

## Axioms for Group

1) Given set  $G$  and binary operation  $*$

Associative 2)  $a, b, c \in G$  then  $a * (b * c) = (a * b) * c$

Identity 3)  $\exists e \in G$  s.t.  $\forall g \in G, e * g = g * e = g$

Inverse 4)  $\forall g \in G \exists g^{-1}$  s.t.  $g * g^{-1} = g^{-1} * g = e$

Commutative 5)  $\forall a, b \in G, a * b = b * a$

$\mathbb{N}$  whole numbers  $\mathbb{N}_0$  (with zero)

$\mathbb{Z}$  integers is a group under  $(+)$  (not  $\cdot$ )

$\mathbb{Q}$  rationals group under  $+$ , and  $\setminus \{0\}$  under  $\cdot$

$\mathbb{R}$  reals

"

"

$\mathbb{C}$  complex numbers "

"

$$(a+bi)^{-1} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} \stackrel{?}{=} x+iy/i$$

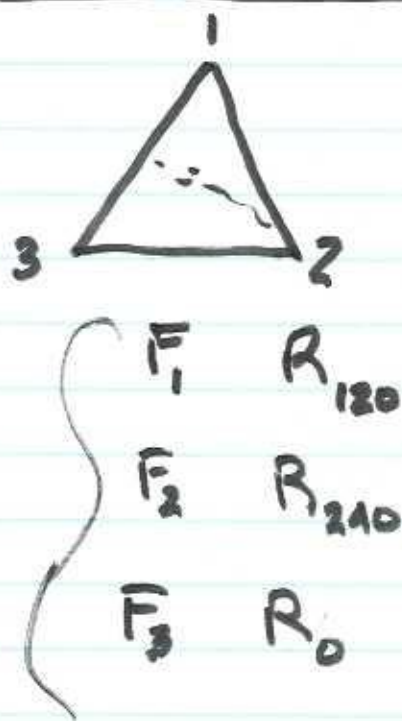
(2)

Differential Operators - not group  
under composition

$$\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \dots$$

Consider:  $\frac{\partial}{\partial x}(e^{x^2y}) \xrightarrow{\int e^{x^2y} \cdot 2x dx} \text{OK}$   
 $\int e^{x^2} dx \text{ DNE}$

---



Check list:

- 1) Associative ✓  
by functional composition
- 2)  $R_0$  is identity
- 3)  $F_1, F_2, F_3, R_0$  are  
own inverses

$$R_{120}^{-1} = R_{240} \text{ and v.v.}$$

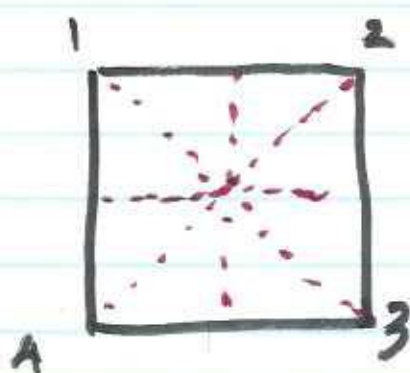
3-gon

n-gon

③

Symmetry operations on n-gons are called "dihedral" groups  $D_{2n}$

Note: the number of elements in a group is called its "order."  $|D_{2n}| = 2n$



$$D_8 = \left\{ \begin{array}{cccc} F_V & F_H & F_D & F_A \\ R_0 & R_{90} & R_{180} & R_{270} \end{array} \right\}$$

