FRI, SEPT 19, 2014

More on quotients.

We'll prove

Thm If $H \subset G$ is normal, then

$$G/H \times G/H \to G/H$$

$$(Hg_1, Hg_2) \mapsto Hg_1g_2$$

is well-defined, and defines a group structure on G/H.

gHg^{-1}
$\shortparallel$
$\{ghg^{-1} \mid h \in H\}$
$\shortparallel$ normal
H

Ex Let $H = n\mathbb{Z}$

$= \{\text{multiples of } n\}$

$= \{\dots, -2n, -n, 0, n, \dots\}$

Then $Ha = \{a' \in \mathbb{Z} \text{ s.t. } a' = kn + a \text{ for some } k \in \mathbb{Z}\}$

$= \mathcal{O}_a$.

Ex: $H3 = \{\dots 3-2n, 3-n, 3, 3+n, 3+2n, \dots\}$.

Prop'n $\exists$ bijection

$$\mathbb{Z}/n\mathbb{Z} \to \{0, 1, \cdots, n-1\}$$

$\forall\ n \geq 1$.

Pf Given $\mathcal{O}_a \in \mathbb{Z}/n\mathbb{Z}$, let r_a be unique # s.t.

$$a = kn + r_a.$$

$k \in \mathbb{Z}$,
$r_a \in 0, 1, \cdots, n-1$.

i.e., the remainder of $a \div k$. (From elementary school.)

So let the bijection be

$$\mathbb{Z}/n\mathbb{Z} \to \{0, 1, \cdots, n-1\}$$
$$\mathcal{O}_a \longmapsto r_a \quad .$$

· Well-defined?

If $\mathcal{O}_a = \mathcal{O}_{a'}$,

$a' = a + k'n$ (by defn of orbit)

so

$a' = k'n + kn + r_a$.

$= (k'+k)n + r_a$

$\Rightarrow r_{a'} = r_a$. So well-defined!

the unique number in $\{0, 1, \cdots, n-1\}$ such that $a' = Kn + r_{a'}$.

· injection? Given $\mathcal{O}_a, \mathcal{O}_b$,

$r_a = r_b$

$\Rightarrow$ $a = kn + r_a$
$b = ln + r_b$
$= ln + r_a$

$\Rightarrow a - b = (k - l)n$

$\Rightarrow a \in \mathcal{O}_b$

$\Rightarrow \mathcal{O}_a = \mathcal{O}_b$.

· surjection? Yes.

$\mathcal{O}_0 \mapsto 0$

$\mathcal{O}_1 \mapsto 1$

$\mathcal{O}_2 \mapsto 2$

$\vdots$

$\mathcal{O}_{n-1} \mapsto n-1$

By the theorem, this means

$$\mathbb{Z}/n\mathbb{Z}$$

is a group of order

$$n = |\{0, 1, \dots, n-1\}|$$

What's the group structure?

$$\begin{tikzcd}
\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[ddd, bend right, "\text{bijection}"'] & \mathbb{Z}/n\mathbb{Z} \\
(\theta_a, \theta_b) \arrow[r, mapsto] \arrow[d, mapsto] & \theta_{a+b} \arrow[d, mapsto] \\
(r_a, r_b) \arrow[r, mapsto] & r_{a+b} \\
\{0, \dots, n-1\} \times \{0, \dots, n-1\} \arrow[r] & \{0, \dots, n-1\}
\end{tikzcd}$$

ie, the group structure is:

Add numbers, then find the remainder when dividing by n.

Defn Let $a, b \in \mathbb{Z}$.

We write

$$a \equiv b \pmod{n}$$

or

$$a = b \pmod{n}$$

if

$$a - b = kn \text{ for some } k \in \mathbb{Z}.$$

equivalently, $a \equiv b \pmod{n}$

$$\Updownarrow$$

$\theta_a = \theta_b$.

When we write

$$a \pmod{n}$$

we mean the equivalence class

$$\mathcal{O}_a = Ha \in G/H.$$

<u>Rmk</u> You might find it annoying to keep track of giant equivalence classes $\mathcal{O}_a, \mathcal{O}_b$, etc, in your head all the time. So instead, it may help to think of $\mathcal{O}_a$ simply as a <u>number</u>, namely, the remainder r you get when dividing a by n:

$$a = kn + r.$$

This is justified by the bijection

$$\mathbb{Z}/n\mathbb{Z} \cong \{0, \dots, n-1\}.$$

So when you see "$a \pmod{n}$," you can just think of the number r. Likewise, the group operation is just "clock arithmetic":

$$(a,b) \longmapsto a+b \pmod{n}.$$

which you can think of as the remainder in $(a+b) \div n$.

Pf of theorem.

To show the operation is well-defined, need to show:

$$\text{If} \quad Hg_1 = Hg_1'$$

$$\text{and} \quad Hg_2 = Hg_2'$$

for some $g_1, g_1', g_2, g_2' \in G$,

then

$$Hg_1g_2 = Hg_1'g_2'.$$

Well,

$$Hg_1'g_2' = \{ h g_1' g_2' \mid h \in H \}.$$

That $Hg_1 = Hg_1' \Rightarrow O_{g_1} = O_{g_1'}$

$\Rightarrow g_1, g_1'$ are in same orbit

$\Rightarrow g_1' = h_1 g_1$, for some $h_1 \in H$

Likewise, $Hg_2 = Hg_2' \Rightarrow g_2' = h_2 g_2$ for some $h_2 \in H$.

So

$$Hg_1'g_2' = \{ h \cdot h_1 g_1 \cdot h_2 g_2 \mid h \in H \}$$

key step! Very clever trick. Insert 1_G in convenient way.

$$= \{ h \cdot \underbrace{h_1 g_1 \cdot h_2 \boxed{g_1^{-1}}}\, g_1 g_2 \mid h \in H \}$$

since H is normal, $g_1 h_2 g_1^{-1} \in H$. Call it h_3.

$$= \{ h \cdot h_1 h_3 \, g_1 g_2 \mid h \in H \}$$

$$\subset Hg_1g_2.$$

Since $H_{g_1 g_2}$, $H_{g_1' g_2'}$

are orbits/equivalence classes,

$$H_{g_1 g_2} \supset H_{g_1' g_2'}$$

$\Rightarrow$

$$H_{g_1 g_2} = H_{g_1' g_2'},$$

Done w/ "well-defined."

Why is it a group?

$$
\begin{aligned}
(H_{g_1} \cdot H_{g_2}) \cdot H_{g_3} &= H_{g_1 g_2} \cdot H_{g_3} \\
&= H_{(g_1 g_2) g_3} \\
&= H_{g_1 (g_2 g_3)} \\
&= H_{g_1} H_{g_2 g_3} \\
&= H_{g_1} \cdot (H_{g_2} H_{g_3}) \Rightarrow \text{associative.}
\end{aligned}
$$

$$H_{1_G} \cdot H_g = H_g = H_g \cdot H_{1_G} \quad \Rightarrow \text{identity.}$$

$$
\begin{aligned}
H_g \cdot H_{g^{-1}} &= H_{gg^{-1}} = H_{1_G} \\
&= H_{g^{-1} g} \quad \Rightarrow \text{inverses.} \\
&= H_{g^{-1}} H_g
\end{aligned}
$$

//