

Algebraic Structures :

(Group)

(Laws of Composition) .1

$$\begin{array}{ccccccc}
 E \times F & & & & G & F & E \\
 & & & & \cdot & & \\
 & & & & \cdot G & E \times F & f & G \\
 z = x \oplus y, & z = xy, & z = x * y, & (x, y, z) \in E \times F \times G & & & & \\
 \cdot * & & y & x & z & & z = f(x, y) &
 \end{array}$$

$$\begin{array}{ccccccc}
 f & & f : E \times F \rightarrow F & & E \rightarrow F = G & & \bullet \\
 & & \cdot E & & F & &
 \end{array}$$

$$\begin{array}{ccccccc}
 f & & f : E \times E \rightarrow E & & E = F = G & & \bullet \\
 & & & & & & \cdot E
 \end{array}$$

$$\mathbb{N} \quad \vdots$$

$$\cdot * \quad * \quad E$$

$$\forall (x, y) \in E^2; \quad x * y = y * x \quad ; \quad -1$$

$$\forall (x, y, z) \in E^3; (x * y) * z = x * (y * z) : \quad -2$$

$$: \quad e \in E \quad -3$$

$$\forall x \in E, x * e = e * x = x$$

$$* \quad (\quad) \quad x \in E \quad -4$$

$$. \quad (x' * x = e) x * x' = e \quad x' \in E$$

$$. x * x' = x' * x = e \quad x' \quad x \in E$$

$$* \quad . E \quad \perp \quad * \quad -5$$

$$\perp \quad (\quad)$$

$$\forall (x, y, z) \in E^3; x * (y \perp z) = (x * y) \perp (x * z)$$

$$\forall (x, y, z) \in E^3; (x \perp y) * z = (x * z) \perp (y * z)$$

$$\perp \quad *$$

$$. \perp$$

$$: \quad * \quad E$$

$$. \quad e \quad * \quad E \quad e \quad -1$$

$$. x' \in E \quad x \in E \quad -2$$

$$. \quad x' \quad *$$

(Isomorphism) .2

$$f : E \rightarrow F \quad (F, \perp) \quad (E, *)$$

$$: \quad (F, \perp) \quad (E, *) \quad f \quad .$$

$$\forall (x, y) \in E^2, f(x * y) = f(x) \perp f(y)$$

f

(Group) .3

$E \quad E$

$(G, *)$

$*$

G

:

: * -1

$$\forall (x, y, z) \in G^3; \quad x * (y * z) = (x * y) * z$$

: * -2

$$\exists e \in G, \forall x \in G; \quad x * e = e * x = x$$

:G G -3

$$\forall x \in G; \exists x^{-1} \in G; \quad x * x^{-1} = x^{-1} * x = e$$

$$(G, *) \quad (\forall (x, y) \in G^2; \quad x * y = y * x) \quad *$$

(+)

G

.0

0_G

(-x) x

$$\begin{array}{l}
 n > 0 \quad \underbrace{x + x + \dots + x}_n \quad nx \quad n \in \mathbb{Z} \quad x \in G \\
 \quad \quad \quad \cdot nx = (-n)(-x) \quad n < 0 \quad n = 0 \quad 0 \\
 \quad \quad \quad (0) \quad (\quad) \quad G \quad \bullet \\
 \quad \quad \quad \cdot x \quad \quad \quad x^{-1} \quad x \quad \cdot \\
 \quad \quad \quad \cdot \quad \quad \quad 1 \quad 1_G \\
 \cdot n < 0 \quad x^n = (x^{-1})^{-n} \quad n > 0 \quad x^n = x \cdot x \cdot \dots \cdot x \quad n \in \mathbb{Z} \quad x \in G \\
 \quad \quad \quad G \quad \quad \quad (0) \quad \bullet
 \end{array}$$

$(\mathbb{C}, \times), (\mathbb{C}, +), (\mathbb{R}^*, +), (\mathbb{R}, +), (\mathbb{Q}^*, +), (\mathbb{Q}, +), (\mathbb{Z}, +), (\{-1, 1\}, +)$

