

Recall: $G \supseteq H$ subgp, H is normal if
 $\forall g \in G \text{ and } h \in H \quad ghg^{-1} \in H.$

Equivalently, $gHg^{-1} \subseteq H$.

Claim: H normal $\Leftrightarrow gHg^{-1} = H \quad \forall g \in G.$

Pf: H normal, $gHg^{-1} \subseteq H$

Also $g^{-1}Hg \subseteq H \Rightarrow H \subseteq gHg^{-1}$

$\Rightarrow gHg^{-1} = H \quad \forall g \in G.$

Other direction: If $gHg^{-1} = H \quad \forall g \in G,$

then $gHg^{-1} \subseteq H \quad \forall g \in G \Rightarrow H$ is normal.

Propⁿ $H \leq G$ is a subgp. TFAE:

- 1) H is normal
- 2) $\forall g \in G, \underline{gH} = \underline{Hg}$
- 3) Every left coset of H is a right coset of H .

Pf: (1) $\Leftrightarrow$ (2):

H normal $\Leftrightarrow gHg^{-1} = H \quad \forall g \in G$

$\Leftrightarrow \underline{gH} = \underline{Hg} \quad \forall g \in G.$

(2) $\Rightarrow$ (3): $gH = Hg$ implies every left coset of H is a

(2) $\Rightarrow$ (3) : $gH = Hg$ implies every left coset of H is a right coset

(3) $\Rightarrow$ (2) Suppose every left coset ^{of H} is a right coset of H .

I.e., $\forall g \in G \exists g' \in G$ so that $gH = Hg'$.

Have $g \cdot 1 = hg'$ for some $h \in H$.

$$\begin{aligned} gH &= Hg' = Hhg' \\ &= Hg. \end{aligned} \quad \begin{array}{l} \text{(since } H = Hh \\ \text{b/c } H \text{ is a subgroup)} \end{array}$$

$\square$

Propⁿ a) H a subgp of a gp G , $g \in G$. Then gHg^{-1} is a subgp of G .

b) If G has a unique subgp of order r , and $H \leq G$ is that subgp, then H is normal.

Pf: a) $\phi_g : G \rightarrow G$ defined by $\phi_g(x) = gxg^{-1}$ is a gp homom.

Therefore $\phi_g(H) \leq G$ is a subgp.

$$\text{But } \phi_g(H) = gHg^{-1}.$$

b) $\forall g \in G$, gHg^{-1} is a subgp of order r .

$\Rightarrow gHg^{-1} = H$ because we've assumed there's a unique subgp of order r .

$\Rightarrow H$ is normal. $\square$

$\Rightarrow H$ is normal. $\square$

Modular Arithmetic

Fix $n \neq 0$ an integer.

Say a is congruent to b modulo n if $b-a \in n\mathbb{Z}$.

One writes $a \equiv b \pmod{n}$ or $a \equiv b \pmod{n}$.

We've checked before that this is an equivalence relⁿ.

(Associated to cosets of $n\mathbb{Z} \subseteq (\mathbb{Z}, +)$).

One denotes $\mathbb{Z}/n\mathbb{Z}$ as the set of equivalence classes.

The elements of $\mathbb{Z}/n\mathbb{Z}$ are

$$0+n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}$$

$$\Rightarrow |\mathbb{Z}/n\mathbb{Z}| = |n|$$

Ex $5 \equiv 17 \pmod{6}$, $-4 \equiv 17 \pmod{7}$
 $\pmod{3}$
 $\pmod{21}$

Thm If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$

then $a+b \equiv a'+b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

In other words, addition and multiplication define L.O.C. on

In other words, addition and multiplication define L.O.C. on $\mathbb{Z}/n\mathbb{Z}$.

Pf $a \equiv a' \pmod{n} \Rightarrow a' = a + rn$ for some int. r
 $b \equiv b' \pmod{n} \Rightarrow b' = b + sn$ for some int. s .
 $\Rightarrow a' + b' = a + b + (r+s)n \Rightarrow a' + b' \equiv a + b \pmod{n}$.
 $a'b' = (a + rn)(b + sn)$
 $= ab + (br + sa + rsn)n$
 $\Rightarrow a'b' \equiv ab \pmod{n}$. $\square$

Ex What's the remainder when 8^{10} is divided by 10?

$$8 \equiv -2 \pmod{10}$$

$$8^{10} \equiv (-2)^{10} \pmod{10}$$

$$\equiv 1024 \pmod{10}$$

$$\equiv 4 \pmod{10}$$

The remainder is 4.

