HW5 MTH 450/550 Fall 2023

Friday, October 13, 2023 10:23 PM

p.55 #4 $i\mathbb{R} = \{ix : x \in \mathbb{R}\}$

Is $\langle i\mathbb{R}, +\rangle$ a subgroup of $\langle \mathbb{C}, +\rangle$?

Check:

① (closure)
If $t, s \in i\mathbb{R}$, then $\exists\, x_1, x_2 \in \mathbb{R}$ so that $t = ix_1$ and $s = ix_2$.
Then $t+s = ix_1 + ix_2 = i(x_1+x_2)$. Since $x_1 + x_2 \in \mathbb{R}$, we conclude that $t+s \in i\mathbb{R}$, so closure is ok! ✓

② (identity)
$0 \in i\mathbb{R}$ and 0 is the identity of $\langle \mathbb{C}, +\rangle$ ✓

③ (inverses)
For any $t \in i\mathbb{R}$ with $t = ix$, $-t = i(-x) \in i\mathbb{R}$, and
$t + (-t) = 0$ ✓

Thus by Thm 5.14, $\langle i\mathbb{R}, +\rangle$ is a subgroup of $\langle \mathbb{C}, +\rangle$

#5 $\pi\mathbb{Q}$ also a subgroup ~ Same argument as above!

#6 $\{\pi^n : n \in \mathbb{Z}\}$ not a subgroup of $\langle \mathbb{C}, +\rangle$.
For example, 0 is identity of $\langle \mathbb{C}, +\rangle$ but $0 \notin \{\pi^n : n \in \mathbb{Z}\}$
(do you see why?)

#8 Recall $GL(n, \mathbb{R}) = \{n\times n \text{ matrices that are invertible}\}$
Let $X = \{M \in GL(n, \mathbb{R}) : \det(X) = 2\}$
But X is not closed under matrix multiplication, because (for $n=2$, for example)
$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in X$ (since $\det \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = 2 - 0 = 2$)
While
$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$ and $\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}\right) = 4 \neq 2$

#9 Let $X = \left\{\begin{bmatrix} a_1 & & 0 \\ & a_2 & \\ 0 & & \ddots \ a_n \end{bmatrix} : \forall i \in \{1, \dots, n\},\ a_i \neq 0\right\}$

① (closure)
Let $\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}, \begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix} \in X$
Then
$$\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}\begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix} = \begin{bmatrix} a_1b_1 & & & 0 \\ & a_2b_2 & & \\ & & \ddots & \\ 0 & & & a_nb_n \end{bmatrix}$$
and since no a_i or b_i is zero, all $a_ib_i \neq 0$
Thus closed under matrix mult. ✓

② (identity)
$\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in X$ ✓

③ (inverses)
$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{a_1} & & & 0 \\ & \frac{1}{a_2} & & \\ & & \ddots & \\ 0 & & & \frac{1}{a_n} \end{bmatrix} \in X$$ ✓

Thus by Thm 5.14, $\langle X, \cdot\rangle$ is a subgroup of $\langle GL(n, \mathbb{R}), \cdot\rangle$

#11 Let $X = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : \det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = -1\right\}$
Then X not closed under the op since, for example
$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in X$ since $\det\left(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\right) = -1$
and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in X$ since $\det\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = -1$
While
$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ and $\det\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) = 1 \neq -1$
So it fails to be closed under the operation, even when $n=2$

#12 Let $X = \{M \in GL(n, \mathbb{R}) : \det M = 1 \text{ or } \det M = -1\}$

① (closure)
Let $M_1, M_2 \in X$. Then
$$\det(M_1M_2) \underset{\substack{\uparrow \\ \text{linear algebra!}}}{=} \det(M_1)\det(M_2) = \underbrace{(\pm 1)(\pm 1)}_{\substack{\text{this product is} \\ 1 \text{ or } -1 \text{ no matter what!}}}$$
So, closed.