$(G, *)$ -1
-1

e, e

$$e = e * e = e$$

$x^n \quad x \quad x$ •

$$e = x * x^{-1}$$

$$\Rightarrow x^{-n} * e = x^n * (x * x^{-1})$$

$$\Rightarrow x^{-n} = (x^n * x) * x^{-1} \quad *$$

$$\Rightarrow x^n = e * x^{-1} \quad x \quad x^n$$

$$\Rightarrow x^{-n} = x^{-1}$$

: (G,.) -2

$$\forall (a, x, y) \in G^3; \begin{cases} ax = ay \Rightarrow x = y \\ xa = ya \Rightarrow x = y \end{cases}$$

:

$$an = ay$$

$$\Rightarrow a^{-1}(ax) = a^{-1}(ay)$$

: (.)

$$\Rightarrow (a^{-1}a)x = (a^{-1}a)y$$

$$\Rightarrow 1.x = 1.y$$

$$\Rightarrow x = y$$

. $x = a^{-1}.b$ $a.x = b$ $(a, b) \in G^2$ -3

:

$$\forall (x, y) \in G^2; (x, y)^{-1} = y^{-1}.x^{-1} -4$$

:

$$(x, y)^{-1}.(x, y) = 1$$

$$\Rightarrow ((x, y)^{-1}.x).y = 1 \quad (.)$$

$$[(x, y)^{-1}.x].y.y^{-1} = 1.y^{-1}$$

$$\Rightarrow [(x, y)^{-1}.x].1 = y^{-1} \Rightarrow (x, y)^{-1}.x = y^{-1}$$

$$: x^{-1}$$

$$[(x, y)^{-1}.x].x^{-1} = y^{-1}.x^{-1}$$

$$\Rightarrow (x, y)^{-1}.(x.x^{-1}) = y^{-1}.x^{-1} \quad (.)$$

$$\Rightarrow (x, y)^{-1} = y^{-1}.x^{-1}$$

$$\Rightarrow (x, y)^{-1} = y^{-1}.x^{-1}$$

: -5

$$(H, *) \quad (G, .)$$

: $G \times H$

$$\forall (x, y), (x', y') \in G \times H; (x, y)T(x', y') = (x.x', y * y')$$

$$(G \times H, T)$$

Subgroup -2

$$H \quad .H \quad H \quad (G, .)$$

:

$$\forall (x, y) \in H^2; \quad x.y \in H \quad (.) \quad H \quad -1$$

$$. \quad (H, .) \quad -2$$

$$H \quad .G \quad H \quad (G, .)$$

:

$$. e \in H \quad -1$$

$$\forall (x, y) \in H^2; \quad x.y^{-1} \in H \quad -2$$

:

$$.(\quad) \quad (H, .) \quad -I$$

$$.G \quad H \quad (2) \quad (1) \quad -II$$

$$G \quad (.)$$

$$\forall (x, y) \in H \subset G \Rightarrow x^{-1} \in G \Rightarrow x^{-1}.(x, y^{-1}) = (x^{-1}.x).y^{-1} = e.y^{-1} = y^{-1}$$

$$y^{-1} \in H \quad e.y^{-1} \in H \quad H \quad y \quad e \quad :$$

$$\forall y \in H; y^{-1} \in H$$

$$.(.) \quad H$$

$$\forall (x, y) \in H^2; y^{-1} \in H$$

$$\Rightarrow (x, y) \in H^2; y^{-1} \in H$$

$$\Rightarrow x(y^{-1})^{-1} \in H \Rightarrow xy \in H$$

$$.(\quad) (y^{-1})^{-1} = y$$

$$e \in H \quad (.) \quad (H,.)$$

$$. \quad (G,.) \quad (.) \quad H$$

$$: \quad H \subset G$$

$$. e \in H \quad -1$$

$$. (x, y) \in H^2 \quad x.y^{-1} \quad -2$$

$$. x.y^{-1} \in H : H \quad x.y^{-1} \quad -3$$

$$. G \quad (H,.) \quad -4$$

:

H

$$B(E) \quad G = \{f \in B(E); f(a) = a\} \quad a \in E \quad E$$

$$G \quad (G, \circ) \quad . E \quad E$$

:

$$\begin{array}{ccc} & & (B(E), \circ) \\ & & \cdot \\ & & \cdot II_E \\ & B(E) & (G, \circ) \\ & & : \end{array}$$

$$\forall x \in E; I_E(x) = x \Rightarrow I_E \in G$$

$$\begin{array}{ccc} & & \cdot G \\ & & \cdot f \circ g^{-1} \quad G \quad f, g \end{array}$$

