Group Theory
2nd class

Recall: A monoid M is a set with binary operation $M \times M \xrightarrow{*} M$ which is associative and has an identity, e.

$a*e = e*a = a$ $\forall a \in M$

Notation: $\mathcal{M} = (M, *, e)$

eg: • $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \ldots$ with $* = +$ or $\cdot$
$\qquad e=0 \quad e=1$

• $\mathrm{Fun}(S)$, $\mathrm{Sym}(S)$, $\mathrm{Mat}_{n\times n}(\mathbb{R})$, $GL_n(\mathbb{R})$

Prop There is a unique identity $e \in M$.

Proof Suppose e' is another identity. Then

$$e' \underset{\substack{\uparrow \\ \text{since } e \text{ is identity}}}{=} e'*e \underset{\substack{\uparrow \\ \text{since } e' \text{ is identity}}}{=} e \qquad \boxed{\text{ok}}$$

$\boxed{\text{Groups}}$

Def A group is a monoid G such that every element in G has an inverse, i.e.,

$$\left[\begin{array}{l} \forall a \in G, \ \exists b \in G \text{ such that} \\ \qquad a*b = b*a = e \end{array}\right]$$

Eg • $G = (\mathbb{Z}, +, 0)$ $\qquad a + (-a) = (-a) + a = 0$

• $M = \mathrm{Mat}_{2\times 2}(\mathbb{R})$ $\qquad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\qquad B = A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

check: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & -1+1 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

in general: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible iff $\det A \neq 0$, i.e. $ad - bc \neq 0$

in which case $A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ ✓

The set $(M, \cdot, I_2)$ is a monoid, but not a group, since for instance

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{or} \quad A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

are not invertible. But

$$G = GL_2(\mathbb{R}) = \{ A : A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ ad - bc \neq 0 \}$$

is a group

Terminology: GL = general linear group

Prop Every element in G has a unique inverse.

Proof Let $a \in G$, with inverse b, i.e.

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

Suppose b' is another inverse, i.e.,

$$a * b' = \boxed{b' * a = e}$$

Then

$$b' \underset{\substack{\uparrow \\ e \text{ identity} \\ \text{of } G}}{=} b' * e \underset{\substack{\uparrow \\ b \text{ inverse} \\ \text{of } a}}{=} b' * (a * b) \underset{\substack{\uparrow \\ \text{associativity}}}{=} (b' * a) * b$$

$$\underset{\substack{b' \text{ inverse} \\ \text{of } a}}{=} e * b \underset{\substack{\uparrow \\ e \text{ identity} \\ \text{of } G}}{=} b \quad \blacksquare$$

Recap now the def. of a group:

Notation We will write the inverse of $a \in G$ as a^{-1}. That is: $a * a^{-1} = a^{-1} * a = e$

$\underline{\underline{\text{Def}}}$ A ~~group~~ $(G, *, e)$ is a set G w/ binary op $*: G \times G \to G$, identity e, such that

(1) [Associativity] $a*(b*c) = (a*b)*c \quad \forall a,b,c \in G$

(2) [Identity] $a*e = e*a = a \quad \forall a \in G$

(3) [Inverses] $\forall a \in G, \exists a^{-1} \in G$ st $a*a^{-1} = a^{-1}*a = e$

<u>Examples</u> / <u>Non-examples</u>

(1) $(\mathbb{Z}, \cdot, e=1)$ is a monoid but not a group!
$\left(2^{-1} = \frac{1}{2} \notin \mathbb{Z}\right.$, 0^{-1} does not exist, etc$\left.\right)$

(2) $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$ $\qquad (\mathbb{R}^{\times}, \cdot, e=1)$ is a group

$\forall a \in \mathbb{R}^{\times} \quad a^{-1} = \frac{1}{a} \in \mathbb{R}^{\times}$

(3) $GL_n(\mathbb{R})$ is a group $\qquad$ [note: $GL_1(\mathbb{R}) = \mathbb{R}^{\times}$]
$\qquad [a] \longleftrightarrow a$

$GL_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) : \det A \neq 0\}$

(4) $(\text{Fun}(S), \circ, \text{id}_S)$ is a monoid but not a group (in general)

eg: $S = \{1,2\}$ $\quad f: S \to S$, $f(1) = f(2) = 1$
has no inverse! (neither inj nor surj)

$(\text{Sym}(S), \circ, \text{id}_S)$ is a group

eg: $S = \{1, 2, \dots, n\}$, $S_n := \text{Sym}(S)$ symmetric group of all permutations of $1, \dots, n$

The size of S_n is $n!$

eg: $(n=2)$ $\quad S_2 = \left\{ \underset{e}{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}, \underset{\sigma}{\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}} \right\} \qquad |S_2| = 2! = 2$

Prop (Cancellation law for groups)
In a group G, if $a*b = a*c$, then $b = c$.

