Groups

Def. A **group** $(G,*)$ is a set G, and a binary operation $*$, such that the following axioms hold:

0) G is closed under $*$

1) For all $a, b, c \in G$ we have
$(a * b) * c = a * (b * c)$ i.e. $*$ is associative

2) There is an element $e \in G$ such that
for all $x \in G$, $e * x = x * e = x$.
e is called the **identity element**.

3) To each $a \in G$ there exists an element $a' \in G$
such that $a * a' = a' * a = e$.
a' is called the **inverse** of a.

Def. A group G is **abelian** if its binary operation is commutative.

Ex. Show that $(\mathbb{Z}, +)$ is a group (so are $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$).

0) $\mathbb{Z}$ is closed under $+$.
1) Addition in $\mathbb{Z}$ is associative.
2) $0 \in \mathbb{Z}$ is the identity element.
3) For any $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ is the inverse of a.

$(\mathbb{Z}, +)$ is also an abelian group because $+$ is commutative.

Ex. Show that $(\mathbb{Z}^+, +)$ is not a group.

0) $\mathbb{Z}^+$ is closed under $+$.
1) $+$ is associative.
2) There is no identity element $(0 \notin \mathbb{Z}^+)$.
3) No element of $\mathbb{Z}^+$ has an inverse $(-a \notin \mathbb{Z}^+)$ in $\mathbb{Z}^+$.

So $(\mathbb{Z}^+, +)$ fails axioms 2 and 3.

Ex. $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ are all abelian groups under multiplication.

0) Each set is closed under multiplication.
1) Multiplication is associative (and commutative).
2) 1 is the identity element.
3) If a is in any of the above sets, so is $\frac{1}{a}$, the multiplicative inverse.

Ex. Show the set F of all real valued functions on $\mathbb{R}$ is an abelian group under addition.

0) F is closed under addition.
1) Addition of functions is associative (and commutative).
2) $f(x) = 0$ is the identity element.
3) If $f(x) \in F$ then $-f(x) \in F$ and $-f(x)$ is the inverse of $f(x)$.

Ex. Show the set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices with real entries is an abelian group under addition, but not under multiplication .

0) $M_{m\times n}(\mathbb{R})$ is closed under addition.
1) Matrix addition is associative (and commutative).
2) The matrix with all entries equal to zero is the identity element.
3) If $A \in M_{m\times n}(\mathbb{R})$ then $-A \in M_{m\times n}(\mathbb{R})$ and $-A + A = 0$ is the identity element .

$M_{m\times n}(\mathbb{R})$ is not a group under multiplication because, in general, you can't multiply an $m \times n$ matrix by an $m \times n$ matrix (you can multiply $m \times n$ and $n \times q$ matrices). $M_n(\mathbb{R}) = \{nxn$ matrices with real entries$\}$ is not a group under multiplication because not every $n \times n$ matrix has an inverse.

Ex. The set of all invertible $n \times n$ matrices, $\boldsymbol{GL(n,\mathbb{R})} =$ **the general linear group of degree $\boldsymbol{n}$**, is a (non-abelian) group under matrix multiplication.

0) To show $GL(n,\mathbb{R})$ is closed under multiplication, we must show that if $A, B \in GL(n,\mathbb{R})$, i.e. A and B are invertible then AB is invertible. $A, B \in GL(n,\mathbb{R}) => A^{-1}, B^{-1}$ exist. Now notice that:
   $$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$
   $$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = B^{-1}B = I.$$
   So, $B^{-1}A^{-1}$ is the inverse of AB thus $AB \in GL(n,\mathbb{R})$.

1) Matrix multiplication is associative (but <u>not</u> commutative).

2) The matrix with 1s on the major diagonal and 0s elsewhere is the identity element.

3) By the definition of $GL(n,\mathbb{R})$, if $A \in GL(n,\mathbb{R})$ then so is A^{-1}.

Ex. Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = \frac{ab}{3}$

Show $(\mathbb{Q}^+, *)$ is an abelian group.

0) if $a, b \in \mathbb{Q}^+$ then $a * b = \frac{ab}{3} \in \mathbb{Q}^+$, so $\mathbb{Q}^+$ is closed under $*$.

1) $(a * b) * c = \frac{ab}{3} * c = \frac{abc}{9}$

$a * (b * c) = a * \frac{bc}{3} = \frac{abc}{9}$

So, $(a * b) * c = a * (b * c)$ and $*$ is associative.

$a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$ so $*$ is commutative.