$$\begin{aligned} \forall x \in E; (f \circ g^{-1})(x) &= f(g^{-1}(x)) \\ &= g^{-1}(x) \quad (g^{-1}(x) \in E) \\ &= g^{-1}(g(x)) \quad (g \in G) \\ &= (g^{-1} \circ g)(x) \\ &= I_E(x) = x \end{aligned}$$

$$\begin{array}{ccc} & B(E) & (G, \circ) \quad \cdot f \circ g^{-1} \in G \\ & & : \end{array}$$

$$\begin{array}{ccc} (B(N_n), \circ) & (S_n, \circ) & E = \mathbb{N}_n \\ & & \cdot n \end{array}$$

$$\begin{array}{ccc} AB & : G & B \quad A \quad (G, \cdot) \\ & & \cdot \{ab; (a \in A) \wedge (b \in B)\} \\ & A\{b\}, \{a\}B & Ab \quad aB \\ AA = \{ab; (a \in A) \wedge (b \in A)\} & \neq \{a^2; a \in A\} & : A \\ & \cdot \{a^{-1}; a \in A\} & A^{-1} \quad \emptyset \neq A \subset G \end{array}$$

$$n \in \mathbb{N} \quad (n\mathbb{Z}, +) \quad (\mathbb{Z}, +)$$

:

$$(\mathbb{Z}, +)$$

$$(2\mathbb{Z} \cup 3\mathbb{Z})$$

G

$.G$

X

$(G, .)$

G

G

X

$.\langle X \rangle$

X

:

$\langle X \rangle$

$.X$

: $x \neq \emptyset$

$$\langle X \rangle = \{x_1, x_2, \dots, x_n, n \in \mathbb{N}^*, \forall i \in \mathbb{N}_n; x_i \in X \cup X^{-1}\}$$

$\langle X \rangle$

$.X$

$\{x\}$

$\langle x \rangle$

$(G, .)$

x



$$. o(x) = \text{Card} \{x\}$$

x

$$. o(x) = +\infty$$

x

$\langle x \rangle$

G

$G = \langle x \rangle$

x

$(G, .)$



$.G$

x

.

.

G

$$. x^n = \underbrace{x \dots x}_{n\text{-times}}$$

$$G = \{x^n; n \in \mathbb{Z}\}$$

$(G, .)$



$.G$

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \quad (\mathbb{Z}, +)$$

:

:

$$\langle 1 \rangle = \{n \cdot 1; n \in \mathbb{Z}\} = \{(-n)(-1); n \in \mathbb{Z}\} = \langle -1 \rangle.$$

: $p \in \mathbb{Z}$

$$p = 0. 1 \in \langle 1 \rangle = \langle -1 \rangle; n = 0 \quad p = 0 \quad -1$$

$$: \quad q = -p > 0 \quad p < 0 \quad -2$$

$$P = (-1) + (-1) + \dots + (-1) = q(-1) \in \langle -1 \rangle; n = q$$

$$= (-q)(1) = p \cdot 1 \in \langle 1 \rangle$$

$$P = 1 + 1 + \dots + 1 = P \cdot 1 \in \langle 1 \rangle \quad p > 0 \quad -3$$

$$= (-p)(-1) \in \langle -1 \rangle$$

$$. \quad (\mathbb{Z}+) \quad p \in \langle -1 \rangle = \langle 1 \rangle \quad \forall p \in \mathbb{Z}$$

(Lagrange)

$$\text{Card}(H) \quad G \quad H \quad (G, \cdot) \\ \cdot \text{Card}(G)$$

:

: G

$$\forall (x, y) \in G^2, x \mathfrak{R}_H y \Leftrightarrow x \cdot y^{-1} \in H$$

:

$$: \quad H \quad 1 \in H \quad 1 \in G \quad : \quad \mathfrak{R}_H \bullet$$

$$\forall x \in G; x \cdot x^{-1} = 1 \in H \Rightarrow x \mathfrak{R}_H x$$

: \mathfrak{R}_H •

$$\forall x, y \in G, x\mathfrak{R}_H y \Rightarrow xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H$$

: $G \quad H$

$$(xy^{-1})^{-1} = y.x^{-1} \in H \Rightarrow y\mathfrak{R}_H x$$

: \mathfrak{R}_H •

$$\forall (x, y, z) \in G^3, (x, \mathfrak{R}_H z) \Rightarrow (xy^{-1} \in H) \wedge (yz^{-1} \in H)$$

$$\Rightarrow ((xy^{-1})(yz^{-1}) = xz^{-1} \in H$$

$$\Rightarrow x\mathfrak{R}_H z$$

$$. k = \text{Card}(G/\mathfrak{R}_H) \quad \mathfrak{R}_H \quad k$$

:

$$G/\mathfrak{R}_H = \{[x_1], [x_2], \dots, [x_k]\}; \quad x_1, x_2, \dots, x_k \in G$$

