Q7. $S := \mathbb{R} \setminus \{-1\}$

Define binary operation $*$ on $S$ by

$a, b \in S \quad a * b := a + b + ab.$

Prove $(S, *)$ is an abelian group

We showed $*$ is closed on $S$

i.e. $a, b \in S \Rightarrow a * b \in S$

<u>Associativity</u>

claim $(a*b)*c = a * \overbrace{(b*c)}^{b+c+bc}$

Proof:

$(a*b)*c = (a+b+ab) * c$ , def of $*$

$= (a+b+ab) + c + (a+b+ab)c$

, by def of $*$

$= a+b+ab+c+ac+bc+abc$

$= a + ab + (b+c+bc) + ac + abc$

$= a + (b+c+bc) + a(b+c+bc)$

$= a * (b+c+bc)$ , def of $*$

$= a * (b * c)$

Pause: Claim $x * y = y * x$.

$\boxed{x * y} = x + y + xy$, def of $*$

$= y + x + yx$, since $+, \cdot$ commutative on $\mathbb{R}$.

$= \boxed{y * x}$

$(S, *)$ will be abelian.

Identity The identity for $*$ is $\underline{0}$.

For any $a \in S$.

since $a * 0 = a + 0 + a \cdot 0$

$= a$

Inverses For $\underline{a \in S}$, is there an $a^{-1} \in S$?

Claim: $a^{-1} = \dfrac{-a}{1+a}$. Good.

Let's discover this.

We want

$a * a^{-1} = 0$

$$\iff a + a^{-1} + aa^{-1} = 0$$

$$\iff a + a^{-1}(1+a) = 0$$

$$\iff a^{-1} = \frac{-a}{1+a}, \quad \text{and } 1+a \neq 0$$

So yes there is an inverse in $S$

$\left(\text{note also } \frac{-a}{1+a} \neq -1\right)$

Therefore $(S, *)$ is a group.

and abelian property proved above. $\blacksquare$

Basic properties that come straight from the definition

Prop 3.17 The identity element is unique.

Proof Suppose there are two identities $e_1, e_2$. Consider the product $e_1 e_2$ element

(Writing the group products without $\circ$)

$$e_1 = e_1 e_2 = e_2$$

$e_2$ is an identity

since $e_1$ is an identity

So $e_1 = e_2$. ∎

<u>Prop 3.18</u> Inverses are unique.

<u>Proof</u> Let $g \in G$, suppose $g', g''$ are both inverses of $g$.

Consider $g' g g''$

$$g'' = g' g g'' = g'$$

<u>Prop 3.19</u> $\forall a, b \in G$

$$(ab)^{-1} = b^{-1} a^{-1}.$$

- Seen in linear algebra for mat. mult.
- Seen in reality.

<u>Prop 3.20</u> $\forall a \in G \quad (a^{-1})^{-1} = a$.

<u>Prop</u> 3.21, 3.22.

3.21 $ax = b \implies x = a^{-1}b$.

$$a(a^{-1}b) = aa^{-1}b = eb = b.$$

$$xa = b \Rightarrow x = ba^{-1}$$

---

$$ba = ca \Rightarrow b = c$$

Proof

$$ba = ca$$

$$\Leftrightarrow b = caa^{-1}, \text{ using Prop 3.21.}$$

$$= ce$$

$$= c$$

---

Warning.

If $ba = ac$

does not imply that $b = c$.

We can say

$$ba = ac \Rightarrow baa^{-1} = aca^{-1}$$

$$\Rightarrow b = aca^{-1}$$

ie always be aware of abelian status of your group

---

We can use exponential notation

For $g \in (G, \circ)$

$g^n$ will mean , for $n > 0$

$$g^n := \underbrace{g \circ g \circ g \circ \cdots \circ g}_{n \text{ } g\text{s here.}}$$

and can extend to this with the definitions

$$g^0 := e.$$

and for $n > 0$

$$g^{-n} := \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ copies of } g^{-1}}.$$

Then it will satisfy usual rules of indices in theorem 3-23.

WARNING Unless you know $G$ is abelian, we can't simplify

$(gh)^n$ to $g^n h^n$

$(gh)^n = gh \, gh \cdots gh$

## Additive notation

For a known abelian group we can use the + symbol for the operation

In this we talk about/use "multiple notation"

For $n \in \mathbb{Z}$, $n \geq 0$

$$ng := g + g + \cdots + g$$

Inverse elements are written as negatives. $-g$ etc.

Continue at 5:05.

---

## Subgroups

Compare with/consider the concept of vector subspaces of a vector space.

**Def** If $G$ is a group. A subset $H$ of $G$ ($H \subseteq G$) forms a subgroup of $G$ if $H$ is a group under the same operation as in $G$.

For any group $G$ we can always point to two particular subgroups

The trivial subgroup $\{e\} \subset G$

The whole group $G$ itself. $G \subseteq G$.

So of real interest will be

any non-trivial proper subgroups.

i.e. subgroups $H$

$$\{e\} \neq H \subset G \quad \text{but } H \neq G.$$

If indeed there are any.

---

Eg 3.24.

$$(\mathbb{R}^*, \cdot)$$

has the subgroup $\mathbb{Q}^*$, non-zero rationals


note $\mathbb{R}^* \setminus \mathbb{Q}^*$ is not a group.

