9/21/2018
Fr

Recall A subgroup H of a group G is a nonempty subset H of G which is a group under the multiplication of G. So (i) the identity e of G is in H 11.1
(ii) $\forall h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$
(iii) $\forall h \in H$, $h^{-1} \in H$.

Ex $\mathbb{Z} \leq (\mathbb{R}, +, 0)$ is a subgroup.
$\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$ is a group with group operation "times" and $e = 1$. It's not a subgroup of $(\mathbb{R}, +, 0)$.

Proposition 11.1 Let G be a group, $\emptyset \neq H \subseteq G$.
H is a subgroup of $G \iff \forall h_1, h_2 \in H$, $h_1 \cdot h_2^{-1} \in H$.
Proof ($\Rightarrow$) easy (?) exercise
($\Leftarrow$) Since $H \neq \emptyset$, $\exists a \in H$. Then (i) $e = a \cdot a^{-1} \in H$.
Also, $\forall h \in H$, $h^{-1} = e \cdot h^{-1} \in H$
Finally, $\forall h_1, h_2 \in H$, $h_2^{-1} \in H$. So $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$. $\square$

Definition Let H, G be two groups. A homomorphism from H to G is a map $f: H \to G$ so that $f(h_1 \cdot h_2) = f(h_1) \cdot f(h_2)$ for all $h_1, h_2 \in H$.

Ex $\exp: \mathbb{R} \to (0, \infty)$, $x \mapsto e^x$ is a homomorphism from $(\mathbb{R}, +, 0)$ to $((0,\infty), \cdot, 1)$ since
$$e^{x+y} = e^x \cdot e^y \quad \forall x, y \in \mathbb{R}$$

Ex $\det: GL(2, \mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism since
$$\det(A \cdot B) = \det A \cdot \det B \quad \forall A, B \in GL(2, \mathbb{R})$$

Ex $\pi: \mathbb{Z} \to \mathbb{Z}_n$ $\pi(n) = [n]$ is a homomorphism since
$$\pi(n+m) = [n+m] = [n] + [m] \quad \forall n, m \in \mathbb{Z}.$$

<u>Ex</u> Let g be an element of a group G. Define, for $n \in \mathbb{Z}$

$$g^n = \begin{cases} \overbrace{g \cdots g}^{n} & n>0 \\ e & n=0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{|n|} & n<0 \end{cases}$$

<u>Ex</u> $G = \mathbb{R}^\times$, $g=2$, $g^n = 2^n$, $n \in \mathbb{Z}$.

$G = \mathbb{Z}_6$ $g = [2]$ $g^2 = [2]+[2] = [4]$

$g^3 = [2]+[2]+[2] = 0 = g^0$

$g^{-1} = [-2] = [4]$.

So in this case $\{ [2]^n \mid n \in \mathbb{Z} \} = \{ [0], [2], [4] \}$.

<u>NB</u> (note well) For $g \in G$, g^n is defined so that the map $f : \mathbb{Z} \to G$, $f(n) = g^n$ is a homomorphism:

$$f(n+k) = g^{n+k} = g^n \cdot g^k = f(n) \cdot f(k)$$

(This is not entirely obvious. Try to prove this)

<u>Proposition 11.2</u> Let $f : H \to G$ be a homomorphism. Then $f(e_H) = e_G$.

<u>Proof</u> $f(e_H) = f(e_H \cdot e_H) = f(e_H) \cdot f(e_H)$

Now multiply both sides by $(f(e_H))^{-1}$. We get

$$e_G = (f(e_H))^{-1} f(e_H) f(e_H) = f(e_H)$$ $\square$

<u>Proposition 11.3</u> Let $f : H \to G$ be a homomorphism. Then $f(h^{-1}) = (f(h))^{-1}$ for all $h \in H$.

<u>Proof</u> $e_G = f(e_H) = f(h h^{-1}) = f(h) f(h^{-1})$

Multiply both sides by $(f(h))^{-1}$. We get

$$f(h)^{-1} e_G = (f(h))^{-1} f(h) f(h^{-1}). \Rightarrow f(h^{-1}) = f(h^{-1})$$ $\square$

<u>Corollary 11.4</u> Let $f: H \to G$ be a homomorphism. Then the image $f(H) := \{f(h) \mid h \in G\}$ is a subgroup of G

<u>Proof</u> It is enough to show (by Prop 11.1): $\forall\, a, b \in f(H)$, $ab^{-1} \in f(H)$.

$a, b \in f(H) \Rightarrow a = f(h_1),\ b = f(h_2)$ for some $h_1, h_2 \in H$.

$\Rightarrow ab^{-1} = f(h_1) \cdot (f(h_2))^{-1} = f(h_1) f(h_2^{-1})$ by 11.3

$= f(h_1 h_2^{-1}) \in f(H)$ $\square$

<u>"Ex"</u> For any group G and any $g \in G$

$f: \mathbb{Z} \to G$, $f(n) = g^n$ is a homomorphism.

$\Rightarrow$ $f(\mathbb{Z}) = \{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

<u>Notation</u> $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$, the subgroup <u>generated</u> by $g \in G$.

<u>Ex</u> $G = \mathbb{Z}$, $g = 2$. For $n > 0$ $g^n = \overbrace{2 + \cdots + 2}^{n} = 2n$

For $n < 0$, $g^n = \underbrace{(-2) + \cdots (-2)}_{|n|} = (-2)|n| = 2n$

And for $n = 0$, $g^0 = 0$. (<u>not</u> 1!)

$\Rightarrow$ $\langle 2 \rangle = 2\mathbb{Z}$, the even integers

More generally, $\forall k \in \mathbb{Z}$ $\langle k \rangle = k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$

<u>Ex</u> $G = S_3$ $g = (12)$

$g^2 = (12)(12) = e$. $\Rightarrow$ $\langle (12) \rangle = \{e, (12)\}$

$\langle (123) \rangle = \{e, (123), (123)(123) = (132)\}$

<u>Definition</u> A subgroup H of a group G is <u>cyclic</u> if $H = \langle g \rangle$ for some $g \in G$.

<u>Ex</u> $\mathbb{Z}_n$ is cyclic for any n since
$\mathbb{Z}_n = \langle [1] \rangle$.

S_3 is <u>not</u> cyclic:
If σ is a cycle of length 2 then $\langle \sigma \rangle = \{e, \sigma\}$
if σ is a cycle of length 3 then $\langle \sigma \rangle = \{e, \sigma, \sigma^2\}$
and $|S_3| = 6$.

<u>However:</u> One can show: any element of S_3 is a product of powers of (12) and (23).

$(12) = (12)^1 \cdot (23)^0$
$(23) = (12)^0 (23)^1$
$(123) = (12)(23)$
$(132) = (23)(12)$
$(12)(23)(12) = (13)$

S_3 is generated by two elements, (12) & (23)
or $\boxed{S_3 \text{ is generated by the set } \{(12), (23)\}}$

<u>Definition</u> Let G be a group, $U \subseteq G$ a subset. The subgroup $\langle U \rangle$ <u>generated</u> by U is the smallest subgroup containing the set U.

<u>Ex</u> $G = S_4$ $\quad U = \{e\}$, $\quad \langle U \rangle = \{e\}$,
$U = \{(12)\}$, $\quad \langle U \rangle = \{e, (12)\}$
$U = \{(12), (23)\}$ $\quad \langle U \rangle = S_3 \leq S_4$.