② (identity)
$\det\left(\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}\right) = 1$, so it is in X

③ (inverses)
$M \in X \rightarrow \left.\begin{matrix} \det M = 1 \\ \text{or} \\ \det M = -1 \end{matrix}\right\}$ invertible in either case $\Rightarrow M^{-1}$ exists
Moreover, $\det(M^{-1}) = \frac{1}{\det M}$ and since $\frac{1}{1} = 1$ and $\frac{1}{-1} = -1$,
we see $M^{-1} \in X$.

Thus by Thm 5.14, $\langle X, \circ\rangle$ is a subgroup of $\langle GL(n, \mathbb{R}), \cdot\rangle$

#23 Let $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$M^2 = M \cdot M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

$M^3 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}M = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$

$M^4 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$

$\vdots$

So I claim $\{M^n : n = 1, 2, 3, \dots\} = \left\{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \{1, 2, 3, 4, \dots\}\right\}$

Proof of claim: (induction proof)
Base case $n=1$ is true since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = M^1$
Suppose $\boxed{M^N = \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}} \in \langle M\rangle$. We need to argue that $M^{N+1} = \begin{bmatrix} 1 & N+1 \\ 0 & 1 \end{bmatrix}$

induction hypothesis

But
$M^{N+1} = M^N M = \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & N+1 \\ 0 & 1 \end{bmatrix}$,
Which was what we needed to show, completing the proof. ∎

Also we need to do negative powers.
$M^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ (test and see)
$M^{-2} = M^{-1}M^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$
$M^{-3} = \cdots = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}$
So by induction similar to above, can show
$\{M^{-n} : n = -1, -2, \dots\} = \left\{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n = -1, -2, \dots\right\}$
So $\langle M\rangle = \left\{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z}\right\}$

#24 Let $M = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \longrightarrow M^{-1} = \begin{bmatrix} 1/3 & 0 \\ 0 & 1/2 \end{bmatrix}$

$M^{-2} = \begin{bmatrix} 1/9 & 0 \\ 0 & 1/4 \end{bmatrix}$
$\vdots$

$M^2 = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 3^2 & 0 \\ 0 & 2^2 \end{bmatrix}$
$M^3 = \begin{bmatrix} 3^2 & 0 \\ 0 & 2^2 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 3^3 & 0 \\ 0 & 2^3 \end{bmatrix}$
$\vdots$
Similar to above, can use induction to show
$\langle M\rangle = \left\{\begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix} : n \in \mathbb{Z}\right\}$

#27 $\langle \mathbb{Z}_4, +_{\text{mod } 4}\rangle$

$\langle 3\rangle$
3
$3^2 = 6 \bmod 4 = 2$
$3^3 = 5 \bmod 4 = 1$
$3^4 = 4 \bmod 4 = 0$
$3^5 = 3 \bmod 4 = 3$
$3^6 = 6 \bmod 4 = 2$
So $\langle 3\rangle = \{0, 1, 2, 3\}$

#28 $\langle V, \star\rangle$ given by Table 5.11:

$V = \{e, a, b, c\}$

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\langle c\rangle$
$c^2 = c \star c = e$
$c^3 = e \star c = c$
$\Rightarrow \langle c\rangle = \{e, c\}$

#41 Let $\phi : G \to G'$ be an isomorphism from $\langle G, \star\rangle$ to $\langle G', \tilde{\star}\rangle$
Prove: If $\langle H, \star\rangle$ is a subgroup of $\langle G, \star\rangle$, then $\phi[H] := \{\phi(h) : h \in H\}$ makes $\langle \phi[H], \tilde{\star}\rangle$ a subgroup of $\langle G', \tilde{\star}\rangle$

Proof: Will use Thm 5.14 for this.
① (closed)
Let $a, b \in \phi[H]$. Then $\exists\, x, y \in H$ so that $\phi(x) = a$ and $\phi(y) = b$.
Since $\langle H, \star\rangle$ is a (sub)group, $x \star y \in H$.
Thus we can compute
$$\phi(x \star y) \underset{\substack{\uparrow \\ \text{structure} \\ \text{preserving property} \\ \text{of isomorphism}}}{=} \phi(x)\, \tilde{\star}\, \phi(y) = a\, \tilde{\star}\, b \in \phi[H] \quad (\text{since it is an output of } \phi)$$
Thus $\phi[H]$ is closed under the operation $\tilde{\star}$

② (identity)
Since $\langle H, \star\rangle$ is a group, it has an identity — call it $e \in H$.
By Thm 3.14, $\phi(e) \in \phi[H]$ is the identity in $\phi[H]$.