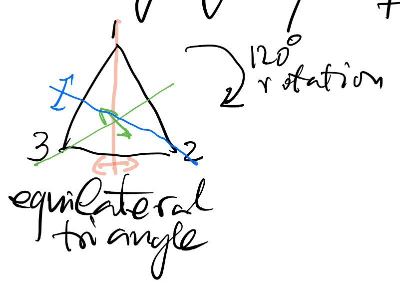
Proof
$$a*b = a*c \xrightarrow[(3)]{} a^{-1}*(a*b) = a^{-1}*(a*c)$$
$$\xrightarrow[(1)]{} (a^{-1}*a)*b = (a^{-1}*a)*c$$
$$\xrightarrow[(3)]{} e*b = e*c$$
$$\xrightarrow[(2)]{} b = c$$
$\boxtimes$

Rem Not true in general for monoids.
$M = M_{2\times2}(\mathbb{R})$ $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ $C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Then: $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ $AC = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, but $B \neq C$

Other groups in Math/Physics/Chemistry/etc

- Groups of Matrices
  - $GL_n(\mathbb{R})$
  - $SL_n(\mathbb{R}) = \{A : \det A = 1\}$
  - $O_n = \{A : AA^T = A^TA = I_n\}$
- Symmetry groups of polygons, polyhedra, etc

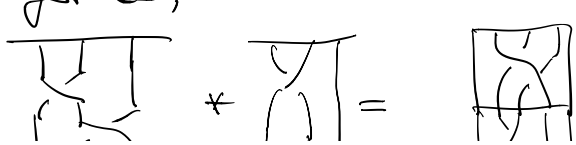


$$\longleftrightarrow S_3 = \left\{ \begin{array}{l} e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \rho_2 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{array} \right.$$

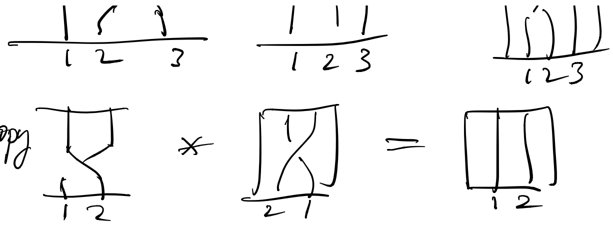
$|S_3| = 3! = 6$

Symmetries of crystals, etc

- Braid groups



$B_n = \{\text{braids on } n \text{ strings}\}/\text{isotopy}$



- **Fundamental groups** in Topology

Question Can you understand the braid group B_n as a group of matrices?

Review of basic number theory

(Divisors, Division algorithm, primes, gcd, lcm)

Axiom $\forall A \subseteq \mathbb{N}$, $\exists a \in A$ s.t. $a \leq b$, for all $a \in A$

(every subset of $\mathbb{N}$ has a smallest element)

equivalent to: every subset of $\mathbb{Z}$ which is bounded below has a smallest element.

equivalent to: every subset of $\mathbb{Z}$ which is bounded above has a largest element.

Thm (Euclidean division algorithm)

$\forall a, b \in \mathbb{Z}$ with $b > 0$, there are unique $q \in \mathbb{Z}$ (quotient) and $r \in \mathbb{Z}$ (remainder) such that $\boxed{a = bq + r, \text{ with } 0 \leq r < b}$

Thm Let $I \subseteq \mathbb{Z}$ be a set closed under addition and subtraction. Then either

- $I = \{0\}$, or
- $I = b \cdot \mathbb{Z}$ for some $b > 0$

where $b\mathbb{Z} := \{\dots, -2b, -b, 0, b, 2b, \dots\}$

proof later or in notes

Def Let a, b integers. We say that
a divides b (written $a \mid b$)
if $b = an$, for some $n \in \mathbb{Z}$.
(We also say b is a multiple of a)

Def Let $a, b \in \mathbb{Z}$, not both 0. We say that
$d \in \mathbb{Z}$, $d > 0$ is a gcd (greatest common divisor) of a and b if:

(i) $d \mid a$ and $d \mid b$

(ii) $c \mid a$ and $c \mid b \implies c \mid d$

Lemma Any two gcd's of a and b are equal.
Therefore, we can talk about __the__ gcd of a & b, and write it as

$$(a, b) = \gcd(a, b)$$

Proof Suppose d' is another gcd for a & b.
Then, by (i), (ii) for d & d':

$$d \mid d' \quad \text{and} \quad d' \mid d$$

[since $d \mid a$ & $d \mid b \implies d \mid d'$ (by (i) for d, (ii) for d')

$d'|a$ & $d'|b \Longrightarrow d|d$ (by (ii) for d)

Hence $d' = d \cdot n = (d' \cdot m) \cdot n = d'mn$

$\Longrightarrow 1 = mn \Longrightarrow m = n = 1$
or $m = n = -1$

Since d & $d' > 0$, we must have $m = n = 1$

$\therefore d = d'$ $\boxtimes$

---

eg: $\gcd(8, 6) = 2$

$\gcd(15, 9) = 3$

$\gcd(36, 24) = 12$

$\left(36 = 3^2 \cdot 2^2 \qquad 24 = 2^3 \cdot 3 \right.$

$\left. \gcd(36, 24) = 2^2 \cdot 3 = 12 \right)$