. G

: $x \in G$

$$[x] = \{y \in G, yx^{-1} \in H\} = \{x.h \in G; h \in H\} = x.H$$

$$\text{Card}(H) = \text{Card}[x]$$

$$\varphi: H \rightarrow [x]$$

$$: h \rightarrow x.h$$

$$\text{Card}(G) = \sum_{i=1}^k \text{card}[x_i] = \sum_{i=1}^k \text{Card}(H) = k \cdot \text{Card}(H).$$

:

$$. \mathfrak{R}_H \quad k \quad \frac{\text{Card}(G)}{\text{Card}(H)} = k \in N$$

-3

$$f \quad . \quad H \quad G \quad f \quad (G, .), (H, *)$$

:

$$\forall (x, y) \in G^2; \quad f(x.y) = f(x) * f(y)$$

$$f \quad x = y \Leftrightarrow x.y^{-1} = 1_G \quad x.y^{-1} \in \ker(f) = \{1_G\}$$

$$H \subset \text{Im}(f) \Leftrightarrow y \in \text{Im}(f) \Leftrightarrow \forall y \in H; \exists x \in G; y = f(x) \Leftrightarrow f^{-1}(y) \neq \emptyset$$

$$\text{Im}(f) = H \quad \text{Im}(f) \subset H$$

$$f^{-1}$$

$$f$$

$$f : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$$

$$x \rightarrow e^x$$

$$f$$

:

:

$$f$$

$$\forall (x, y) \in \mathbb{R}; f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \times f(y)$$

$$g : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$$

$$: y \rightarrow \ln(y)$$

$$f$$

:

$$g$$

$$\forall a, b \in \mathbb{R}_+^* \Rightarrow g(a \times b) = \ln(a \times b)$$

$$\Rightarrow g(a \times b) = \ln(a) + \ln(b)$$

$$\Rightarrow g(a \times b) = g(a) + g(b)$$

$$. f$$

$$g$$

:

$$. E$$

$$G$$

$$f : G \rightarrow E$$

$$(G, .)$$

:

$$E$$

*

$$\forall (x, y) \in E^2, x * y = f[f^{-1}(x) \cdot f^{-1}(y)]$$

$$f : (E, *) \rightarrow (G, +)$$

$$f : (\mathbb{R}, +) \rightarrow]-1, +1[$$

$$f(x) = \frac{x}{1+|x|}$$

$$1+|x| \neq 1+|y| \quad x \neq y \quad f(x) \neq f(y) \quad \frac{x}{1+|x|} \neq \frac{y}{1+|y|}$$

$$y \in]-1, +1[$$

$$x = \begin{cases} \frac{y}{1+y} \in \mathbb{R}; & -1 < y \leq 0 \\ \frac{y}{1-y} \in \mathbb{R}; & 0 \leq y < 1 \end{cases}$$

$$\Rightarrow f(x) = \begin{cases} \frac{\frac{y}{1+y}}{1+\left|\frac{y}{1+y}\right|} = \frac{\frac{y}{1+y}}{1-\frac{y}{1+y}} = y; & -1 < y \leq 0 \\ \frac{\frac{y}{1-y}}{1+\left|\frac{y}{1-y}\right|} = \frac{\frac{y}{1-y}}{1+\frac{y}{1-y}} = y; & 0 \leq y < 1 \end{cases}$$

$$y = f(x) \quad x \in \mathbb{R} \quad \forall y \in]-1, +1[$$

$$(-1, +1[, *)$$

Quotient group

$$G / H \quad (G, +)$$

$$\forall (x, y) \in G^2; x \mathfrak{R}_H y \Leftrightarrow x - y \in H \quad \mathfrak{R}_H$$

$$= \{a+h; a \in A, h \in H\}$$

$$= \{a\} = A$$

$$-A = [-a] \quad G/H \quad A \in G/H \quad \bullet$$

$$: \quad G/H \quad -A = \{-a; a \in A\}$$

$$A = \{a+h \in G; h \in H\} \quad A = [a]$$

$$-A = [-a] \quad H \quad -h \in H \quad -A = \{-a-h \in G; h \in H\}$$

$$A \dot{+} (-A) = \{a+(-a)+h; h \in H\} = \{0+h, h \in H\} = H = [0]$$

$$(-A) \dot{+} A = \{(-a)+a+h, h \in H\} = 0+H = [0]$$

$$Q: (G, \bullet) \rightarrow G/H$$

$$: a \rightarrow [a]$$

(12)

$$: \quad n \quad (n \neq 0) \quad \mathbb{Z}/n\mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

