Algebra. Lec 1. Basic notion. , Symmetry group.

Monoids.

- S. set.

  $S \times S \to S$. a law of composition.

  $(x.y) \mapsto xy$

- $(xy)z = x(yz)$ associative.

- $e \in S$. is called. a unit element. if $xe = x = ex$. $\forall x \in S$
  (identity)

Def.
A monoid is a set G with a law of composition. associative. and having. a unit element.

- G is commutative (abelian). if $xy = yx$. $\forall x, y \in G$

Def.
A group. G is a monoid. s.t. $\forall x \in G$ $\exists y \in G$. $xy = e = yx$.

Prop. G: group.

① . The unit element e is unique

② $\forall x \in G$. x^{-1} unique

③ $(x^{-1})^{-1} = x$. $\forall x \in G$

④. $(xy)^{-1} = y^{-1}x^{-1}$

⑤. $\forall x_1, \ldots, x_n \in G$. $x_1 x_2 \cdots x_n$ is indep of how they are bracketed

Ex 1. pf

Eg.1. G. group. S: set. $M(S,G)$: the set of maps from S to G.

$f.g \in M(S,G)$ $\begin{cases} (f\cdot g)(x) \triangleq f(x)g(x), \quad f^{-1}(x) \triangleq (f(x))^{-1} \\ x \in S. \end{cases}$ $\Rightarrow M(S,G)$ is a group.

unit element. $S \xrightarrow{\varphi} G$

$x \mapsto e$.

Eg.2. $(A, *)$. $(B, \diamond)$. groups. $\Rightarrow$ form a new group $A\times B$.

group $A\times B = \{(a,b) : a\in A, b\in B\}$

$(a_1, b_1)\cdot(a_2, b_2) \triangleq (a_1 * a_2, b_1 \diamond b_2)$

Eg.3. V vector space over F $(V,+)$: group.

Def. G. group. $x \in G$.

We define the order of x.

to be the smallest positive integer s.t. $x^n = 1$. $|x| = n$

Def. $G = \{g_1, \dots, g_n\}$ $|G| = n < \infty$

define multiplication. table. is a matrix M

$M_{ij} = g_i g_j$

Def. A subgroup $H \neq \emptyset$ of G is a subset of G closed under composition and taking inverses

Notation. $H \leqslant G$

Subgroup criterion.

$\emptyset \neq H \subseteq G$ if $\forall x, y \in H$. we have $xy^{-1} \in H$.

$$\Rightarrow H \leqslant G$$

$x \in H$. $xx^{-1} = e \in H$. $\quad e \cdot x^{-1} = x^{-1} \in H$.

$\forall x, y \in H$. $x(y^{-1})^{-1} = xy \in H$.

Def. G, G' groups.

$f: G \to G'$ is called a (group) homomorphism

if $f(xy) = f(x) f(y) \quad \forall x, y \in G$

$$\begin{tikzcd}
(x,y) \arrow[d] \arrow[rrr, bend left, mapsto] & G \times G \arrow[r] \arrow[d] & G' \times G' \arrow[d] & (f(x), f(y)) \arrow[d] \\
xy \arrow[rrr, bend right, mapsto] & G \arrow[r, "f"'] & G' & f(x) f(y)
\end{tikzcd}$$

Rmk. • $f(e) = f(e \cdot e) = f(e) f(e)$.

$\quad\; \|$

$\quad e' f(e)$. $\Rightarrow e' = f(e)$

• $e' = f(e) = f(x) f(x^{-1}) \Rightarrow f(x)^{-1} = f(x^{-1}) \quad \forall x \in G$.

Def. $f: G \to G'$ hom

is called an isomorphism. if f is bijective.

Prop. $f: G \to G'$ iso $\Leftrightarrow$ $\exists g: G' \to G$ hom

s.t. $f \circ g$ $g \circ f$ identity maps

Rmk. ①. $\left.\begin{array}{l} f: G \to G' \text{ hom} \\ g: G' \to G'' \text{ hom} \end{array}\right) \Rightarrow g \circ f \; G \to G''$ hom

②. $f: G \to G'$ iso $\Rightarrow f^{-1}$ iso.

