6/2/23 L12

Recall: Definition: A group G is a set with operation $*: G \times G \longrightarrow G$

(G1) $xy \in G \; \forall x y \in G$

(G2) $x(yz) = (xy)z \; \forall x, y, z \in G$

(G3) $\exists e \in G$ s.t. $ex = xe = x \; \forall x \in G$ ($e = 1$ if $* = \times$, $e = 0$ if $* = +$)

(G4) $\forall x \in G \; \exists x^{-1}$ s.t.

<u>Quiz:</u> 1. $\mathbb{Z}$ under $+$ ✓

2. $\mathbb{Z}$ under $\times$ ✗

3. $2\mathbb{Z}$ under $+$ ✓

4. $\mathbb{R}_{>0}$

5. $\{1\}$ under $\times$ ✓

6. $\emptyset$ ✗ ($e \notin \emptyset$)

7. $\{0\}$ under $+$ ✓ $(7) \cong (5) \cong \{e\}$

8. $\{1, -1\}$ under $\times$ ✓ ($e = 1$)

9. $\{\underset{\overset{\shortparallel}{e}}{1}, 3\}$ multiplicity mod 8 ✓ $(3 \cdot 3 = 1 = e,\ 3^{-1} = 3)$

note: $(8) \cong (9)$

note: If $|H| = |G| = p$ prime then $H \cong G$.

why $(8) \cong (9)$?
$$\begin{array}{c|cc} \times & 1 & 3 \\ \hline 1 & 1 & 3 \\ 3 & 3 & 1 \end{array} \longleftrightarrow \begin{array}{c|cc} \times & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}$$
so $(8) \cong (9)$

10 $\{1, (123), (132)\}$ under $\circ$ ✓ $\big((132) = (123)^2,\ (123)^3 = 1,\ (123)^{-1} = (132),$
$(132)^{-1} = (123)\big)$

<u>Definition 5.14:</u> The <u>order</u> of is $|G| = \#$ elements in G. G is (in)finite if $|G|$ is (in)finite.

<u>Definition 5.15:</u> The <u>direct product</u> (or cartesian product) of groups G and H is

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}$$

with operation: $(g_1 \cdot h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$ for all $g_1, g_2 \in G$, $h_1, h_2 \in H$

Lemma 5.16 (Cancellation): Let $x, y, y' \in G$. If $xy = xy'$ (or $yx = y'x$) then $y = y'$.

Proof: $xy = xy' \Rightarrow x^{-1}(xy) = x^{-1}(xy')$

$$(xx^{-1})y = (x^{-1}x)y'$$

$$ey = ey'$$

$$y = y'$$

Corollary 5.17 (Latin Square Property): In the Cayley Table of G each element appears exactly once in each row/column

$$\begin{array}{c|ccccc}
 & \cdots & b & \cdots & c & \cdots \\ \hline
\vdots & & \vdots & & \vdots & \\
a & \cdots & ab & \cdots & ac & \cdots \\
\vdots & & & & &
\end{array}$$

Proof: $ab = ac \Rightarrow b = c$

Example 5.18 (solving equations): Let $a, b \in G$. Find $x \in G$ s.t. $ax = b$.

$$ax = b \qquad \Leftrightarrow x = a^{-1}b$$

$$\Updownarrow$$

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

$$(a^{-1}a)x = x \quad \text{by } (G2)$$

$$ex = x \quad \text{by } (G4)$$

$$x = x \quad \text{by } (G3)$$

Definition 5.19: Let $x \in G$. Set $x^0 = e$ and for $n > 0$ define $x^n = \underbrace{x\,x \cdots x}_{n}$ and $x^{-n} = \underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n}$

Exercise: check $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ $\forall m, n \in \mathbb{Z}$

Note: If $(xy)^n \neq x^n y^n$ in general

$$\overset{\shortparallel}{xy\,xy \cdots xy} \qquad \overset{\shortparallel}{xx \cdots xyy \cdots y}$$

however, if $xy = yx$ then $(xy)^n = x^n y^n$

Note: If operations is "+", then n'th power is $nx = x + x + x + \cdots + x$.

Lemma 5.21: $(x_1 x_2 \cdots x_k)^{-1} = x_k^{-1} x_{k-1}^{-1} \cdots x_2^{-1} x_1^{-1}$ $(x_i \in G)$

Proof: Indeed, $(x_1 x_2 \cdots x_{k-1} x_k)(x_k^{-1} x_{k-1}^{-1} \cdots x_2^{-1} x_1^{-1}) = 1$

$$\| $$

$$x_1 \cdots x_{k-1} \underbrace{x_k x_k^{-1}}_{= 1} x_{k-1} \cdots$$