Warm up questions

1) Is $(\underbrace{\mathbb{R} \cup \{\infty\}}_{S}, *)$ a group with $a*b = \min\{a,b\}$?

2) What is the inverse of $z=-1$ in the gp $(\mathcal{U}, \cdot)$

3) If c' denotes the inverse elt of $c \in G$ then $(a' * b')' = ?$

4) assume $*$ and $\#$ are associative for which operation is $\underbrace{\{e, a, b, c\}}_{\text{correction}}$ a group ?

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	e
b	b	c	e	a
c	c	e	a	e

G2 e = identity ✓

G3 inverses are supp. to be

not a group

bcl $a*a = a*c = e$ ✗

$\#$	e	a	b	c
e	e	b	a	c
a	b	b	e	c
b	a	e	c	a
c	c	c	a	a

no identity element

✗ not a group

1) Is $(\underbrace{\mathbb{R} \cup \{\infty\}}_{=S}, *)$ a group with $a*b = \min\{a,b\}$?

Last time: $(\mathbb{R}, \max)$ max was associative ✓

__G1__ $a*(b*c) = \min\{a,b,c\} = (a*b)*c$

__G2__ Identity? $a*e = e*a = a$ $e := \infty$
$\min\{a, e\}$ is the identity

__G3__ Inverses $a*a' = e$?
$\min\{a, a'\} = \infty$.

say $a = 0$ $\min\{0, a'\} \leq 0 < \infty$ no inverses for $\min = *$.

2. inverse of $z = -1$ in $(U, \cdot)$

$U = \{z \in \mathbb{C} \mid |z| = 1\}$.

inverse is z' s.t.

$$z \cdot z' = z' \cdot z = 1 \Rightarrow z' = -1.$$

$$z' \cdot (-1) = 1$$

$$z' = -1.$$

3. $(a' * b')' = (b')' * (a')' = b * a$

<u>Cor 4.18</u>. $(a * b)' = b' * a'$

Thm 4.16 (Solving equations in groups)

Let $(G,*)$ be a group and $a, b \in G$. Then

$a * x = b$ and $y * a = b$ have unique

solutions for x and y, respectively. ("linear equations")

Proof Consider $a * x = b$, let $a' \in G$ be inverse of a $\boxed{G3}$

Then $a' * (a * x) = a' * b$

$\underline{G1} \Rightarrow (a' * a) * x = a' * b$

$\underline{G3} \Rightarrow e * x = a' * b.$

$\underline{G2} \Rightarrow x = a' * b \in G.$

See text for a slightly different proof

Therefore, $x = a' * b$ is the <u>unique</u> solution $\square$.

Question Why does $x = a' * b$ imply x is unique.

$\underline{a' * b} : *(a', b)$

$* : S \times S \to S.$

a function!

it is well defined

ie. $a' * b$ is a <u>unique</u> elt of S.

Group multiplication tables pg 43. $|G| = n$

	g_0	g_1	$\cdots$	g_{n-1}
g_0	g_0	g_1	$\cdots$	g_{n-1}
g_1	g_1		$\cdots$	
$\vdots$	$\vdots$			
g_{n-1}	g_{n-1}			

<u>G1</u> associativity is unfortunately <u>not</u> easy to check from the table.

<u>G2</u> $\exists$ an elt g_0 $= e$. s.t. the row & column for g_0 are exactly the list of gp elts as ordered in the table. $\circledast$

<u>G3</u> $\exists$ of inverses $\forall\, g_i$, e must appear at <u>least</u> once.

These properties follow from the axioms!

<u>Thm 4.17</u> uniqueness of inverses and identity elt. $\Rightarrow$ there is one such g_0 with property $\circledast$. Also e appears exactly once in each row and column.

<u>Thm 4.15</u> Every group elt must appear exactly once in each row and each column.

Def 4.1 A group $(G, *)$ is a binary structure such that

$\boxed{G1}$: $*$ is associative
$\forall\ a,b,c \in G \quad (a*b)*c = a*(b*c)$

$\boxed{G2}$: Identity element
$\exists\ e \in G$ s.t. $\forall\ a \in G \quad e*a = a*e = a$.

$\boxed{G3}$: Inverse elements Say "a' is the inverse of a in G"
$\forall\ a \in G \quad \exists\ a' \in G$ s.t. $a*a' = a'*a = e$.

Ques What should we require of a group isomorphism?

$(G, *)$, $(G^\#, \#)$

$f : G \to G'$

1) $f : G \to G^\#$ is bijective
2) $\forall\ x,y \in G. \quad f(x*y) = f(x) \# f(y)$

isomorphism of binary structures.

We should also desire:

3) G2 $f(e) = e^\# \in G^\#$ e iden. in G $e^\#$ iden. in $G^\#$.

4) G3 $f(a') = f(a)'$ where $'$ denotes inverse of elts in G and $G^\#$

If $(G, *)$ and $(G', *')$ are groups and the underlying binary structures are isomorphic then:

(i.e. we get property 3 + 4 from previous page for free.)

- $\varphi(e) = e' \in G'$

exercise

- $\varphi(a') = \varphi(a)' \in G'$

exercise

Equivalent group axioms

Finally, it is possible to give axioms for a group $\langle G, *\rangle$ that seem at first glance to be weaker, namely:

1. The binary operation $*$ on G is associative.
2. There exists a **left identity element** e in G such that $e * x = x$ for all $x \in G$.
3. For each $a \in G$, there exists **a left inverse** a' in G such that $a' * a = e$.

pg 43

Exercise 4.38 (also see 4.39!)

Group multiplication tables and isomorphisms

The following two tables define groups. Are they isomorphic?

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$*$	e'	a'	b'	c'
e'	e'	a'	b'	c'
a'	a'	b'	c'	e'
b'	b'	c'	e'	a'
c'	c'	e'	a'	b'