HW 3.1.: Consider $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 

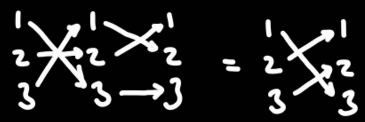
Pick any two transpositions:

$\langle (12) \rangle = \{e, (12)\}$, $\langle (13) \rangle = \{e, (13)\}$, $\langle (12) \rangle \cup \langle (13) \rangle = \{e, (12), (13)\}$

Transpositions: $(i\,j)$ $i, j \in \mathbb{Z}^+$

but $(12)(13) = (132) \notin \langle (12) \rangle \cup \langle (13) \rangle$

All the elements of S_n are called permutations.



(12) (12) $=$ (132)

HW 3.8.: $D_3 \cong S_3$, $frf = r^{-1}$ and $r \neq r^{-1}$, so D_3 not abelian. (if D_3 was abelian then $r^{-1} = frf = ffr = r$, contradiction.)

$|f| = 2$, $|r| = 3$, but now:

$(fr)^2 = frfr = r^{-1}r = e$, so $|fr| = 2 \neq 6 = 2 \cdot 3 = |f| \cdot |r|$.

HW 3.4.: Pick $|G|$. Assume G is commutative, what do we have? Is there any non-commutative group of order strictly less than 6?

Hint: look at the orders of the elements in G.

$|G| = 1 \rightsquigarrow$ trivial group.

$|G| = 2 \rightsquigarrow G = \{1, a\}$, $a^2 = 1$ because if $a^2 = a$ then multiplying by a^{-1} : $a = 1$, contradiction.

So $a^{-1} = a$. Now: $G \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is a group isomorphism.

$1 \longmapsto 0$

$a \longmapsto 1$

$|G| = 3 \rightsquigarrow G = \{1, a, b\}$. Can G be non-commutative? If $ab \neq ba$ then

either $ab = a$, no because then $b = 1$

$ab = 1 \longleftarrow$ is the only option left.

$ba = a$ no because then $b = 1$

$ba = 1 \longleftarrow$ same here.

So G is commutative: $ab = 1 = ba$.

Now: $G \longrightarrow \mathbb{Z}/3\mathbb{Z}$ is a group isomorphism.

$$1 \longmapsto 0$$
$$a \longmapsto 1$$
$$b \longmapsto 2$$

Alternatively:

$1 = a^0$

$a = a^1$

If $a^2 = 1$, we have problems: $H = \langle a \rangle$, by Lagrange's Thm: $\underbrace{|G|}_{3} = [G:H]\underbrace{|H|}_{2}$.

If $a^2 = a$, we have problems.

So $a^2 = b$.

So $G = \langle a \rangle$.

$|G| = 6$, we know that $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, S_3 are candidates.

Note: by the Chinese Remainder Theorem $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

HW 3.2.: Use that $\langle W \rangle = \bigcap\limits_{\substack{W \subseteq H \subseteq G \\ H \text{ subgroup}}} H$.

Is $\{g \in G \mid \exists\, w_1, \dots, w_r \in W$ and $n_1, \dots, n_r \in \mathbb{Z}$ with $g = w_1^{n_1} \cdots w_r^{n_r}\}$ a subgroup of G?

HW 3.4.: $\mathbb{Z}/p\mathbb{Z}$ finite field with p elements.

$GL_n(F)$ is the set of invertible matrices.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & & \vdots \\ a_{n-1\,1} & a_{n-1\,2} & \cdots & a_{n-1\,n} \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

choose any entry in F except all 0: $\overbrace{p \cdot p \cdot \cdots \cdot p}^{n} - 1 = p^n - 1$

choose any entry in F except all multiples of the first column: $p^n - p$

choose any entry in F except a linear combination of the first two columns:
nothing like $a \cdot c_1 + b \cdot c_2$, namely nothing like a pair (a,b) : $p^n - p^2$

$\vdots$

Each $p^n - p^i$ are the options for the column. Then:

$$|GL_n(F)| = \prod_{i=0}^{n-1} (p^n - p^i).$$