:

$$[x] = \{x + nk; k \in \mathbb{Z}\} \quad [x] \in \mathbb{Z}/n\mathbb{Z} \quad x \in \mathbb{Z}$$

$$\mathbb{Z} \quad \mathbb{Z}/n\mathbb{Z} \quad n = 0$$

$$\begin{array}{r} \mathbb{Z}/4\mathbb{Z} = \{[0],[1],[2],[3]\} \\ + \begin{array}{c} [0] \ [1] \ [2] \ [3] \\ \hline [0] \ [0] \ [1] \ [2] \ [3] \\ [1] \ [1] \ [2] \ [3] \ [0] \\ [2] \ [2] \ [3] \ [0] \ [1] \\ [3] \ [3] \ [0] \ [1] \ [2] \end{array} \quad \times \begin{array}{c} [0] \ [1] \ [2] \ [3] \\ \hline [0] \ [0] \ [0] \ [0] \ [0] \\ [1] \ [0] \ [1] \ [2] \ [3] \\ [2] \ [0] \ [2] \ [0] \ [2] \\ [3] \ [0] \ [3] \ [2] \ [1] \end{array} \end{array} \quad \mathbb{Z}/4\mathbb{Z}$$

$$\begin{aligned} [3]+[2]&=[5]=[1] & [a][b]&=[ab] & [a]+[b]&=[a+b] \\ & & & & [3][2]&=[6]=[2] \end{aligned}$$

$$\begin{aligned} [6] &= \{6+4k; k \in \mathbb{Z}\} \\ &= \{2+4+4k; k \in \mathbb{Z}\} \\ &= \{2+4(1+k); k \in \mathbb{Z}\} \\ &= \{2+4l; l=1+k \in \mathbb{Z}\} \\ &= [2] \end{aligned}$$

-4

: $x \in G$

(G, \bullet)

$$G = \langle a \rangle = \{a^k, k \in \mathbb{Z}\}$$

$$a^k = a \bullet \dots \bullet a$$

G

.

(13)

: (G, \bullet)

$$f : (\mathbb{Z}, +) \rightarrow (G, \bullet)$$

$$: k \rightarrow a^k$$

$\ker(f) = n\mathbb{Z}$ $n \in \mathbb{N}$ $(\mathbb{Z}, +)$ $\ker(f)$
 :
 . $(\mathbb{Z}, +)$ $f) \mathbb{Z}$ G $n = 0$ **-1**
 . $(\mathbb{Z}/n\mathbb{Z}, +)$ G $n > 0$ **-2**

n $Card(G) = n$ $G = \langle a \rangle$ (G, \bullet)
 : G 1_G $a^k = 1_G$ $k \in \mathbb{N}^*$
 $n = \min\{k \in \mathbb{N}^*; a^k = 1_G\}$

$\mathbb{Z}/n\mathbb{Z}$ $G = \langle a \rangle$
 :
 $f : (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (G, \bullet)$
 : $[k] \rightarrow a^k$
 :
 $n \in \mathbb{N}^*$
 $[n] = [0]$
 $a^n = 1_G$ n f

(Symmetric group) -5

(S_E) $\sigma : E \rightarrow E$ E E
 (\circ) S_E $S_E = B(E, E)$ E
 E

\mathbb{N}_n S_n $E = \mathbb{N}_n$ $Card(S_n) = n!$ σ $\sigma \in S_n$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \sigma(6) \end{pmatrix}$$

:

 $3! = 6$ \mathbb{N}_3

:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$S_3 = \{I, a, b, c, d, e, f\}$$

