Groups

G set w/ a binary operation $*$

Definition: An identity for G is an element $e \in G$ satisfying $x * e = e * x = x$ for all $x \in G$.

Prop: If e and $\tilde{e}$ are two identities for G, then $e = \tilde{e}$.

Proof:
$$= \begin{cases} e * \tilde{e} = \tilde{e} & \text{because } e \text{ is an identity} \\ e * \tilde{e} = e & \text{because } \tilde{e} \text{ is an identity} \end{cases}$$

Hence $e = \tilde{e}$ $\square$

Remark: It's important that both $x * e = x$ and $e * x = x$

Assume G has an identity e.

Definition: An inverse of an element $a \in G$ is an element $b \in G$ satisfying $a * b = b * a = e$. $\boxed{\text{Book } a'}$

Notation: the inverse of a is denoted by a^{-1}

Proposition: Inverses, if they exist, are unique! as long as $*$ is associative

Proof: S'pose $b, c \in G$ are inverses of $a \in G$.
Then $a * b = b * a = e$ and $a * c = c * a = e$.

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

$\square$

Definition: A semigroup is a set G with an associative binary relation $*$.
A monoid is a semigroup with an identity e.
A group is a monoid with inverses.

Groups $\subseteq$ Monoids $\subseteq$ Semigroups

Def: A group is a set G with a binary relation $*$ satisfying the following three properties

Semigroup{ (1) $*$ is associative

(2) there is an identity $e \in G$ } monoid

(3) every $a \in G$ has an inverse a^{-1}

Ex: The set

$$S_n = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\} \mid \sigma \text{ is a bijection}\}$$

is a group with binary operation given by composition

How we write these elements is flexible

This is the <u>symmetric group</u> on $\{1,\dots,n\}$.

Ex: The set $\mathbb{Z}_n = \{0,1,\dots,n-1\}$ with binary operation $+_n$ is a group. Abelian!

Def: A group G whose binary operation $*$ is commutative is called <u>abelian</u>.

R ring $R^\times$ = units

Ex: The set $\mathbb{Q}^\times = \{r \mid r \text{ is a nonzero rational } \#\}$ is a group under multiplication Abelian

Ex: The set General Linear Group

$$GL_n(\mathbb{R}) = \{A \mid A \text{ is an invertible } n\times n \text{ real matrix}\}$$

is a group with matrix multiplication.

Subgroups: G group, binary operation $*$, identity e

Def: A <u>subgroup</u> of G is a subset $H \subseteq G$ which is also a group under $*$.

In other words $H \subseteq G$ is a <u>subgroup</u> iff
(1) $e \in H$
(2) If $a, b \in H$ then $a * b \in H$
(3) If $a \in H$ then $a^{-1} \in H$

<u>Notation</u>: $H \leq G$ means H is a subgroup of G

Two obvious subgroups of G:
- G improper subgroup any other is called proper
- $\{e\}$ trivial group any other is called nontrivial

<u>Ex</u>: $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$
Special linear group.

<u>Ex</u>: $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$

<u>Theorem</u>: $\emptyset \neq H \subseteq G$ is a subgroup iff
- $a * b \in H$ for all $a, b \in H$
- $a^{-1} \in H$ for all $a \in H$

<u>Proof</u>: Choose $a \in H$. Then $a^{-1} \in H$
so $a * a^{-1} \in H$. Since $a * a^{-1} = e$, we get $e \in H$ $\square$

<u>Theorem</u>: $\emptyset \neq H \subseteq G$ is a subgroup iff
- $a * b^{-1} \in H$ for all $a, b \in H$.

<u>Proof</u>:
Choose $a \in H$. Know $a * a^{-1} \in H \Rightarrow e \in H$
Thus $e * a^{-1} \in H \Rightarrow a^{-1} \in H$.

S'pose $a, b \in H$. Then $b^{-1} \in H$ so $a * (b^{-1})^{-1} \in H$

Use fact that $(b^{-1})^{-1} = b$. So $a * b \in H$ $\square$

Cyclic Groups

G group, binary operation $*$, identity e.

Proposition: Let $a \in G$. The set
$$\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$$
is a subgroup of G

Proof:

NTS given $x, y \in \langle a \rangle$ that $xy^{-1} \in \langle a \rangle$.

$x = a^m$, $y = a^n$ so $y^{-1} = a^{-n}$ and

$x * y^{-1} = a^m * a^{-n} = a^{m-n} \in \langle a \rangle$. $\square$

Here $a^k = \underbrace{a * a * a * a * \ldots * a}_{k \text{ times}}$

$a^{-k} = a^{-1} * a^{-1} * a^{-1} * \ldots * a^{-1}$

Definition: $\langle a \rangle$ is called the <u>cyclic subgroup generated by a</u>. If $G = \langle a \rangle$ for some a, then G is called <u>cyclic</u>.

Ex: $\mathbb{Z}_n = \langle 1 \rangle$ is cyclic.

Ex: $\mathbb{Z}$ with binary operation $+$ is cyclic.

$$\mathbb{Z} = \langle 1 \rangle = \{ 1, 1*1=2, 1*1*1=3, -1, -2, -3, \ldots \}$$

Theorem: If G is cyclic, then either
(1) $|G|$ is infinite and isomorphic to $\mathbb{Z}$
(2) $|G| < \infty$ and isomorphic to $\mathbb{Z}_n$ for $n = |G|$.

Note: If G, H groups, $|G| = |H| \not\Rightarrow G, H$ isomorphic

Ex: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic
↑ Klein 4-group.

Ex: $GL_2(\mathbb{R}) = \{2\times 2 \text{ invertible matrices}\}$

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

isomorphic to $\mathbb{Z}_4$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \longmapsto 1$ $\qquad$ $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \longmapsto 3$

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \longmapsto 2$ $\qquad$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longmapsto 0$

\mapsto

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^k \longmapsto k$$

$\mathbb{Z}_n = \langle 1 \rangle$

$$a^k = \overbrace{a * a * \dots * a}^{k \text{ times}}$$

$$1^k = k \cdot 1 = k$$

$$1^0 = 0 \cdot 1 = 0$$