Chapter 2 Groups

§2.2, 2.1 Groups & subgroups (& laws of composition)

DEF'N: A group is a set G with a law of composition (just a function!) $G \times G \to G$, $(a,b) \mapsto ab$

satisfying
- associativity: $(ab)c = a(bc)$ $\forall a,b,c \in G$
- existence of (2-sided) identity: $\exists\, 1 \in G$ with $1 \cdot a = a \cdot 1 = a$ $\forall a \in G$
- existence of (2-sided) inverses: $\forall a \in G$ $\exists\, b \in G$ with $ab = ba = e$ (and b is called a^{-1})

A subset $H \subseteq G$ is called a subgroup of G (written $H \leq G$) if it is also a group using the same composition law $G \times G \to G$, that is, it satisfies

- closure (under composition): $a,b \in H \Rightarrow ab \in H$ (this lives in G, a priori, maybe not in H)
- existence of identity: $1 \in H$
- closure under inverses: $a \in H \Rightarrow a^{-1} \in H$

9/21/18

EXAMPLES: ① S_n = symmetric group (on n letters)

$= \{$ permutations $\{1,2,\dots,n\} \xrightarrow{p} \{1,2,\dots,n\} \}$

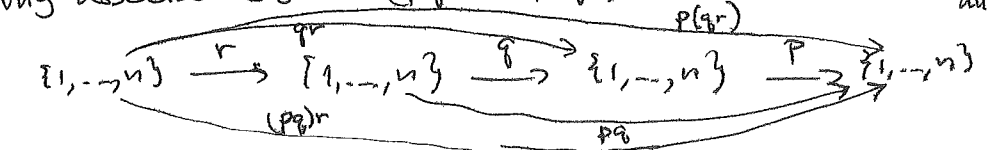
with Law of Composition: $S_n \times S_n \longrightarrow S_n$

$(p, q) \longmapsto pq$

Q: Who is 1?

$1 = e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ since $ep = pe = p$ $\forall p \in S_n$

Why associative? $(pq)r = p(qr)$? YES: Both equal the result of doing all 3 in a row here...



(2) $GL_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : A \text{ invertible, i.e. } A^{-1} \text{ exists in } \mathbb{R}^{n\times n}\}$
(i.e. $\det A \neq 0$)

general linear group

with $GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$
$(A, B) \longmapsto AB$
always invertible, if A, B were!

associative ✓
identity? $1 = I_n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ✓
inverses? Yes, by defin!

---

(3) One also has (with same composition laws)
$GL_n(\mathbb{C}) := \{A \in \mathbb{C}^{n\times n} : \det A \neq 0\}$ a group
$GL_n(\mathbb{Q}) := \{A \in \mathbb{Q}^{n\times n} : \det A \neq 0\}$ a group
$GL_n(\mathbb{Z}) := \{A \in \mathbb{Z}^{n\times n}, \det A \neq 0\}$ Nope! $A \in \mathbb{Z}^{n\times n}$ with $\det A \neq 0$ might have $A^{-1} \notin \mathbb{Z}^{n\times n}$
$= \in \mathbb{Q}^{n\times n}$
$\frac{1}{\det A}\,\mathrm{cof}(A)$

$:= \{A \in \mathbb{Z}^{n\times n} : \det A \in \{\pm 1\}\}$

and this gives a tower of subgroups

$$GL_n(\mathbb{Z}) < GL_n(\mathbb{Q}) < GL_n(\mathbb{R}) < GL_n(\mathbb{C})$$

"is a subgroup of"

---

(4) $SL_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : \det A = 1\} < GL_n(\mathbb{R})$

special linear group

Why?

Check: closure: $\left.\begin{matrix}\det A = 1 \\ \det B = 1\end{matrix}\right\} \Rightarrow \det(AB) = \det A \cdot \det B = 1 \cdot 1 = 1$ ✓

identity: $\det(I_n) = 1$ ✓

inverses: $\det A = 1 \Rightarrow \det(A^{-1}) = 1$ since
$A \cdot A^{-1} = I_n$
$\Rightarrow \det(A) \cdot \det(A^{-1}) = \det(I_n) = 1$
so $\det(A^{-1}) = \frac{1}{\det A} = \frac{1}{1} = 1$ ✓

(24) Before more examples, a few "housekeeping" details...