 I I (S_3, \circ)

$$b \circ a(1) = b(a(1)) = b(2) = 1,$$

$$b \circ a(2) = b(a(2)) = b(3) = 2,$$

$$b \circ a(3) = b(a(3)) = b(1) = 3$$

$$b \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

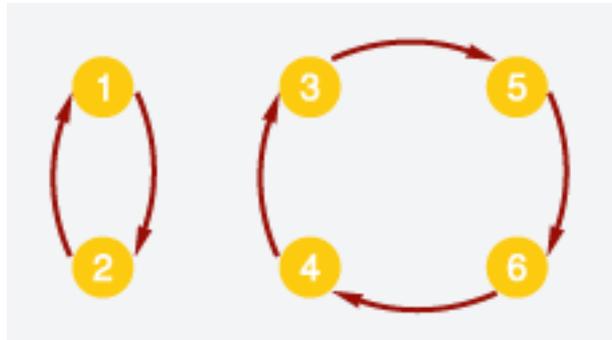
(Cayley) (14)

$x \in \mathbb{N}_n$ $\sigma \in S_n$
 $O(x) = \{\sigma^k(x); k \in \mathbb{N}\}$

$E = \{1,2,3,4,5,6\}$ $E = \mathbb{N}_6$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$$

$O(3) = O(4) = O(5) = O(6) = \{3,4,5,6\}, O(1) = O(2) = \{1,2\}$:



$O(x) = O(y) \quad y \in O(x)$

(\quad)

$x \in \mathbb{N}_n$

$\sigma \in S_n$

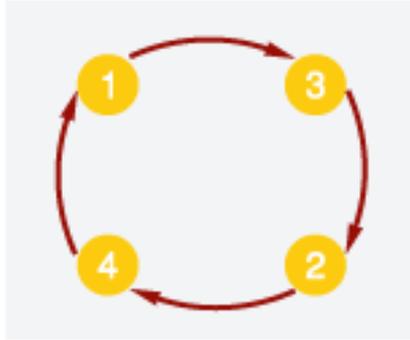
$O(x) = \mathbb{N}_n$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

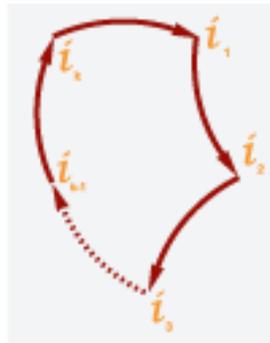
$\mathbb{N}_4 = \{1,2,3,4\}$

$O(1) = \{1, 3, 4, 2\} = \mathbb{N}_n$

:



$$\begin{aligned}
 & 2 \leq k & \sigma & \in S_n \\
 & : & k \in \mathbb{N}_n & i_1 i_2, \dots, i_k \\
 & & & \forall j \in \mathbb{N}_n \setminus \{i_1, i_2, \dots, i_k\}; \sigma(j) = j \bullet
 \end{aligned}$$



$$\begin{aligned}
 \forall p \in \mathbb{N}_{k-1}; \quad \sigma(i_p) &= i_{p+1} \bullet \\
 \sigma(i_k) &= i_1 \bullet
 \end{aligned}$$

$$\{i_1, i_2, \dots, i_k\} \quad . C = (i_1, i_2, \dots, i_k)$$

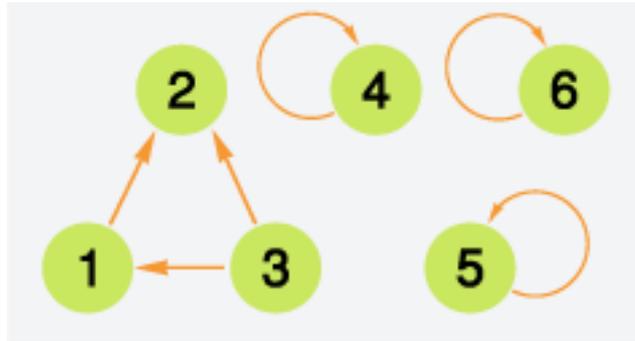
.C

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} \quad E = \mathbb{N}_6 = \{1, 2, 3, 4, 5, 6\}$$

{1,2,3}

(3)

$$C = \{1 \ 2 \ 3\}$$



$$\mathbb{N}_n \quad \tau_{a,b} \quad (2) \quad S_n$$

$$.b,a \quad \tau_{a,b} \quad (a,b) \quad \tau$$

$$\mathbb{N}_n \quad I \quad \tau \circ \tau = I \quad \tau$$

$$.S_n$$

$$:$$

$$\tau = \begin{pmatrix} 1, 2, \dots, a, \dots, b, \dots, n \\ 1, 2, \dots, b, \dots, a, \dots, n \end{pmatrix}$$

$$\tau \circ \tau = \begin{pmatrix} 1, 2, \dots, a, \dots, b, \dots, n \\ 1, 2, \dots, a, \dots, b, \dots, n \end{pmatrix} = I$$