Cor $\mathbb{Z}/n\mathbb{Z}$ is a set w/ 2 laws of composition, $+$ and $\times$.

Claim: $\mathbb{Z}/n\mathbb{Z}$ with addition is a cyclic gp of order n .

Df: The identity of $\mathbb{Z}/n\mathbb{Z}$ is 0 .

I.e. $0 + l \equiv l \equiv l + 0 \pmod{n} \quad \forall l \in \mathbb{Z}$.

Inverses: $l + (-l) \equiv 0 \equiv (-l) + l \pmod{n} \quad \forall l \in \mathbb{Z}$

$\Rightarrow l + n\mathbb{Z}$ has inverse $-l + n\mathbb{Z}$.

Assoc: $l_1 + (l_2 + l_3) \equiv l_1 + l_2 + l_3 \equiv (l_1 + l_2) + l_3 \pmod{n}$

$\forall l_1, l_2, l_3 \in \mathbb{Z}$.

Cyclic because every equiv class is a power of $1 + n\mathbb{Z}$.

I.e., the equiv classes are

$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \underbrace{1+1}_{1+1+1} + n\mathbb{Z} = 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}.$

$\Rightarrow$ cyclic of order n .

Note: $\mathbb{Z}/n\mathbb{Z}$ with L.O.C. as $\times$ (multiplication) is
not a sp.

Define: $(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ x \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \exists y \in \mathbb{Z}/n\mathbb{Z} \text{ with } xy \equiv 1 \pmod{n} \right\}.$

Propn: $(\mathbb{Z}/n\mathbb{Z})^\times$ is a sp.

Df: Know: multiplication on $\mathbb{Z}/n\mathbb{Z}$ defines an assoc. L.O.C.
... 0 ... 1 ... $1 + n\mathbb{Z}$

1.1: Know: multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined on units with identity $1+n\mathbb{Z}$.

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the subset of invertible elts $\xrightarrow{\text{HW question}}$ is a gp. ~~is~~

Ex $(\mathbb{Z}/10\mathbb{Z})^\times = \{1+10\mathbb{Z}, 3+10\mathbb{Z}, 7+10\mathbb{Z}, 9+10\mathbb{Z}\}$
has size 4 ~~(1), (3), (7), (9)~~

Propⁿ $r+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \gcd(r, n) = 1.$

Pf: Suppose $r+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that $\exists$ int. s with
 $rs \equiv 1 \pmod{n}.$

$$\implies rs - 1 = ln \implies rs - ln = 1 \implies \gcd(r, n) = 1.$$

Conversely, suppose $\gcd(r, n) = 1.$

Then $\exists$ s, l integers so that $rs - ln = 1.$

$$\implies rs = 1 + ln \implies rs \equiv 1 \pmod{n}. \quad \square$$

Defⁿ Suppose $n \geq 1$ is an integer. The number of elements
of $\{1, 2, 3, \dots, n\}$ that are relatively prime to n
is denoted $\phi(n)$, called Euler's ϕ -fcn

We just proved: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n).$

Cor: Suppose $\gcd(r, n) = 1.$ Then $r^{\phi(n)} \equiv 1 \pmod{n}.$

Cor: Suppose $\gcd(r, n) = 1$. Then $r^{\phi(n)} \equiv 1 \pmod{n}$.

Pf: $r \in (\mathbb{Z}/n\mathbb{Z})^\times$. Let l denote the order of r as an elt of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $r^l \equiv 1 \pmod{n}$.

$\Rightarrow l = |\langle r \rangle|$, size of cyclic gp gen'd by r .
 $= \{1, r, r^2, \dots, r^{l-1}\}$.

Lagrange's Thm: l divides $\phi(n)$
 $|\langle r \rangle| \quad |(\mathbb{Z}/n\mathbb{Z})^\times|$.

$$r^l \equiv 1 \pmod{n} \Rightarrow r^{\phi(n)} \equiv 1 \pmod{n}.$$

(raise both sides to $\frac{\phi(n)}{l}$ 'th power)

□

Ex $\phi(10) = 4$

$$\Rightarrow 7^4 \equiv 1 \pmod{10}$$

$$(1723)^4 \equiv 1 \pmod{10}.$$

Cor: If p is prime, $\phi(p) = p-1$.

Therefore, if $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.