right

xoy

left

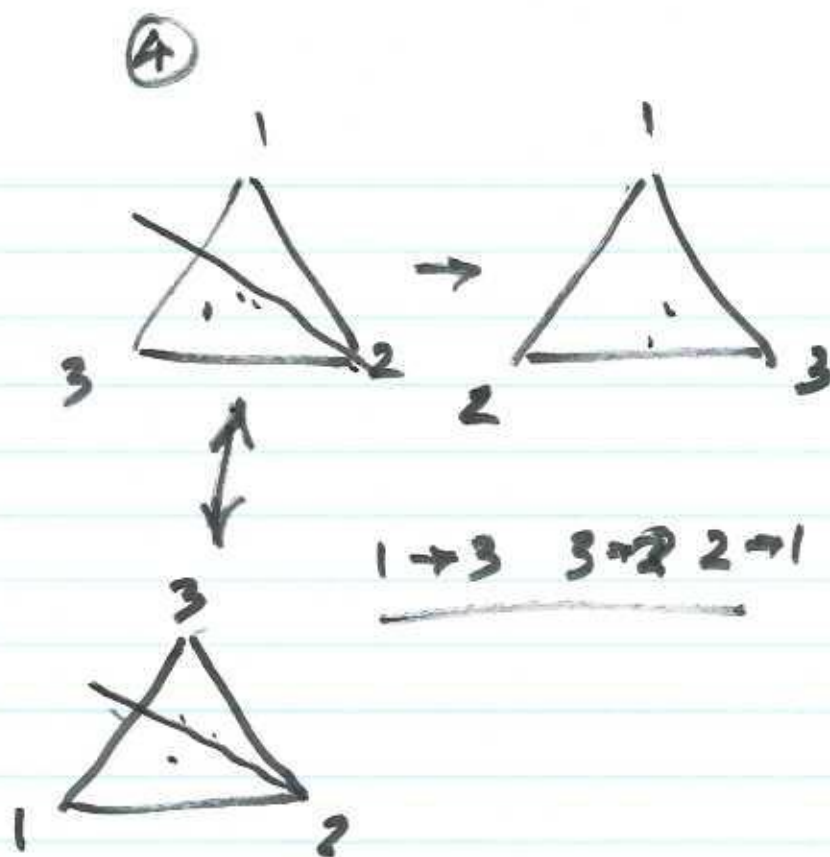
|           | $R_0$     | $R_{120}$ | $R_{240}$ | $F_1$ | $F_2$ | $F_3$ |
|-----------|-----------|-----------|-----------|-------|-------|-------|
| $R_0$     | $R_0$     | $R_{120}$ | $R_{240}$ | $F_1$ | $F_2$ | $F_3$ |
| $R_{120}$ | $R_{120}$ | $R_{240}$ | $R_0$     | $F_3$ |       |       |
| $R_{240}$ | $R_{240}$ | $R_0$     | $R_{120}$ |       |       |       |
| $F_1$     | $F_1$     |           |           |       |       |       |
| $F_2$     | $F_2$     |           |           |       |       |       |
| $F_3$     | $F_3$     |           |           |       |       |       |

Arthur Cayley

Cayley Table

$$R_{120} = \frac{1}{\omega}$$

$$R_{120} \vec{F}_1 = \vec{F}_2$$



$$R_0 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \leftarrow$$

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$$

$$R_{120} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$R_{240} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$F_1 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\vec{F}_2 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\vec{F}_3 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{array}{ccc} & 1 & 2 & 3 \\ F_1 & 1 & 3 & 2 \\ R_{120} & 2 & 1 & 3 \end{array} \leftarrow$$

$$R_{120} \circ F_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\vec{F}_3$$

(5)

$$F_1 \circ R_{120} = ?$$

$$\begin{array}{cccc} & 1 & 2 & 3 & \leftarrow \\ R_{120} & & & & \\ & 2 & 3 & 1 & \\ F_1 & & & & \\ & 3 & 2 & 1 & \leftarrow \end{array}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = F_2$$

Symmetric Group  $S_n$

So 3 objects generate  $S_3$

Note  $D_6 = S_3$

$D_{2n} = S_n$  only  $n=3$

$$D_8 \neq S_4 \quad |S_4| = 4! = 24$$

$\{e, a, b, c\}$

$C_4$

|   | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

|       |       |
|-------|-------|
| $a$   | $= a$ |
| $a^2$ | $= b$ |
| $a^3$ | $= c$ |
| $a^4$ | $= e$ |

cyclic

Klein group

$V_4$

|   | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

$$\underline{e^2 = a^2 = b^2 = c^2 = e}$$

$V \sim$  vierergruppe 4-group

Table 10.1 Modular Arithmetic Operations

$x, y, u, v, k, r \in \mathbb{Z}, k \neq 0$

- 
- 1) Addition if  $x \equiv y \pmod{m}$  and  $u \equiv v \pmod{m}$  then  $x+u \equiv y+v \pmod{m}$
  - 2) Subtraction if  $x \equiv y \pmod{m}$  and  $u \equiv v \pmod{m}$  then  $x-u \equiv y-v \pmod{m}$
  - 3) Multiplication if  $x \equiv y \pmod{m}$  and  $u \equiv v \pmod{m}$  then  $xu \equiv yv \pmod{m}$
  - 4) Division if  $x \equiv y \pmod{m}$  and  $x=ku, y=kv$  then  $(x/k) \equiv (y/k) \pmod{m}$  if  $\gcd(k, m)=1$
  - 5) Powers if  $x \equiv y \pmod{m}$  then  $x^r \equiv y^r \pmod{m}$
- 

$$x \equiv y \pmod{m} \quad x^r \equiv y^r \pmod{m}$$

$$7^4 \equiv 1 \pmod{100} \text{ so } \dots 7^{1k} \equiv 1 \pmod{100}$$

$$\text{We say } x \equiv y \pmod{m} \iff x-y = km \quad \exists k \in \mathbb{Z}$$