Problems from Chap 9 not due until next week!

Previously in Math 103a

If $p_1, p_2, \ldots p_m$ are distinct primes, then

$$U(p_1 p_2 \cdots p_m) \approx U(p_1) \oplus U(p_2) \oplus \cdots \oplus U(p_m)$$
$$\approx \mathbb{Z}_{p_1-1} \oplus \mathbb{Z}_{p_2-1} \oplus \cdots \oplus \mathbb{Z}_{p_m-1}$$

Q: Is there are general formula for $U(n)$?

Need $U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$ p odd prime

Also have $U(2^n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$

Ex: How many elts of order 3 are in $\mathrm{Aut}\,\mathbb{Z}_{99}$?

Ans Know $\mathrm{Aut}\,\mathbb{Z}_{99} \approx U(99) = U(3^2 \times 11)$

By above & previous Thm ($U(st) \approx U(s) \oplus U(t)$ if $\gcd(s,t) = 1$)

we know $U(3^2 \times 11) \approx U(3^2) \oplus U(11)$

$$\approx \mathbb{Z}_{3^2-3} \oplus \mathbb{Z}_{10}$$

$\therefore \mathrm{Aut}\,\mathbb{Z}_{99} \approx U(99) \approx \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$

If $(a,b) \in \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$, then $|(a,b)| = \mathrm{lcm}(|a|, |b|)$

$|(a,b)| = 3 \iff |a| = 3, |b| = 1$. There are $\varphi(3) = 2$ elts of order 3 in $\mathbb{Z}_6$.

$\therefore$ 2 elts of order 3 in $\mathrm{Aut}\,\mathbb{Z}_{99}$.

Notation: For $k \mid n$, write

$$U_k(n) = \{x \in U(n) : x \bmod k = 1\}.$$

Ex 1 $U(105) = U(7 \cdot 15) \approx U(7) \oplus U(15)$

$$U_{15}(105) \xrightarrow{\text{iso}} U(7) \oplus \{1\} \approx U(7)$$

by $x \longmapsto (x \bmod 7, x \bmod 15)$

$U_{15}(105)$ $\quad$ $= 1$ by definition

Ex 2. $U(120) \approx U(8) \oplus U(3) \oplus U(5)$

$\therefore U_5(120) \approx U(8) \oplus U(3)$.

Note: $U(105) \longrightarrow U(7)$ given by $x \longmapsto x \bmod 7$ preserves operations but is not an isom Homomorphism. It will be important soon!

Chap 9 Normal subgroups and factor groups.
Very important now!

Def A subgroup $H \subset G$ is **normal** if

$$gH = Hg \quad \forall\, g \in G.$$

Ex 1. If G is abelian, all subgroups are normal.

Ex 2. $A_n \subset S_n$ is normal.

Reason: Take any $\sigma \in S_n$ odd order

Then $S_n = \sigma A_n \cup A_n$ & $S_n = A_n \cup A_n \sigma$ (check it!)

$\therefore \sigma A_n = A_n \sigma$

Similarly, can check that any subgroup $H \subset G$ of index 2 is normal.

(Recall that index $(H) = |G|/|H|$).

Thm $H \subset G$ normal $\Longleftarrow$ $xHx^{-1} \subseteq H$ $\forall x \in G$

Convenient criterion

Ex 3: The subgroup $\left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \neq 0,\ a \in \mathbb{R} \right\} = H$

is not a normal subgroup of

$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \neq 0,\ b \in \mathbb{R} \right\} = G$

Check: Take $x = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then

$$x \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} x^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a & ba^{-1} \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -ba + ba^{-1} \\ 0 & a^{-1} \end{pmatrix}$$

not in H unless $a = a^{-1}$.

Ex 4. $G = S_3$, $H = \langle (1,2) \rangle$. Then H is not normal

Check: $x = (2,3)$ $\quad x^{-1} = (2,3)$

$$(2,3)(1,2)(2,3) = (3,1) \notin \langle (1,2) \rangle = \{(1), (1,2)\}.$$

If take $H' = \langle (1,2,3) \rangle$, then H' is normal in S_3, since $H' = A_3$.

Why normal groups are so important:

Thm: G group, $H \subset G$ normal subgroup, then

$G/H = \{ aH : a \in G \}$ is a group

with operation $(aH)(bH) = (ab)H$. (*)

Note: If H not normal, this operation does not define a group

---

Pf of Thm Check mult'n is well defined i.e. if $aH = a'H$ & $bH = b'H$, does $(ab)H = (a'b')H$? Otherwise (*) makes no sense.

