Groups: Let S be a set. S is a group if there exists a binary operation

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

satisfying

1) (associativity)

$\forall\ g, h, k \in S,$

$$\boxed{g * (h * k) = (g * h) * k}$$

2) (existence of identity)

$\exists\ e_S \in S$ such that

$\forall\ g \in S,$

$$\boxed{g * e_S = e_S * g = g}$$

3) (existence of inverses)

$\forall \ g \in S, \ \exists \ h \in S$ with

$$\boxed{h * g = g * h = e_S}$$

Abelian (commutative) Groups

We say a group $(S, *)$ is abelian if $\forall\, g, h \in S$,

$$\boxed{g * h = h * g}$$

Examples:

1) Let X be any set. Consider

$$S = \{ f : X \to X \mid f \text{ is bijective} \}.$$

With the binary operation of function composition (denoted by "$\circ$"), S becomes a group.

Check that S is a group

1) Is "$\circ$" a binary operation? That is, if f and g are bijections, is $f \circ g$ a bijection?

a) Surjectivity:

Range of g = range of $f = X$,

so $(f \circ g)(x) = f(g(x))$
$= f(X) = X$ ✓

b) <u>injectivity</u>

let $s, t \in X$

and suppose

$(f \circ g)(s) = (f \circ g)(t)$.

Then $f(g(s)) = f(g(t))$.

f injective $\Rightarrow$ $g(s) = g(t)$.

Then g injective $=$ $s = t$. ✓

2) Associativity

automatic since function composition is associative.

3) Identity

$e_S(t) = t$. Check:

if $f \in S$,

$$(f \circ e_S)(t) = f(e_S(t))$$
$$= f(t)$$

$(e_S \circ f)(t)$

$= e_S(f(t)) = f(t)$ ✓

4) <u>Inverses</u>

Given $f \in S$, we know f is bijective. Therefore, for all $t \in X$, $\exists$ (by surjectivity) a unique (by injectivity) $y \in X$ with

$$f(y) = t.$$

Define $g: X \to X$ by

$g(t) = y \;\; \forall\, t \in X.$

g is a bijection since f is, and

for all $t \in X$,

$$(f \circ g)(t) = f(g(t))$$
$$= f(y)$$
$$= t = e_S(t)$$

$\forall\, y \in X,$

$(g \circ f)(y)$

$= g(f(y))$

$= g(t)$

$= y = e_S(y).$

Therefore,

$f \circ g = g \circ f = e_S$ ✓

We usually denote $S = \mathrm{Sym}(X)$, the symmetries of X. When $|X| > 2$, then $\mathrm{Sym}(X)$ is not abelian. When $|X| = n$, we usually write S_n for $\mathrm{Sym}(X)$.

If we let

$S = \mathbb{Z}$ with "+"

as the binary, then

S is an abelian

group.

Identity = 0

(Inverse of n) = $-n$

3) Contraposition

The contrapositive of a statement (If P, then Q) is the statement (If not Q, then not P).

The truth valuc of a statement and its contrapositive are identical.

Proposition If G is a group, then the identity element is unique.

proof: Take the contrapositive and prove it:

"If the identity element either does not exist or is not unique, then G is not a group."

If the identity element does not exist, then G cannot be a group.

If there is more than one identity, there are at least two, e_1 and e_2.

We'll show G is not associative.

If G has no binary operation, then we don't even speak of an identity,

so let "$*$" be the binary operation.

$$e_1 * (e_2 * e_1)$$

$= e_1 * e_2$ (since e_1 is an identity

$= e_2$ (same reasoning)

$(e_1 * e_2) * e_1$

$= e_1 * e_2$ (since e_1 is an identity)

$= e_1$ (Since e_2 is an identity).

As $e_1 \neq e_2$,

$(e_1 * e_2) * e_1 \neq e_1 * (e_2 * e_1)$,

so G is not a group (fails associativity). $\square$

Fields A **field** is a set $\mathbb{F}$ endowed with two binary operations, "$+$" and "$\cdot$" such that

1) $(\mathbb{F}, +)$ is an abelian group

2) $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$

is an abelian group,

where $0_{\mathbb{F}}$ is the

identity element for

$(\mathbb{F}, +)$.

3) Distributivity:

$\forall\ g, h, k \in \mathbb{F},$

$$g \cdot (h+k) = g \cdot h + g \cdot k$$

Notation for multiplicative identity: $1_{\mathbb{F}}$

Examples: $\mathbb{Q}$ or $\mathbb{R}$

are fields with the usual addition and multiplication operations.

$\mathbb{C} = \{x+iy \mid x, y \in \mathbb{R}\}$

is a field with,

for $x, y, z, w \in \mathbb{R}$,

$$(x+iy)+(z+iw)$$
$$= (x+z)+i(y+w)$$

$$(x+iy)\cdot(z+iw)$$
$$=(xz-yw)+i(yz+xw).$$

$\mathbb{Z}_p$ is a field for p a prime number.

4) Proof by Exhaustion (case analysis)

Divide the proof into many cases, prove each case individually.

Theorem (triangle inequality)

If x, y, and z are in $\mathbb{R}$,

$$|x-y| \leq |x-z| + |z-y|.$$

Proof: Letting $a = x - z$

and $b = z - y$,

$$a + b = x - y.$$

We reduce to showing

$$|a+b| \leq |a|+|b|$$

$$\forall\ a,b \in \mathbb{R}.$$

Square both sides to obtain the inequality

$$(a+b)^2 \leq (|a|+|b|)^2,$$

which becomes

$$\cancel{a^2} + \cancel{2}ab + \cancel{b^2} \leq \cancel{a^2} + \cancel{2}|a||b| + \cancel{b^2}.$$

Via cancellation, we reduce to showing

$$ab \le |a| \cdot |b|.$$

Case 1: $a, b \ge 0$.

Then $|a| = a$, $|b| = b$,

so $ab = |a||b|$.

Case 2: $a \ge 0$, $b < 0$.

Then $ab \le 0 \le |a||b|$

Case 3: $a < 0, b \geq 0$

same as Case 2

Case 4: $a < 0, b < 0$

$$a \cdot b = |a||b| \qquad \square$$