Groups

Definition

Let G be a binary algebraic structure:

To say that G is a *semigroup* means G is associative.

To say that G is a *monoid* means G is a semigroup with a two-sided identity element.

To say that G is a *group* means G is a monoid and every element in G has a two-sided inverse.

To say that (semi)group G is *abelian* means G is commutative.

Common examples:

structure	type	reason
$\langle \mathbb{Z}, + \rangle$	abelian	
$\langle \mathbb{Q}, + \rangle$	abelian	
$\langle \mathbb{R}, + \rangle$	abelian	
$\langle \mathbb{C}, + \rangle$	abelian	
$\langle \mathbb{Z}, \cdot \rangle$	monoid	$0^{-1} \notin \mathbb{Z}$
$\langle \mathbb{Q}, \cdot \rangle$	monoid	$0^{-1} \notin \mathbb{Q}$
$\langle \mathbb{R}, \cdot \rangle$	monoid	$0^{-1} \notin \mathbb{R}$
$\langle \mathbb{C}, \cdot \rangle$	monoid	$0^{-1} \notin \mathbb{C}$
$\langle \mathbb{Z}^*, \cdot \rangle$	monoid	Except for $a = \pm 1, a^{-1} \notin \mathbb{Z}^*$
$\langle \{-1, 1\}, \cdot \rangle$	abelian	
$\langle \mathbb{Q}^*, \cdot \rangle$	abelian	
$\langle \mathbb{R}^*, \cdot \rangle$	abelian	
$\langle \mathbb{C}^*, \cdot \rangle$	abelian	

To prove that a binary algebraic structure G is a group, show that:

1). The binary operation is indeed closed and well-defined:

$$\forall\, a, b \in G, ab \in G$$

$$\forall\, a, b, c, d \in G, ab = c \text{ and } ab = d \implies c = d$$

2). G is associative:

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

3). G has an identity element:

$$\exists\, e \in G, \forall\, a \in G, ae = ea = a$$

4). Every element in G has an inverse that is also in G:

$$\forall\, a \in G, \exists\, a^{-1} \in G, aa^{-1} = a^{-1}a = e$$

To prove that a binary algebraic structure G is an abelian group, show that:

1). G is a group

2). G is commutative

Example

Prove: $\langle U_n, \cdot \rangle$ is an abelian group.

Note that $U_n \subset \mathbb{C}$, so as long as U_n is closed, it will inherit certain properties from C.

Closure

Assume $z_1, z_2 \in U_n$
$\exists\, h, k \in \mathbb{Z}_n, z_1 = e^{i\frac{2\pi h}{n}}$ and $z_2 = e^{i\frac{2\pi k}{n}}$
$z_1 z_2 = e^{i\frac{2\pi(h +_n k)}{n}}$
$h +_n k \in \mathbb{Z}_n$
$z_1 z_2 \in U_n$
$\therefore U_n$ is closed under multiplication.

Well-defined

Multiplication is well-defined in $\mathbb{C}$.
$\therefore$ multiplication is well-defined in U_n.

Associativity

$\langle \mathbb{C}, \cdot \rangle$ is associative
$\therefore \langle U_n, \cdot \rangle$ is associative.

Identity

1 is an identity element for $\langle \mathbb{C}, \cdot \rangle$
$1 = e^{i0} \in U_n$
$\therefore 1$ is an identity element for $\langle U_n, \cdot \rangle$.

Inverses

Assume $z \in U_n$
$\exists\, k \in \mathbb{Z}_n, z = e^{i\frac{2\pi k}{n}}$
Let $z^{-1} = e^{i\frac{2\pi(n-k)}{n}}$
$n - k \in \mathbb{Z}_n$
$z^{-1} \in U_n$
$zz^{-1} = z^{-1}z = e^{i2\pi} = 1$
z^{-1} is an inverse for z
$\therefore$ every element in U_n has an inverse that is also in U_n.