2) If $a \in \mathbb{Q}^+$ and a is the identity element then:

$$a * b = b, \text{ for all } b \in \mathbb{Q}^+.$$

Thus we have:

$$a * b = \frac{ab}{3} = b \implies a = 3 \in \mathbb{Q}^+ \text{ is the identity element.}$$

Notice: $3 * a = \frac{3a}{3} = a$ and $a * 3 = \frac{a(3)}{3} = a$

3) If $a \in \mathbb{Q}^+$ and a' is the inverse of a then:

$$a * a' = 3 \text{ (the identity element).}$$

$$\frac{a(a')}{3} = 3 \implies a' = \frac{9}{a} \in \mathbb{Q}^+ .$$

$$a * \frac{9}{a} = \frac{a(9)}{3a} = 3$$

$$\frac{9}{a} * a = \frac{9a}{3a} = 3$$

So $\frac{9}{a}$ is the inverse of a.

Elementary Properties of Groups

Theorem (left and right cancellation laws): Let $(G,*)$ be a group.

1) If $a * b = a * c$ then $b = c$.
2) If $b * a = c * a$ then $b = c$.

Proof of 1: Suppose $a * b = a * c$.

Since G is a group, a has an inverse $a' \in G$.

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

By associativity we have:

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

Since, by definition $a' * a = e$ and $a * a' = e$, we have:

$$e * b = e * c, \text{ or } b = c.$$

Theorem: If $(G,*)$ is a group and $a, b \in G$ then the equations

$a * x = b$ and $y * a = b$ have unique solutions $x, y \in G$.

Proof: First we show there is at least one solution.

If we let $x = a' * b$ (where a' is the inverse of a),

Then $a * (a' * b) = (a * a') * b$ (by associativity)

$= e * b$ (since a' is the inverse of a)

$= b$.

So $x = a' * b$ is a solution to $a * x = b$.

We show this solution is unique by assuming there are two solutions and showing that they must be equal.

Let x_1, x_2 be solutions so that: $a * x_1 = b$ and $a * x_2 = b$.

Thus, $a * x_1 = a * x_2$.

But then $x_1 = x_2$ by the previous theorem (the cancellation law).

Theorem: In a group G, the identity element, e, is unique. Similarly, each element $a \in G$ has a unique inverse.

Proof: Assume e_1, e_2 are both identity elements of G, so

$$e_1 * g = g \quad \text{and} \quad e_2 * g = g \quad \text{For all } g \in G.$$

Thus we have: $e_1 * g = e_2 * g$.

By the right cancellation law $e_1 = e_2$.

So, the identity element is unique.

Assume a has two inverses, $a', a'' \in G$, then:

$$a * a' = a' * a = e \quad \text{and} \quad a * a'' = a'' * a = e.$$

So $a * a' = a * a''$

and $a' = a''$ by the left cancellation law.

So, a has a unique inverse.

Corollary: $(a * b)' = b' * a'$.

Proof: $(a * b) * (b' * a') = a * (b * b') * a'$

$$= a * e * a'$$

$$= a * a'$$

$$= e.$$

Similarly, we get $(b' * a') * (a * b) = e$.

How many different groups can there be with just two elements?

Let $G = \{e, a\}$ with the following multiplication table:

*	e	a
e	e	a
a	a	

Since G is a group $a * a = e$ or a.

But a must also have an inverse element, so $a * a = e$, and there is only one group with two elements.

*	e	a
e	e	a
a	a	e

It's easy to check that $*$ is also associative by using this table.

If we let $G = \{0,1\}$, i.e. $e = 0, a = 1$, and $*$ be addition modulo 2, we can see that G is essentially $\mathbb{Z}_2$ with modulo 2 addition.

Now, suppose G is a group with 3 elements, $G = \{e, a, b\}$

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

To fill out the rest of the table we need: $a * a,\ b * b,\ a * b,\ \text{and}\ b * a$.

$a * b$ must equal e, otherwise either a or b would equal e.

(e.g. $a * b = a$ implies $b = e$), which it can't.

Similarly, $b * a = e$. So a, b are inverses of each other.

Now $a * a = b$ since $a * a = a$ implies $a = e$, and $a * a = e$

implies a is its own inverse, but we just saw b is the unique inverse of a.

Similarly, $b * b = a$.

So we have:

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

If we let $G = \{0, 1, 2\}$ i.e. $e = 0,\ a = 1,\ b = 2$ and $*$ be addition modulo 3, we see that the only group with 3 elements is essentially $\mathbb{Z}_3$.