(15)

$$\sigma \in S_n \setminus \{I\}$$

:

$k < n$

$$\sigma \in S_n \setminus \{I\}$$

$$\sigma_i, i = 1, \dots, k$$

k

$$\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k$$

σ

:

$$\sigma \in S_{10}$$

:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 2 & 3 & 4 & 1 & 6 & 10 & 7 & 8 \end{pmatrix}$$

1

.

1

$$2 \notin C_1 \quad C_1 = (1, \sigma(1), \sigma^2(1), \sigma^3(1)) = (1, 9, 7, 6)$$

$$C_3 = (8, \sigma(8)) = (8, 10) \quad C_2 = (2, \sigma(2), \sigma^2(2), \sigma^3(2)) = (2, 5, 4, 3)$$

:

$$\sigma = C_1 \circ C_2 \circ C_3$$

$$= (1 \ 9 \ 7 \ 6)(2 \ 5 \ 4 \ 3)(8 \ 10).$$

:

1

$$C = \{x \in G; \forall g \in G; g.x = x.g\} \quad (G, .)$$

$$(G, .) \quad C$$

:

$$\forall g \in G; g.e_G = e_G.g \quad e_G \in C \quad e_G \quad \bullet$$

$$.xy^{-1} \in C \quad (.) \quad y \quad y^{-1} \quad .C^2 \ni (x, y) \quad \bullet$$

$$(\forall g \in G) \wedge (\forall x \in C) \Rightarrow gx = xg \Rightarrow g = xgx^{-1}$$

$$\Rightarrow x^{-1}g = x^{-1}xgx^{-1} = gx^{-1} \Rightarrow gx^{-1} = x^{-1}g \Rightarrow x^{-1} \in C$$

$$\forall (x, y) \in C^2, (gx)y^{-1} = (xg)y^{-1}$$

$$\Rightarrow g(x.y^{-1}) = (gx)y^{-1} \quad gx = xg \Leftarrow x \in C$$

$$\Rightarrow g(xy^{-1}) = g(xy^{-1}) \quad (.)$$

$$G \quad C \quad (x, y) \in C^2 \quad xy^{-1} \in C$$

.G

2

$$: \quad (*) \quad G \neq \emptyset$$

$$. \quad (*) \quad .1$$

$$\exists e \in G, \forall x \in G; x * e = x \quad .2$$

$$\forall x \in G, \exists x' \in G; x * x' = e \quad .3$$

$$. \quad (G, *)$$

:

$$. \quad (*) \quad \bullet$$

$$x' \in G \quad . \quad x * x' = e \quad . (*) \quad x \quad x' \quad \bullet$$

$$: \quad x' * x'' = e \quad x'' \in G$$

$$x' * (x * x') = x' * e = x'$$

$$\Rightarrow x' * [(x * x') * x''] = x' * x'' = e$$

$$\Rightarrow x' * [x * (x' * x'')] = e \quad * \text{ تجميعي}$$

$$\Rightarrow x' * (x * e) = e$$

$$\Rightarrow (x' * x) * e = e \quad * \text{ تجميعي}$$

$$\Rightarrow x' * x = e$$

$$. e * x = x \quad . (*) \quad e \quad \bullet$$

$$: \quad x * e = x$$

$$\Rightarrow e * (x * e) = e * x$$

$$\Rightarrow (e * x) * e = (x * x') * x$$

$$\Rightarrow e * x = x * (x' * x)$$

$$\Rightarrow e * x = x * e = x$$

$$(G, *) \quad (*)$$

:3

$$: \quad G \quad H_1, H_2$$

$$\underbrace{H_1 \subset H_2 \text{ or } H_2 \subset H_1}_{(2)} \Leftrightarrow \underbrace{H_1 \cup H_2 \text{ زمرة جزئية من } G}_{(1)}$$