③ (inverses)
Let $a \in \phi[H]$. There is some $x \in H$ so that $\phi(x) = a$.
Since $x \in H$ and $\langle H, \star\rangle$ is a group, $x^{-1} \in H$.
Claim: $a^{-1} = \phi(x^{-1})$
Proof of claim:
Compute
$$\underset{\substack{\uparrow \\ \text{identity} \\ \text{in } \phi[H] \\ \text{by ②}}}{\phi(e)} = \phi(x \star x^{-1}) \underset{\substack{\uparrow \\ \text{property} \\ \text{of} \\ \text{isomorphism}}}{=} \phi(x)\, \tilde{\star}\, \phi(x^{-1}) = a\, \tilde{\star}\, \phi(x^{-1})$$
Similarly
$\phi(e) = \phi(x^{-1} \star x) = \phi(x^{-1})\, \tilde{\star}\, \phi(x) = \phi(x^{-1})\, \tilde{\star}\, a$
So $a\, \tilde{\star}\, \phi(x^{-1}) = \phi(x^{-1})\, \tilde{\star}\, a = \underset{\substack{\uparrow \\ \text{identity!}}}{\phi(e)}$,
Thus $\phi(x^{-1})$ is the inverse of a. So $\phi[H]$ is closed under inverses. □
Therefore by Thm 5.14, $\langle \phi[H], \tilde{\star}\rangle$ is a subgroup of $\langle G', \tilde{\star}\rangle$, completing the proof. ∎

#43 Prove: If $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are subgroups of an abelian group $\langle G, \star\rangle$, then $\langle \underbrace{\{hk : h \in H, k \in K\}}_{\text{call this set } W}, \star\rangle$ is a subgroup of $\langle G, \star\rangle$.

Proof: ① (closure)
Let $x, y \in W$. Then $\exists\, h_1, h_2 \in H$ and $k_1, k_2 \in K$ so that
$x = h_1k_1$ and $y = h_2k_2$.
Then since $h_1, h_2, k_1, k_2 \in G$ (an abelian group),
$xy = h_1k_1h_2k_2$
$= h_1h_2k_1k_2$
But since $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are groups, $h_1h_2 \in H$, $k_1k_2 \in K$,
Let $h_3 = h_1h_2 \in H$ and $k_3 = k_1k_2 \in K$.
Thus $xy = h_3k_3$, so $xy \in W$

② (identity)
Since $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are subgroups of $\langle G, \star\rangle$,
the identity $e \in G$ is also in H and K.
Thus in W, let $h = k = e$. Thus we get $ee = e \in W$,
so it contains the identity.

③ (inverses)
Let $x \in W$ with $x = hk$.
Then $x^{-1} \underset{\substack{\uparrow \\ \text{a product} \\ \text{in } G}}{=} k^{-1}h^{-1} \underset{\substack{\uparrow \\ G \text{ abelian}}}{=} h^{-1}k^{-1}$ and since $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are groups, $h^{-1} \in H$ and $k^{-1} \in K$.
Thus $x^{-1} \in W$
Therefore by Thm 5.14, $\langle W, \star\rangle$ is a subgroup of $\langle G, \star\rangle$. ∎

#51 Let $\langle G, \star\rangle$ be a group and let $a \in G$ be fixed.
Show $H_a = \{x \in G : xa = ax\}$ makes $\langle H_a, \star\rangle$ a subgroup of $\langle G, \star\rangle$.

Proof: ① (closure)
If $x, y \in H_a$, then we know $\begin{cases} xa = ax & (i) \\ \text{and} \\ ya = ay & (ii) \end{cases}$
Now consider
$$(xy)a \underset{\substack{\uparrow \\ \text{assoc} \\ \text{prop}}}{=} x(ya) \overset{(ii)}{=} x(ay) \underset{\substack{\uparrow \\ \text{assoc}}}{=} (xa)y \overset{(i)}{=} axy$$
Thus $xy \in H_a$.