- $1 \notin \mathbb{R}^* \setminus \mathbb{Q}^*$
- also not closed
  $\sqrt{2}\sqrt{2} = 2 \notin \mathbb{R}^* \setminus \mathbb{Q}^*$.

---

Ex 3.25

$$H = \{1, -1, i, -i\} \subset \mathbb{C}^*.$$

forms a subgroup, here's its Cayley

| | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

---

<u>Eg 3.26</u>

$$SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) : \det(A) = 1 \}.$$

forms a subgroup of $GL_n(\mathbb{R})$

<u>Proof</u> needs some facts from linear algebra.

<u>Closure</u> Given $A, B \in SL_n(\mathbb{R})$

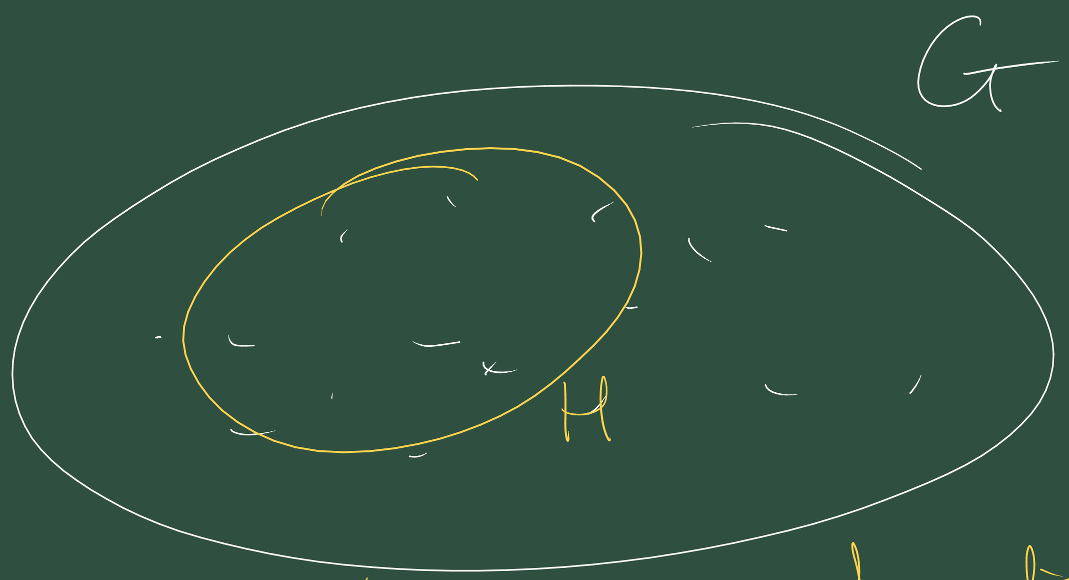
Q $AB \in SL_n(\mathbb{R})$?

$$\det(AB) = \det(A)\det(B)$$
$$= 1 \cdot 1$$
$$= 1$$
$$\Rightarrow AB \in SL_n(\mathbb{R})$$

$I \in SL_n(\mathbb{R})$

Q Is $A^{-1} \in SL_n(\mathbb{R})$

$$\det(A^{-1}) = \frac{1}{\det(A)}$$
$$= \frac{1}{1}$$
$$= 1$$
$$\Rightarrow A^{-1} \in SL_n(\mathbb{R}).$$




Associativity on H automatically follows from the known associativity on G.

Q? Given a subset H of G.
How do we prove H is a subgroup of G.

$\boxed{Q4.1}$ Consider the parent group $\mathbb{R}^*$

Consider the subset.

$$G = \{ a + b\sqrt{2} : a, b \in \mathbb{Q}, \text{ not both zero} \}$$

"adjoining the irrational $\sqrt{2}$ to the rationals"

Prove G is a subgroup of $\mathbb{R}^*$.

Proof using Prop 3.20

1. ~~If~~ Is e in G?
ie, is 1 in G?
yes, $1 = 1 + 0\sqrt{2}$ ✓

a, b not both zero
$a, b, c, d \in \mathbb{Q}$ c, d " " "

2. Closure.
$x = a + b\sqrt{2}$
Let $x, y \in G$, lets say $y = c + d\sqrt{2}$

$$xy = (a + b\sqrt{2})(c + d\sqrt{2})$$
$$= ac + 2bd + ad\sqrt{2} + bc\sqrt{2}$$

$$= (ac + 2bd) + (ad + bc)\sqrt{2}$$

$$\Rightarrow xy = \underset{\in \mathbb{Q}}{\underline{\quad\quad}} + \underset{\in \mathbb{Q}}{\underline{\quad\quad}}\sqrt{2}$$

$$\Rightarrow xy \in G$$

Both new coefficients ~~coeff~~ zero?

No because $xy \neq 0$. since

$x \neq 0, y \neq 0$

3. Existence of ~~identities~~. inverses.

Given $x = a + b\sqrt{2} \in G$

Is $x^{-1}$ in G?

$$x^{-1} = (a + b\sqrt{2})^{-1}$$

$$= \frac{1}{a + b\sqrt{2}}, \quad \text{known inverse in } R^*$$

$$? = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}}, \quad \text{using the conjugate of } a+b\sqrt{2}$$

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

$\in G$ ✓.

So by Prop 3.30 $G$ is a subgroup of $\mathbb{R}^{\times}$.