:

$$(2) \Rightarrow (1)$$

$$\begin{aligned} (x \in H_1) \wedge (y \in H_2) & \quad .G & H_1 \cup H_2 \\ xy^{-1} \in H_1 \cup H_2 & \quad H_1 \cup H_2 & (x \in H_1 \cup H_2) \wedge (y \in H_1 \cup H_2) \\ & & : (xy^{-1} \in H_1) \vee (xy^{-1} \in H_2) \end{aligned}$$

$$\begin{aligned} .H_2 \subset H_1 & \quad H_1 & y \in H_1 & y^{-1} \in H_1 & xy^{-1} \in H_1 \\ .H_1 \subset H_2 & \quad H_2 & x \in H_2 & & xy^{-1} \in H_2 \end{aligned}$$

:4

n

$$\mathbb{Z}/n\mathbb{Z}; n \neq 0$$

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

:

$$[x] \in \mathbb{Z}/n\mathbb{Z}$$

$$\begin{aligned} [x] &= \{y \in \mathbb{Z}; y - x \in n\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}; \exists k \in \mathbb{Z}; y - x = nk\} \\ &= \{y = x + nk; k \in \mathbb{Z}\} \\ &= \{x + nk; k \in \mathbb{Z}\} \end{aligned}$$

$.n$

$$q - p \quad 0 \leq p < q < n$$

$$. [p] \neq [q] \quad q \notin [p]$$

•

$n \quad a$

$$[a] \in \mathbb{Z}/n\mathbb{Z}$$

•

$$a \in [r] \quad a - r = qn \in n\mathbb{Z} \quad a = qn + r \quad 0 \leq r < n \quad \text{حيث } (q, r) \in \mathbb{Z} \times \mathbb{N}$$

$$r \in \{0, 1, \dots, n-1\}$$

$$[a] \in \mathbb{Z}/n\mathbb{Z}$$

$$. [a] = [r]$$

$$. [a] = [r]$$

$$[n] = [0]$$

$$\begin{aligned}
 [n] &= \{n + nk; k \in \mathbb{Z}\} \\
 &= \{nl; l = k + 1 \in \mathbb{Z}\} \\
 &= [0]
 \end{aligned}$$

:5

$$\begin{aligned}
 & \cdot S_n \quad (n-1)! \\
 & \quad \quad \quad \sigma \quad x \quad n-1 \quad x \in \mathbb{N}_n \\
 & \quad \quad \quad \quad \quad \quad n-2 \quad \sigma(x) \in \mathbb{N}_n \\
 & \quad \quad \quad n-3 \quad \sigma^2(x) \in \mathbb{N}_n \quad \cdot \mathbb{N}_n \setminus \{x, \sigma(x)\} \\
 & \sigma^{n-1}(x) \in \mathbb{N}_n \quad \mathbb{N}_n \setminus \{x, \sigma(x), \sigma^2(x)\} \\
 & \quad \quad \quad (n-1)! \quad \cdot \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \cdot S_n
 \end{aligned}$$

:6

$$\begin{aligned}
 & \cdot \quad \sigma \in S_n \quad \cdot 2 \leq n \\
 & \quad \quad \quad \sigma = \tau_1 0 \tau_2 0 \dots 0 \tau_k \\
 & \cdot (S_n \quad S_n \quad 2 \leq n \quad) \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \cdot \\
 & \quad \quad \quad \cdot \{I, \tau_{1,2}\} \quad S_2 \quad n=2 \quad -1 \\
 & : \quad \cdot S_n \quad \sigma \quad (n-1) \quad -2 \\
 & \quad \quad \quad \quad \quad \quad \quad \quad \quad \cdot \sigma(n) = n \quad \bullet
 \end{aligned}$$

$$\begin{aligned}
& \tilde{\sigma} \in S_{n-1} & \tilde{\sigma}: N_{n-1} \rightarrow N_{n-1} \\
& \tilde{\sigma} = \tilde{\tau}_1 \circ \tau_2 \circ \dots \circ \tau_k & S_{n-1} \quad \tilde{\tau}_1, \tilde{\tau}_2, \dots, \tau_k \\
& \tau_i(x) = \begin{cases} n & x = n \\ \tilde{\tau}_i(x), & x \neq n \end{cases} & S_n \quad \tau_1, \tau_2, \dots, \tau_k \\
& & \sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k \\
& & \sigma(n) = p \neq n \\
& \bar{\sigma}(n) = n & \bar{\sigma} \\
& \bar{\sigma} = \tau_{n,p} \circ \tau_1 \circ \dots \circ \tau_k & \bar{\sigma} = \tau_{n,p} \in S_n \\
& \bar{\sigma} = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k
\end{aligned}$$