EXAMPLE: $S_n \xrightarrow{\text{sign}} \{\pm 1\}$ has $|\mathrm{im}(\text{sign})| = |\{\pm 1\}| = 2$

$p \longmapsto \text{sign}(p)$ and $\ker(\text{sign}) = A_n$ = alternating group $= \{\text{even permutations in } S_n\}$

hence $|A_n| \cdot \underbrace{2}_{[S_n : A_n]} = |S_n|$

so $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$

Note that here there are only two left cosets pA_n, namely A_n and pA_n where p is any odd permutation $(\text{sign}(p) = -1)$.

The index $[G:H]$ behaves well in towers $K < H < G$ of subgroups:

PROPOSITION: If $K < H < G$, then $[G:K] = [G:H] \cdot [H:K]$,
(PROP 2.8.14)
even if one of these numbers is infinite.

follows anyway in finite case by canceling fractions: $\dfrac{|G|}{|K|} = \dfrac{|G|}{|H|} \cdot \dfrac{|H|}{|K|}$

In fact, if G has H-leftcosets $\{g_1H, g_2H, \ldots, g_mH\}$ where $m = [G:H]$
and H has K-leftcosets $\{h_1K, h_2K, \ldots, h_nK\}$ where $n = [H:K]$
then G has K-leftcosets $\{g_ih_jK\}_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$

10/5/2018 >

proof: Assume $g_1 = 1 = h_1$ W.L.O.G. (without loss of generality).

Then $G = H \sqcup g_2H \sqcup \cdots \sqcup g_mH$ ($h \mapsto g_2 h$ bijection)

$$= \begin{pmatrix} K \\ \sqcup h_1K \\ \sqcup h_2K \\ \vdots \\ \sqcup h_nK \end{pmatrix} \sqcup \begin{pmatrix} g_2K \\ \sqcup g_2h_1K \\ \sqcup g_2h_2K \\ \vdots \\ \sqcup g_2h_nK \end{pmatrix} \sqcup \begin{pmatrix} g_3K \\ \sqcup \\ \vdots \end{pmatrix} \sqcup \cdots \sqcup \begin{pmatrix} g_mK \\ \sqcup g_mh_1K \\ \sqcup g_mh_2K \\ \vdots \\ \sqcup g_mh_nK \end{pmatrix} \blacksquare$$

EXAMPLE: A tower that we will come back to later inside S_4:

$$\{1\} < \langle (12)(34) \rangle < \{e, (12)(34), (13)(24), (14)(23)\} < A_4 < S_4$$

$[\langle(12)(34)\rangle : \{1\}] = 2$, $[V_4 : \langle (12)(34)\rangle] = 2$, $[A_4 : V_4] = 3$, $[S_4 : A_4] = 2$

$\{e, (12)(34), (13)(24), (14)(23)\}$ = Klein four V_4 $\left(\cong \left\{\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}\right\} < GL_2(\mathbb{R})\right)$

We could have been working with right cosets $Ha := \{ha : a \in G\}$, which will be different in general

EXAMPLE: $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$H = \langle (12) \rangle < S_3$

$H = eH$, $(13)H$, $(23)H$

$= \{e, (12), (13), (23), (123), (132)\}$

$H = He$, $H(13)$, $H(23)$

PROPOSITION: (PROP 2.8.17, 2.8.18) For any subgroup $H < G$, the sets $gHg^{-1} := \{ghg^{-1} : h \in H\}$ are all subgroups of G, isomorphic to H via the maps

$$H \longrightarrow gHg^{-1}$$
$$h \longmapsto ghg^{-1}$$
$$(\text{with inverse } g^{-1}xg \longleftarrow\!\shortmid\, x)$$

and TFAE for H:

(i) $H \triangleleft G$ "H is a normal subgroup of G"
i.e. $gHg^{-1} \subset H \;\; \forall g \in G$

(ii) $gHg^{-1} = H \;\; \forall g \in G$

(iii) $gH = Hg \;\; \forall g \in G$

(iv) Every left coset aH is also a right coset Hb (and in fact, $aH = Ha = bH = Hb$ in this case).

Proof: (ii) $\Leftrightarrow$ (iii) comes from multiplying on right by g or g^{-1}.

(ii) $\Rightarrow$ (i) is clear, but then (i) $\Rightarrow$ (ii) since $gHg^{-1} \subset H$
$\Rightarrow H \subset g^{-1}Hg$ by $x \mapsto g^{-1}xg$
$\Rightarrow H \subset g^{-1}Hg \subset H$
i.e. $g^{-1}Hg = H$, so $gHg^{-1} = H$.

(iii) $\Rightarrow$ (iv) is clear,
but if every left coset is a right coset, then $gH = Hg'$ forces $g \in gH = Hg'$
$\Rightarrow Hg' = Hg$ i.e. $gH = Hg$ ∎

(61)

§2.9 Modular arithmetic

Q: What time of day will it be 50 hours from now?
What day of week 50 days from now?
Last digit of 7539×10746 ?

+	even	odd
even	?	?
odd	?	?

×	even	odd
even	?	?
odd	?	?

Recall $G = \mathbb{Z}^+$ has all subgroups $H < \mathbb{Z}^+$ of form $H = n\mathbb{Z}$
$= \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$
for some n.

The (left or right) cosets of $H = n\mathbb{Z}$ inside $G = \mathbb{Z}^+$
are of form $a + n\mathbb{Z} := \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\} =: \overline{a}$ need to know the modulus n!
which are equiv. classes for $a \equiv b \bmod n$ if $a-b$ divisible by n, or $a = b + nk$ with $k \in \mathbb{Z}$,
and there are only n of them: $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} =: \mathbb{Z}/n\mathbb{Z}$ integers modulo n

$\overline{0} = n\mathbb{Z}$, $\overline{1} = 1 + n\mathbb{Z}$, $\overline{2} = 2 + n\mathbb{Z}$, $\overline{n-1} = n-1+n\mathbb{Z} = -1 + n\mathbb{Z}$

EXAMPLE: $n=10$

$10\mathbb{Z} = \{\ldots, -20, -10, 0, 10, 20, \ldots\}$

$\overline{3} = 3 + 10\mathbb{Z} = \{\ldots, -17, -7, 3, 13, 23, \ldots\} = \overline{-7} = \overline{823}$

$\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{9}\}$

PROPOSITION: One can add, multiply in $\mathbb{Z}/n\mathbb{Z}$ using any representatives:
(LEMMA 2.9.6)

if $a \equiv a' \bmod n$, $b \equiv b' \bmod n$ then $\overline{a \cdot b} := \overline{a' \cdot b'}$, $\overline{a+b} := \overline{a'+b'}$ make sense because
$a \cdot b \equiv a' \cdot b' \bmod n$
$a + b \equiv a' + b' \bmod n$

proof: If $a = a' + k_1 n$, $b = b' + k_2 n$ then $a+b = a'+b' + \overbrace{(k_1+k_2)}^{\in \mathbb{Z}} n$

$a \cdot b = (a'+k_1 n)(b'+k_2 n) = a'b' + k_1 n b' + k_2 n a' + k_1 k_2 n^2$

$= a'b' + \underbrace{(k_1 b' + k_2 a' + k_1 k_2 n)}_{\in \mathbb{Z}} n$ ∎

10/8/18 >

EXAMPLE: $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
even, odd