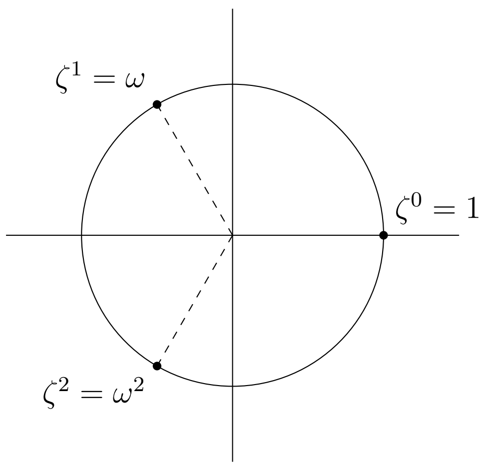
Commutativity

$\langle \mathbb{C}, \cdot \rangle$ is commutative
$\therefore \langle U_n, \cdot \rangle$ is commutative.

$\therefore U_n$ is an abelian group.

Let $n = 3$

$U_3 = \{1, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}}\} = \{1, \omega, \omega^2\}$



$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Definition

The *general linear group of degree n* is given by:

$$GL\langle n, \mathbb{R}\rangle = \{A \in M_n(\mathbb{R}) \mid A \text{ is invertible}\}$$

Example

Prove: $\langle GL\langle n, \mathbb{R}\rangle, \cdot\rangle$ is a group; however, it is not abelian.

Note that $GL\langle n, \mathbb{R}\rangle \subset M_n(\mathbb{R}), soaslongasGL\langle n, \mathbb{R}\rangle$ is closed, it will inherit certain properties from matrix arithmetic.

Well-defined

Matrix multiplication is well-defined.
$\therefore$ multiplication is well-defined in $GL\langle n, \mathbb{R}\rangle$.

Associativity

Matrix multiplication is associative.
$\therefore \langle GL\langle n, \mathbb{R}\rangle, \cdot\rangle$ is associative.

Identity

I_n is an identity for matrix multiplication.
I_n is invertible.
$I_n \in GL\langle n, \mathbb{R}\rangle$
$\therefore I_n$ is an identity element for $\langle GL\langle n, \mathbb{R}\rangle, \cdot\rangle$.

Inverses

Assume $A \in GL\langle n, \mathbb{R}\rangle$
A is invertible
A^{-1} exists and is invertible
$A^{-1} \in GL\langle n, \mathbb{R}\rangle$
$\therefore$ every element in $GL\langle n, \mathbb{R}\rangle$ has an inverse that is also in $GL\langle n, \mathbb{R}\rangle$.

Closure

Assume $A, B \in GL\langle n, \mathbb{R}\rangle$
$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$
So AB is invertible.
$AB \in GL\langle n, \mathbb{R}\rangle$
$\therefore GL\langle n, \mathbb{R}\rangle$ is closed under the binary operation.

Commutativity

Matrix multiplication is not commutative.

$\therefore \langle GL\langle n, \mathbb{R}\rangle, \cdot\rangle$ is a group, but not abelian.

It was already shown that a binary algebraic structure has at most one identity element, so a group always has a unique identity element.

<u>Theorem</u>

Let G be a group:

$\forall\, a \in G, a^{-1}$ is unique

<u>Proof</u>

Assume $a \in G$
Assume b and c are inverses of a
$ab = e = ac$
$b(ab) = b(ac)$
$(ba)b = (ba)c$
$eb = ec$
$\therefore b = c$

Theorem

Let G be a group:
G has exactly one idempotent element, namely e.

Proof

First, note that $ee = e$, so e is indeed idempotent. Now, assume $a \in G$ is idempotent.

$$\begin{aligned} aa &= a \\ a^{-1}(aa) &= a^{-1}a \\ (a^{-1}a)a &= e \\ ea &= e \\ a &= e \end{aligned}$$

$\therefore$ e is the only idempotent element in G.