② (identity)
$ea = a = ae \rightarrow e \in H_a$

③ (inverses)
Let $x \in H_a$. Then $ax = xa$.
Since $x \in G$, x^{-1} also exists.
Is $x^{-1} \in H_a$?
Start with what we know:
$ax = xa$
Mult on left by x^{-1}:
$x^{-1}ax = x^{-1}xa = ea = a$
Mult on right by x^{-1}:
$x^{-1}a\underbrace{xx^{-1}}_{=e} = ax^{-1}$
$x^{-1}ae = ax^{-1}$
$x^{-1}a = ax^{-1}$,
as was to be shown.
Therefore by Thm 5.14, $\langle H_a, \star\rangle$ is a subgroup of $\langle G, \star\rangle$. ∎

#54 Show if $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are subgroups of $\langle G, \star\rangle$, then $\langle H \cap K, \star\rangle$ is a subgroup of $\langle G, \star\rangle$.

Proof: ① (closure)
Let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$.
Since $x, y \in H$ and $\langle H, \star\rangle$ is a group, $xy \in H$.
Similarly, $xy \in K$.
Thus $xy \in H \cap K$, so it is closed!

② (identity)
Since $\langle H, \star\rangle$ and $\langle K, \star\rangle$ are subgroups of $\langle G, \star\rangle$ (identity: e)
Then, $e \in H$ and $e \in K$.
Thus $e \in H \cap K$.

③ (inverse)
Let $x \in H \cap K$. Since $x \in H$ and $x \in K$,
$x^{-1} \in H$ and $x^{-1} \in K$
Thus $x^{-1} \in H \cap K$.
Therefore by Thm 5.14, $\langle H \cap K, \star\rangle$ is a subgroup of $\langle G, \star\rangle$. ∎

For grad students:

#46 Prove a cyclic group w/ only one generator can have at most 2 elts.

Proof: Suppose G is a group with only one generator, call it $a \in G$.
xax^{-1}
Since $\langle a\rangle = G$, also $\langle a^{-1}\rangle = G$, by definition of $\langle a^{-1}\rangle$.
Since there's only one generator, $a = a^{-1}$.
But this means
$\langle a\rangle = \{a, e\}$, completing the proof. ∎

#47 If $\langle G, \star\rangle$ abelian with identity e, then $H = \{x \in G : x^2 = e\}$ makes $\langle H, \star\rangle$ ~~into~~ a subgroup of $\langle G, \star\rangle$.

Proof: ① (closure)
If $x, y \in H$, then $x^2 = e$ and $y^2 = e$.
Now compute
$$(xy)^2 = xyxy \underset{\substack{\uparrow \\ \text{abelian}}}{=} x^2y^2 = ee = e$$ ✓

② (identity)
$e^2 = ee = e \Rightarrow e \in H$ ✓

③ (inverses)
Let $x \in H$. Then $x^2 = e$. Multiply by x^{-2}:
$x^{-2}x^2 = x^{-2}e$
$\underbrace{x^{-1}(x^{-1}x)x}_{x^{-1}ex \,=\, x^{-1}x \,=\, e} = (x^{-1})^2$
So, $e = (x^{-1})^2$, thus $x^{-1} \in H$.
Therefore by Thm 5.14, $\langle H, \star\rangle$ is a subgroup of $\langle G, \star\rangle$. ∎

#49 If $a \in G$, G finite, $\langle G, \star\rangle$ has identity e, then $\exists\, n \in \mathbb{Z}^+$ such that $a^n = e$.

Proof: Since G is finite, $\exists\, n_1, n_2 \in \mathbb{Z}$ (WLOG assume $n_1 > n_2$)
so that $a^{n_1} = a^{n_2}$ (otherwise, G would be infinite!!).
Multiply on right by a^{-n_2} to get
$a^{n_1}a^{-n_2} = e$
$a^{n_1 - n_2} = e$
and $n_1 - n_2 > 0$. ∎