③ G is a group. $\{ f: G \to G \mid f \text{ isomorphism} \} = \mathrm{Aut}(G)$ group.

automorphism

Ex 2. 验证 ③.

Def. $f: G \to G'$ group hom

$\ker(f) \triangleq \{x \in G \mid f(x) = e'\}$

$\forall\ x, y \in \ker f$ i.e. $f(x) = e' = f(y)$

$f(y^{-1}) = f(y)^{-1} = (e')^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \ker f$

$\Rightarrow \ker(f) \leq G.$

Def. $f: G \to G'$ group hom

$\mathrm{Im}(f) = \{y \in G' \mid y = f(x) \text{ for some } x \in G\}.$

Ex 3 verify $\mathrm{Im}(f) \leq G'$.

Prop A group hom, whose kernal is trivial, is injective.

Pf. $f: G \to G'$, $\ker(f) = \{e\}$.

let $x, y \in G$ and $f(x) = f(y)$. $f(xy^{-1}) = f(x) f(y)^{-1} = e'$ (with $f(y)^{-1} = f(x)^{-1}$)

$\Rightarrow xy^{-1} \in \ker(f) = e$

$\Rightarrow x = y$ $\square$

Prop. G group. $H \leq G$, $K \leq G$.

$H \cap K = \{e\}$, $HK \triangleq \{hk \mid h \in H, k \in K\} = G$

and $xy = yx$ $\forall x \in H, y \in K$.

$$\Rightarrow \begin{array}{ccc} H \times K & \xrightarrow{g} & G \\ (x, y) & \longrightarrow & xy. \end{array} \quad \text{is iso.}$$

Pf. • $g((x_1, y_1) \cdot (x_2, y_2))$

$= g((x_1 x_2, y_1 y_2))$.

$= x_1 x_2 y_1 y_2$.

$= (x_1 y_1)(x_2 y_2)$

$= g((x_1, y_1))\, g((x_2, y_2))$. $\Rightarrow g$. group hom

• g. surjective. for $HK = G$

• g. injective. for $\ker(g) = \{(e, e)\}$.

HW 1. [L]. Chap I. ex 1. ex 2.

[DF]. Sec 1.1. 25 . Sec 1.3 13 16. Sec 1.4 10

Symmetry group

Ω : a nonempty set.

S_Ω : the set of all bijections from Ω to Ω.

$\Rightarrow S_\Omega$: a group under composition

$\Omega = \{1, 2, \cdots, n\}$.

$S_\Omega = S_n$. $|S_n| = n!$

cycle decomposition.

a m-cycle. $(a_1\ a_2 \cdots a_m)$. $a_i \to a_{i+1}$. $i = 1, \cdots, m-1$.

$a_m \to a_1$

For each $\sigma \in S_n$.

σ can be expressed as a product of k-cycles.

$\sigma = (a_1 \cdots a_{m_1})(a_{m_1+1} \cdots a_{m_2}) \cdots (a_{m_{k-1}+1} \cdots a_{m_k})$. all are disjoint

eg. $n = 13$.

$\sigma = (1\ 12\ 8\ 10\ 4)(3)(2\ 13)(5\ 11\ 7)(6\ 9)$

$\downarrow$

always omitted.

$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6)$

Computation by cycle decomposition.

$$(1\,2\,3)\cdot(1\,2)(3\,4) = (1\,3\,4)$$

$\xleftarrow{\text{compose}}$

$$\left.\begin{array}{l}(1\,3)\cdot(1\,2) = (1\,2\,3).\\[1em](1\,2)\cdot(1\,3) = (1\,3\,2)\end{array}\right\}\ \text{not commutative}$$

$$(1\,4\,3\,2) = (1\,2)\cdot(1\,3)\cdot(1\,4)$$

Rmk.
- any permutation = product of cycles.
- any cycle = a product of two cycles (transposition)

- $S_n = \langle (i\ j) \mid i \neq j \rangle$

$$\uparrow$$

$$= \langle (i\ i{+}1) \mid i = 1, \dots, n \rangle$$

$$\uparrow$$

$$= \langle (1\,2), (1\,2\,3\,\cdots\,n) \rangle$$