relation is precisely given by the subgroup $n\mathbb{Z} \leq \mathbb{Z}$

$y - x = kn$ for some $k \in \mathbb{Z}$ is precisely saying that for some $h \in n\mathbb{Z}$ $h + x = y$

$\uparrow$

$+$ is the group law of $\mathbb{Z}$

Similarly the partition $\left\{ \begin{array}{l} A = \{1, r, \dots, r^{n-1}\} \\ B = \{s, rs, \dots, r^{n-1}s\} \end{array} \right\}$ of D_{2n}

is given by the subgroup $H = \{1, r, \dots, r^{n-1}\}$ of D_{2n}

The set of elements in the partition defined by a subgroup $H \subseteq G$ is commonly denoted by G/H

($\mathbb{Z}/n\mathbb{Z}$ is really a special case)

Rmk: It is not true for any subgroup $H \subset G$, "$*$" can be defined for G/H

Fermat's Little Theorem

p = prime number $a \in \mathbb{Z}$ $a^p = a \mod p$

E.g. $p=3$ $a=2$ $2^3 \equiv 2 \mod 3$

$p=5$ $a=2$ $2^5 = 32 \equiv 2 \mod 5$

Introduce the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ ← cross

Exercise: The binary operation is indeed defined for $\mathbb{Z}/n\mathbb{Z}$

$(a, b) \mapsto ab$

$$\begin{tikzcd} \mathbb{Z} \times \mathbb{Z} \arrow[r, "\times"] \arrow[d] & \mathbb{Z} \arrow[d] \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \arrow[r, "``\times\text{''}"] & \mathbb{Z}/n\mathbb{Z} \end{tikzcd}$$

For $\mathbb{Z}/n\mathbb{Z}$, write $\times$ for "$\times$"

$\times$ defines a binary operation on $\mathbb{Z}/n\mathbb{Z}$ but it is not a group operation. b/c not all elements have an inverse!

Suppose $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ has an (multiplicative) inverse, then $\exists\, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\bar{a} \times \bar{b} = \bar{1}$

In other words, if $a \in \mathbb{Z}$ is s.t. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse, then $\exists\, b \in \mathbb{Z}$ s.t. $ab = 1 + nk$ for some $k \in \mathbb{Z}$

$\Uparrow$ if this condition holds, then $d = \gcd(a, n) = 1$

$d \mid a$ $d \mid n$ $\Rightarrow d \mid ba - kn = 1 \Rightarrow d \mid 1 \Rightarrow d = 1$

The converse is also true!

<u>Thm</u> Given $x, y \in \mathbb{N}$ $d \overset{\text{def}}{=} \gcd(x, y)$. Then $\exists\, \lambda, \mu$ in $\mathbb{Z}$ s.t. $\lambda x + \mu y = d$

$x = 20 \quad y = 6 \quad d = 2 \qquad x - 3y = 2$

$x = 5 \quad y = 7 \quad d = 1 \qquad 3y - 4x = 1$

$x = 30 \quad y = 18 \quad d = 6 \qquad 2x - 3y = 6 \quad 2y - x = 36 - 30 = 6$

$x = y + 12$

$y = 12 + 6 \qquad 6 = y - 12 = y - (x - y) = 2y - x)$

Pf Define $S = \{ n \in \mathbb{Z}_{>0} \mid n = \lambda x + \mu y$ for some $\lambda, \mu \in \mathbb{Z} \}$

Then $S \neq \emptyset$. so by well-ordering principle we have S_{min}

s.t. $\exists d \mid S_{min}$

It suffices to show $S_{min} \mid d$ i.e., $S_{min} \mid x$ and $S_{min} \mid y$

By division w/ remainder, $\exists q$ and r s.t.

$x = q \cdot S_{min} + r \qquad 0 \leq r < S_{min}$

If $r \neq 0$, then $r \in S$, which contradicts the minimality of $S_{min} \Rightarrow r = 0$, i.e., $S_{min} \mid x$

Similarly $S_{min} \mid y$ $\square$

Now define $(\mathbb{Z}/n\mathbb{Z})^{\times} \subseteq \mathbb{Z} \times n\mathbb{Z}$ to be the subset of elements w/ a multiplicative inverse

$a \in \mathbb{Z}, \quad \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times} \Leftrightarrow \gcd(a, n) = 1$

Exercise: This implies that $(\mathbb{Z}/p\mathbb{Z})^{\times} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$|(\mathbb{Z}/p\mathbb{Z})^{\times}| = p - 1$

(# elements)

$(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a group under multiplication (Exercise)

Lemma If H is a subgroup of a finite group G, then $|H| \mid |G|$

In particular, $g \in G$, then $|g| \mid |G|$

Lemma $\Rightarrow$ Fermat little theorem

Take $a \in \mathbb{Z}$ $p \nmid a$. Consider $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^{\times}$

Lemma $\Rightarrow$ $|\bar{a}| \mid |(\mathbb{Z}/p\mathbb{Z})^{\times}| \Rightarrow |\bar{a}| \mid p-1$

$\Rightarrow a^{p-1} \equiv 1 \mod p$, i.e., $a^p \equiv a \mod p$

Lemma is actually called Lagrange theorem left to HW