consider $a * x = b$ in the following structures

$(\mathbb{Z}, +)$

$a + x = b$ for $a, b \in \mathbb{Z}$

$(-a) + a + x = (-a) + b$

$((-a) + a) + x = (-a) + b$ (associativity)

$0 + x = -a + b$

$x = -a + b$

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

$a \cdot x = b$ $a, b \in \mathbb{Q}^*$

$\frac{1}{a} \cdot (a \cdot x) = \frac{1}{a} \cdot b$

$(\frac{1}{a} \cdot a) \cdot x = \frac{1}{a} \cdot b$

$x = b/a$

Definition

let S^* be an alg. structure

Then $(S, *)$ is a **group**

(has group structure iff

1) $*$ is associative iff

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

2) The identity element e is in S

$\exists! e \in S, \ \forall a \in S \quad a*e = e*a = a$

3) All elems of S have (unique) inverses in S (wrt $*$)

$\forall a \in S, \ \exists! a' \in S, \ a*a' = e$

examples

1) $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ - groups bcs

1) addition is associate

2) identity is 0

3) additive inverse of a is $-a$

but $(\mathbb{N}, +)$ is not a group bcs
$\mathbb{N}$ does not contain additive identity 0

2) $(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - groups
1) mult is associative
2) identity is 1
3) inverse of $a \in \mathbb{R}^* (\mathbb{Q}^*)$ is
$1/a \in \mathbb{R}^* (\mathbb{Q}^*)$

but $(\mathbb{Z}^*, \cdot)$ is not a group bcs
not all elems have inverses

Definition

let $(G, *)$ be a group
Then G is an **abelian** group iff
$*$ is commutative

$\forall a, b \in G, \quad a * b = b * a$

Notice that all prev. examples were abelian groups.

example

$(U, \cdot)$ is a group (abelian)

1) complex # mult. is associative
2) Identity is $1 + 0i = e^{0i} \in U$
3) Inverse of z is $z^{-1} = e^{i(2\pi - \theta)} \in U$

& $(U, \cdot) \simeq (\mathbb{R}_{2\pi}, +_{2\pi})$

$\Rightarrow (\mathbb{R}_{2\pi}, +_{2\pi})$ - abelian group

Definition

let $(S, *)$ be an alg. struct.

S is a **semigroup** iff $*$ is associative on S

Definition

Let $(S, *)$ be a semigroup

S is a **monoid** iff

S contains the identity w.r.t. $*$

Definition

Let $(S, *)$ be a monoid

S is a **group** iff

all elements of S have unique inverses wrt $*$

<u>examples</u>

$(\mathbb{Z}^+, +)$ ~ (commutative) semigroup
$\parallel$
$\mathbb{N}$

$(\mathbb{Z}^+, \cdot)$ - (commutative) monoid

$(M_n(\mathbb{R}), \cdot)$ - (non-commutative) monoid

Properties

Lemma.

Let G^* be a group w/ identity e

The left & right cancellation laws hold in G (that is)

$$\forall a,b,c \in G, \quad a*b = a*c \Rightarrow b=c$$
$$\wedge \quad b*a = c*a \Rightarrow b=c$$

Proof

consider $a*b = a*c$ for $a,b,c \in G$

Then $\exists! a' \in G, a'*a = e$ hence

$$a'*(a*b) = a'*(a*c)$$

By group property ①,

$$(a'*a)*b = (a'*a)*c$$

By group prop 2 & 3

$$e*b = e*c \Rightarrow b=c$$

Fact 1

let $(G,*)$ be a group

the inverse a' of a in G
is a unique elem of G

Proof

Assume a' & a'' are inverses of a wrt $*$

$$a' * a = a * a' = e \wedge a'' * a = a * a'' = e$$

(by property 3)

Since $a * a' = e \wedge a * a'' = e$,

$a * a' = a * a''$ so $a' = a''$

Fact 2

let $(G,*)$ be a group (not abelian)

$a * x = b \wedge x * a = b$ have
unique solns in G

Proof

consider $a * x = b$, by prop 3 & 2

$\exists' a' \in G$, $a' * a = e$ hence

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

By group prop 1,

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

By prop 3 + 2

$e * x = a' * b$ + $x = a' * b$

To show soln is unique, assume both x_1 + x_2 are solns to $a * x = b$

$a * x_1 = b \wedge a * x_2 = b$ hence

$$a * x_1 = a * x_2$$

By property of cancellation,

$$x_1 = x_2$$

Finite Groups + Group Tables

The least group is 1 element

$(\{e\}, *)$ with table

$*$	e
e	e

consider 2-elem group struct.

$(\{e, a\}, *)$ w/ table

$*$	e	a
e	e	a
a	a	e

since all elems must have inverses, a must be its own inverse

consider set $\mathbb{Z}_2 = \{0, 1\}$ w.r.t. addition mod 2

0: all even integers

1: all odd integers

$+$	0	1
0	0	1
1	1	0

Def

The order of a group $(G, *)$ is $|G|$

Note: There is only one group of order 1, the identity group

Note: There is only one group of order 2, up to isomorphism

$(\mathbb{Z}_2, +_2)$

consider $(\{e, a, b\}, *)$

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

There is only 1 group of order 3, isomorphic to $(\mathbb{Z}_3, +_3)$