Check: $a(bH) = a(b'H) = a(Hb') = (aH)b' = (a'H)b'$

(= : assumption; = : normality; = : assumption)

$= (Ha')b' = (a'b')H$ ✓

(= : normality; = : normality.)

In G/H H = identity

Inverse: $(aH)^{-1} = a^{-1}H$

Associativity is "inherited" from G

Def G/H is called the factor group of G by H. Say "mod out by H"

This is an important technique!

Ex 1: Find $\mathbb{Z}/3\mathbb{Z}$, $3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$

Cosets: $0+3\mathbb{Z} = 3\mathbb{Z}$

$1+3\mathbb{Z} = \{1, \pm 4, \pm 7, \dots\}$

$2+3\mathbb{Z} = \{1, \pm 5, \pm 8, \dots\}$

$3+3\mathbb{Z} = 3\mathbb{Z}$

$3\mathbb{Z}$ is normal, since $\mathbb{Z}$ is abelian

$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\} \approx \mathbb{Z}_3$

$(2+3\mathbb{Z}) + (1+3\mathbb{Z}) = 3+3\mathbb{Z} = 3\mathbb{Z}$

In general $(a+3\mathbb{Z}) + (b+3\mathbb{Z})$

$= (a+b) \bmod 3 + 3\mathbb{Z}$,

This works for any n: $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$.

Ex 2. $G = \mathbb{Z}_{20}$, $H = \langle 4 \rangle$, $G/H = ?$

$G/H = \{H, 1+H, 2+H, 3+H, 4+H\}$

$\approx \mathbb{Z}_5$

Note: $\mathbb{Z}_{20} \approx \mathbb{Z}_4 \oplus \mathbb{Z}_5$, $x \longmapsto (x \bmod 4, x \bmod 5)$

not a coincidence!

mod out by 4

Ex 3. $G = D_4$, $H = \{R_0, R_{180}\} = Z(G)$

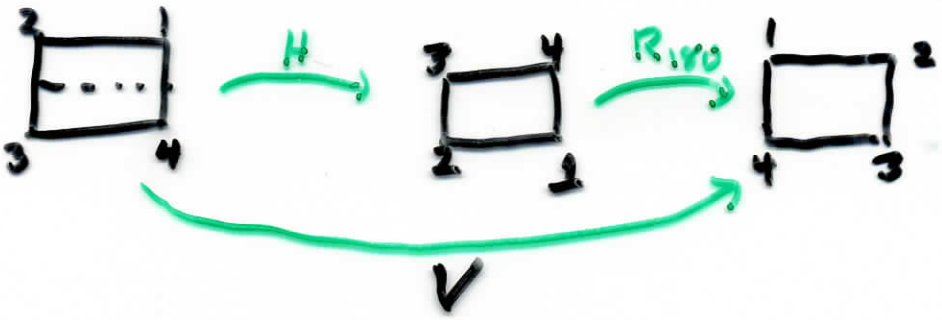
normal

$|D_4/H| = 8/2 = 4$

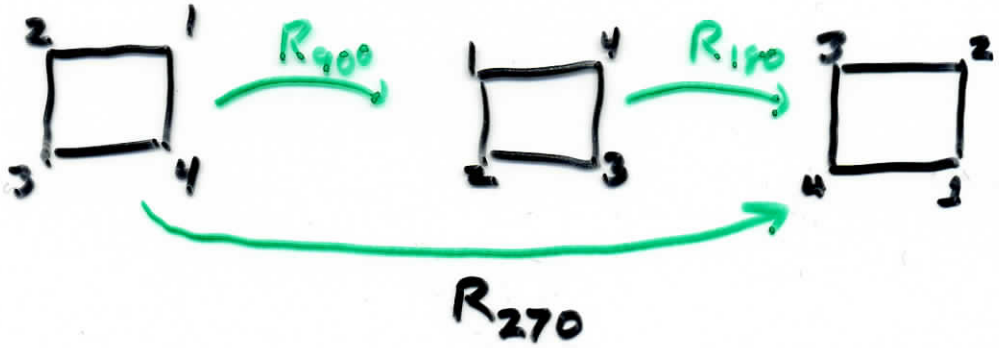
$D_4/H = \{H, R_{90}H, HH, DH\}$

horizontal flip

main diagonal flip.



so $HH = VH$



$\therefore R_{90}H = R_{270}H$

Similarly, $DH = D'H$