<u>Definition 5.6</u> A <u>group</u> is a set G with operation $* : G \times G \longrightarrow G$.

(G1)

(G2)

(G3)

(G4)

We normally use multiplic. notation for $*$: xy; $e=1$; x^{-1}, x^k

Sometimes (if G is abelian, i.e. (G5) $x * y = y * x \ \forall x, y$) then we can use additive notation: $x+y$, $e=0$, $(-x)$, kx.

Examples: (1) $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ under x; $e=1$, x^{-1}

$\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ for any field $\mathbb{F}$.

(2) $(\mathbb{Z}, +)$: $e=0$, $(-x)$ (inverse of x). also $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, ..., $(\mathbb{F}, +)$

$(\mathbb{Z}, \times)$ <u>not</u> a group: (G4) fails: $2^{-1} \notin \mathbb{Z}$.

(3) $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ (the ring of integers mod n).

Then $\mathbb{Z}_n$ is a group under $+$: (G1) $\forall x, y \in \mathbb{Z}_n$ $\quad \underset{\substack{\uparrow \\ \text{mod } n}}{x+y} \in \mathbb{Z}_n$ $\quad (n-1+2 = 1 \text{ mod } n)$

(G2) ✓

(G3) $e=0$

(G4) ✓, e.g. $(-2) = n-2 \in \mathbb{Z}_n$.

Note: $(\mathbb{Z}_n, \times)$ is not a group as $0^{-1} \notin \mathbb{Z}_n$. Denote $\mathbb{Z}_n^* = \{\text{all invertible elements in } \mathbb{Z}_n\}$.

$\| $ all $m \in \mathbb{Z}_n$ s.t. m, n are coprimed

e.g. $\mathbb{Z}_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\}$

Then $\mathbb{Z}_n^*$ is group under x: $e=1$, $x^{-1} \in \mathbb{Z}_n^*$ $\forall x$ (also can use Cayley Table to check (G1) and (G4)

$\mathbb{Z}_p^* = \{1, 2, 3, 5, 7, \dots, p-1\}$

Then $\mathbb{Z}_n^*$ is group under x: $e=1$, $x^{-1} \in \mathbb{Z}_n^*$ $\forall x$ (also can use Cayley Table to check (G1) and (G4)).

$\mathbb{Z}_n^*$ is especially nice if $n=p$ prime

Then $\mathbb{Z}_p^* = \{1, 2, 3, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}$

Note: examples (1)-(3) are all abelian groups (commutative)

(4) Set $M_{n\times m}(F) = \{$all $n \times m$ matrices over field $F\}$ is abelian group under $+$: $e = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$

denote $GL_n(F) = \{$all invert $n\times n$ matrices over $F\}$

Then $GL_n(F)$ is a group under $\times$: $(AB)^{-1} = B^{-1}A^{-1}$, $e = I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ (Not abelian if $n \geq 2$)

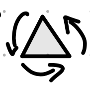
(5) The symmetric group $S_n = \{$all bijections $X \to X\}$

(G1) $f \circ g$ is a bijection if f, g are bijections $\quad X = \{1, 2, 3, \dots, n-1\}$.

(G2) Composition of maps is associative

(G3) $e = 1_X$ (identity map)

(G4) $(\text{bijection})^{-1}$ is a bijection

(6) The group $D_3 = \{$all symmetries of equilateral $\Delta\} = \{$  $=$ rot$(120°) =$ rot$(\frac{2\pi}{3})$; $e = 1 =$ rot$(0°)$;

rot$(240°) =$  $\}$ 6 elements

In general, every symmetry group of a shape X, sym(X) is a group under $\circ$:

(G1) sym 1 $\circ$ sym 2 must be a symmetry

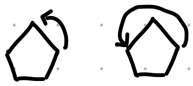
(G2) $\circ$ is associative.

(G3) $e = Id$. is a symmetry.

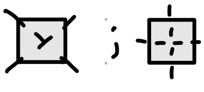
(G4) $(\text{sym})^{-1}$ is symmetric.

(7) More generally, $D_n = \{$all symmetries of a regular n-gon$\}$

has $2n$ elements: rot$(0°) = e$, rot$(\frac{2\pi}{n})$, rot$(\frac{2\pi \cdot 2}{n})$, …, rot$(\frac{2\pi(n-1)}{n})$

n rotations:  …

n reflections:  n odd

n even:  n in total so $|D_n| = 2n$.

D_n is the dihedral group of degree n

<u>Proposition 5.13:</u> Let G be a group. Then (1) The identity e is unique.

(2) The inverse x^{-1} is unique $\forall x \in G$

Proof: (1) suppose e, e' are identities in G.

then $e = e'$ and $e' = e$ by (G3) $\Rightarrow e' = e$

(2) if y and y' are inverses of x,

then $y = y \cdot e = y(x \cdot y') = (y \cdot x) y' = e \cdot y' = y'$