

Last time: Laws of composition

Today: Continue w/ laws of comp; define a group

Recall: S set, a LOC on S is a map $S \times S \rightarrow S$
 defined ~~assoc~~ LOC: This means

$$(ab)c = a(bc) \quad \forall a, b, c \in S$$

Defⁿ If S is a set w/ ^{an associative} LOC, we say S has an identity if there is an elt $e \in S$ s.t

$$ea = a = ae \quad \forall a \in S.$$

Ex 1) $S = M_n(\mathbb{R})$, LOC is mult. Then $e = I_n$
 (the identity matrix) $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is an identity for S .

2) $(\mathbb{R}, +)$. Then 0 is an identity b/c

$$0 + a = a = a + 0 \quad \forall a \in \mathbb{R}$$

3) T set, $S = \{f: T \rightarrow T\}$. Then $e: T \rightarrow T$
 defined by $e(t) = t$ for all t is an identity for S .

S has LOC as composition of fns.

e identity: $f \circ e = f = e \circ f \quad \forall f: T \rightarrow T$

Claim: Suppose $e, e' \in S$ are both identities. Then $e = e'$.
 (identities are unique)

or.

(identifiers are unique)

Pf: $e = e e' = e'$

Frequently: write 1 or 0 for the identity on S w/ a LOC

1: if LOC is written mult

○: if LOC is written additively

an associative

Inverses Suppose S is a set w/ $\sqrt{\text{L.O.C.}}$ and an identity, $1 \in S$. An elt $a \in S$ is said to be invertible

with inverse b.e.s if

$$ab = 1 = ba.$$

b' is called "the" inverse of a .

Properties of inverses S a set w/ assoc L.O.C.

1) If $\exists l, r \in S$ w/ $la = 1 = ar$, then $l = r$ and a is invertible.

2) If a is invertible, then its inverse is unique

3) $(ab)^{-1} = b^{-1}a^{-1}$. I.e., if a and b are both invertible, then so is ab , and its inverse is $b^{-1}a^{-1}$.

Pf: 1) $r = (1)r = (l_a)r = l(ar) = l \cdot 1 = l$
 $\uparrow$ $\uparrow$
 b/c 1 an identity assoc. $\checkmark$

2) Suppose b_1 and b_2 are both inverses to an elt a .
 • Have: $b_1 a = 1 = a b_2$
 • now apply 1) to obtain $b_1 = b_2$. ✓

$$3) \cdot (5^{-1} \vec{a}) (ab) = b^{-1} (\vec{a}^{-1} a) b = b^{-1} 1 b = b^{-1} b = 1.$$

$$3) \cdot (b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1b = b^{-1}b = 1.$$

$$\bullet \text{ Similarly, } (ab)(b^{-1}a^{-1}) = 1$$

$\Leftrightarrow ab$ is inv. w/ inverse $b^{-1}a^{-1}$. $\checkmark$ ~~10~~

Rmk: 1) It's possible that $a \in S$ has a left inverse
(ie an elt $l \in S$ w/ $la = 1$) but not a right
inverse.

2) Notation: If $a \in S$, then $a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}$ if $n > 0$.

If a is invertible, $n > 0$

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ times}}.$$

$n=0$, $a^0 = 1 \in S$
 With this notation, $\underbrace{a^r a^s = a^{r+s}}_{\text{think about this}}$ for all $r, s \in \mathbb{Z}$.

Main defⁿ of course

Defⁿ: Suppose G is a set w/ a L.O.C. Then G is said to be
a group if

- 1) the L.O.C. is assoc.
- 2) there is an identity
- 3) every elt of G has an inverse.

Examples

- 1) $\mathbb{R}^{\times}$: nonzero real #'s w/ mult as L.O.C.
- 2) $\mathbb{C}^{\times}$: nonzero complex #'s w/ mult as L.O.C.

3) $n > 0$ integer $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$

4) $(\mathbb{R}, +)$: real #'s w/ addition as L.O.C.

5) C_n : $n > 0$ positive integer. All rotations of $\mathbb{R}^2$ by angles that are multiples of $\frac{2\pi}{n}$.

Defⁿ. A gp is said to be abelian if the gp law (ie the L.O.C.) is commutative.

- If G is a gp, the order of G , written $|G|$, is the # of elts of G .
 - If order is finite, we say G is a finite gp
 - If order is infinite, we call G an infinite gp.

Examples

- $\mathbb{R}^*$, $(\mathbb{R}, +)$ are infinite ab^l gps
- $GL_n(\mathbb{R})$ is an infinite non-ab^l gp
- C_8 : is a finite, ab^l gp.

non examples

- $(\mathbb{R}, \times)$: not a gp: 0 does not have an inverse
- $(\mathbb{R}^3, \times)$: not a gp: L.O.C. is not assoc, no identities
 $\uparrow$
 cross product

Propⁿ G a gp, $a, b, c \in G$. Then

- $ab = ac \implies b = c$
- $ba = ca \implies b = c$.

$$\cdot ab = ac \implies b = c$$

$$\cdot ba = ca \implies b = c.$$

Pf: $ab = ac \implies a^{-1}(ab) = a^{-1}(ac)$ by inverses

$$\Downarrow$$

$$(\bar{a}^{-1}a)b = (\bar{a}^{-1}a)c \quad \text{by assoc.}$$

$$\Downarrow$$

$$1b = 1c \quad \text{by identities}$$

$$\Downarrow$$

$$b = c$$

More examples of gps

T a set

$f: T \rightarrow T$ is bijective if

$$\cdot f(t_1) = f(t_2) \implies t_1 = t_2$$

$$\cdot \text{and for every } t \in T \exists t' \in T \text{ w/ } f(t') = t$$

bijective fns permute the elts of T .

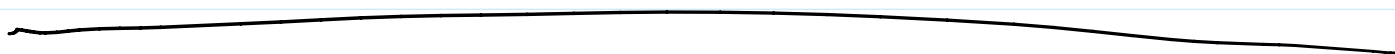
$G = \{f: T \rightarrow T \text{ bijective}\}$. Then G is a gp w/ gp law composition of fns.

Important special case: $T = \{1, 2, 3, \dots, n\}$ $n > 0$ positive integer.

The gp of permutations of T is denoted S_n and is called the symmetric gp on n -elts.

Q: For $T = \{1, 2, \dots, n\}$, 1) what is the size of the set of fns from $T \rightarrow T$? 2) what is the size of the set of bijective fns from $T \rightarrow T$, i.e. what is the order of S_n ?

Ans 1) n^n
2) $n! = n(n-1)(n-2) \dots (1)$.



A hand-drawn black curve on lined paper. The curve starts with a small vertical tick on the left, rises to a peak, and then gradually descends. The paper has horizontal blue lines and a vertical red margin line on the left.