PROPOSITION: A group G has a unique identity element 1, and for each $a \in G$ the (2-sided) inverse a^{-1} is unique

proof: If both $1, 1' \in G$ have $1 \cdot a = a \cdot 1 = a \quad \forall a \in G$
$1' \cdot a = a \cdot 1' = a$

then
$$1' = 1 \cdot 1' = 1$$

If $a \in G$ has both $ba = ab = 1$
$ca = ac = 1$

then
$$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$$ ∎

PROPOSITION: The associative law $(ab)c = a(bc)$ implies any parenthesization of $a_1 a_2 \cdots a_n$ takes the same value, say that of $(\cdots((a_1 a_2) a_3) a_4) \cdots) a_n)$.

↑ call this the left-parenthesization

e.g.
$$((ab)c)d = (a(bc))d$$
$$(ab)(cd) \qquad a((bc)d)$$
$$a(b(cd))$$

proof: Prove the assertion by induction on n, with base case $n=3$ being the assoc law $a_1(a_2 a_3) = (a_1 a_2) a_3$.

In the inductive step, given some parenthesization, it looks like

$A \cdot B$ where A parenthesizes $a_1 a_2 \cdots a_k$ for some $1 \le k \le n-1$
B parenthesizes $a_{k+1} a_{k+2} \cdots a_n$

e.g. $\underbrace{(a((b\ c)\ d))}_{A}\underbrace{(((e\ f)(g\ h))\ i)}_{B}$ has $n=9$, $k=4$

If B is just a single letter (i.e. $k=n-1$) then we can apply $(-A-)a_n$ induction to say A evaluates to the left-parenthesization of $n-1$ letters

and we're done, since AB is the left-parenthesization of n letters.

If B has more letters, apply induction to B to say that it evaluates to the left parenthesization of $a_{k+1} a_{k+2} \cdots a_n$

so AB evaluates to

$$(-A-)((\cdots((a_k a_{k+1}) a_{k+2}) \cdots a_{n-1}) a_n)$$

$\|$ assoc. law applied to this pair ( )

$$(((-A-)(((a_k a_{k+1}) a_{k+2}) \cdots a_{n-1}))a_n$$

$\|$ the case $k=n-1$

$$(\cdots(((a_1 a_2) a_3) a_4) \cdots a_{n-1}) a_n \quad \blacksquare$$

More EXAMPLES

(5) $\mathbb{R}^+ := \mathbb{R}$ with composition law $\mathbb{R}\times\mathbb{R} \to \mathbb{R}$, $(a,b) \mapsto a+b = b+a$

this is not the positive reals $\{x \in \mathbb{R} : x > 0\}$!

↑ commutative, or an abelian group

Here one writes 0 instead of 1 for the identity, since $0+a = a+0 = a$

and one writes $-a$ instead of a^{-1} for inverses

(and one writes $a+b$ not ab); people do this traditionally for other abelian groups.

Similarly one has subgroups

$$\mathbb{Z}^+ < \mathbb{Q}^+ < \mathbb{R}^+ < \mathbb{C}^+$$

---

(6) $\mathbb{R}^\times := \{x \in \mathbb{R} : x \text{ has a multiplicative inverse in } \mathbb{R}\}$ i.e. $\frac{1}{x} \in \mathbb{R}$

$= \mathbb{R} - \{0\}$

with composition law $\mathbb{R}^\times \times \mathbb{R}^\times \longrightarrow \mathbb{R}^\times$

$(a, b) \longmapsto ab$

$1 = 1$ (!)

$a^{-1} = \frac{1}{a}$

One has subgroups

$$\mathbb{Z}^\times < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$$

$\mathbb{Z}^\times \not\hookrightarrow \mathbb{Z} - \{0\}$ $\quad \mathbb{Q}^\times = \mathbb{Q} - \{0\}$ $\quad \mathbb{R}^\times = \mathbb{R} - \{0\}$ $\quad \mathbb{C}^\times = \mathbb{C} - \{0\}$

Q: Why not?

Why is $\mathbb{Z}^\times := \{x \in \mathbb{Z} : x \text{ has a mult. inverse in } \mathbb{Z}\}$

$= \{\pm 1\}$?

Q: Given $z = x + iy \in \mathbb{C} - \{0\}$, what is z^{-1} in terms of x, y?

$$\frac{1}{z} = \frac{1}{x+iy} = \frac{x-iy}{x-iy} \cdot \frac{1}{x+iy}$$

$$= \frac{x-iy}{x^2+y^2}$$

Why can't this vanish?

$$= \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}$$

9/29/18 >

P. Pylyavskyy will be subbing...