More Examples of Groups

Groups from Modular Arithmetic

Let $n \in \mathbb{Z}$, $n > 1$ ← "modulus"

Definition: Two integers $x, y \in \mathbb{Z}$ are congruent modulo n

written $x \equiv y \pmod{n}$

if $x - y$ is divisible by n:

$$x - y = kn \quad \text{for some } k \in \mathbb{Z}.$$

Equivalently, $x \equiv y \pmod{n}$ if x and y have the same remainder when divided by n.

Examples:

- $19 \equiv 12 \pmod{7}$ or 5 or −2 or . . .
- $29 \equiv 16 \pmod{13}$
- $-3 \equiv 7 \pmod{10}$. or 2 or 5

We can use congruence mod n to construct two "families" of groups, as follows:

Additive group

The set of remainders modulo n

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$

is a group with operation addition modulo n:

$$(x, y) \longmapsto \underbrace{x + y \pmod{n}}_{\text{add up, then take remainder mod } n}$$

Check group axioms:

- identity element 0:

$$x + 0 \pmod{n} = x \quad \forall\, x \in \mathbb{Z}_n$$

- inverses:

$$x + (n - x) \equiv \underset{\text{identity element}}{0} \pmod{n}$$

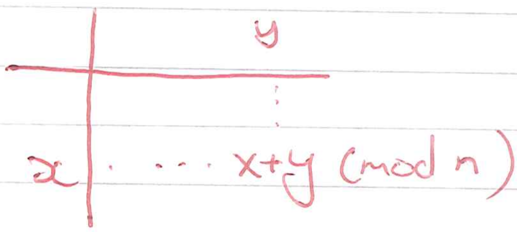
So the inverse of x is $\begin{cases} n-x & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.

- associativity: (boring!) exercise.

Example $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

"Operation table":

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



Multiplicative group

For $n = p$, a prime number, the set

$$\mathbb{Z}_p^\times := \{1, 2, \ldots, p-1\}$$

of nonzero remainders mod p is a group with the operation multiplication mod p:

$$(x, y) \longmapsto xy \pmod p$$

multiply, then take remainder mod p

Exercise: check all the group axioms.

Example: $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$

Operation table:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	y
x	$xy \pmod 5$

Identity element: $\underline{1}$

Inverses: $1^{-1} = \underline{1}$, $2^{-1} = \underline{3}$

$3^{-1} = \underline{2}$, $4^{-1} = \underline{4}$.

Groups from Geometry

Let $X \subset \mathbb{R}^n$ be any subset : e.g.

think of a plane polygon or a solid in space.

Definition: the symmetry group $\mathrm{Sym}(X)$ is the set of all maps $f : \mathbb{R}^n \to \mathbb{R}^n$ such that

- f preserves distances - "isometry"
- $f(X) = X$ - f maps X to itself.

Group operation is composition of maps :

$$(f, g) \longmapsto fg$$

where $fg : \mathbb{R}^n \to \mathbb{R}^n$ is defined by

$$(fg)(x) = f(g(x)).$$

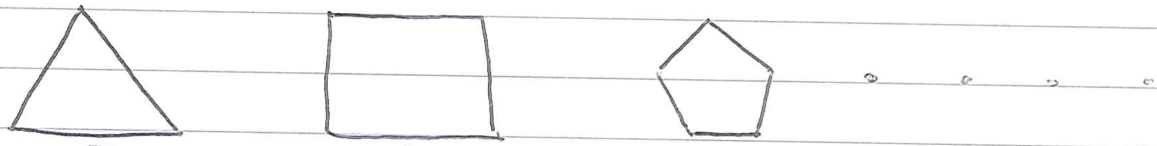
Check group axioms :

- associativity : composition of maps is associative
- identity : identity map $\mathrm{id} : \mathbb{R}^n \to \mathbb{R}^n$
  $x \longmapsto x$
- inverses : isometries are bijective, therefore invertible.

Example : Dihedral groups

$$D_n := \mathrm{Sym}(P_n)$$

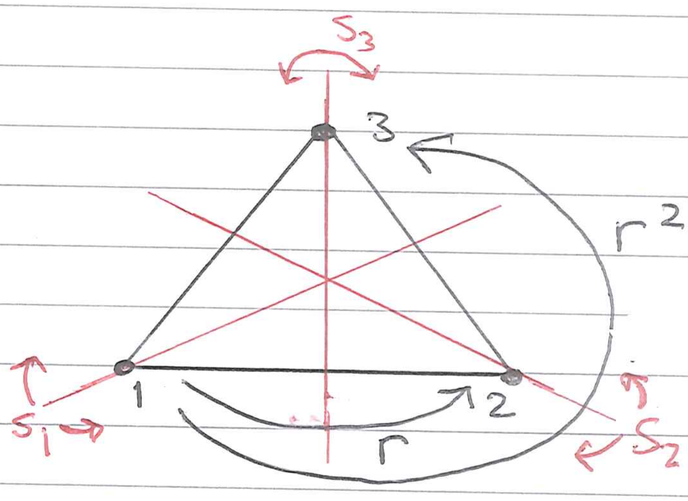
- symmetry group of regular n-gon P_n.



P_3 $\quad$ P_4 $\quad$ P_5

Example $n=3$

D_3 consits of :



- identity map e
- rotations anticlockwis by $\begin{cases} 2\pi/3 & - r \\ 4\pi/3 & - r^2 \end{cases}$
- 3 reflections s_1, s_2, s_3.

Important : Can write all elements in terms of r and $s = s_1$ since

$$\boxed{s_2 = r^2 s \quad , \quad s_3 = rs.}$$

So

$$D_3 = \{ \underbrace{e, r, r^2}_{\text{rotations}}, \underbrace{\overset{s_1}{\overset{\shortparallel}{s}}, \overset{s_3}{\overset{\shortparallel}{rs}}, \overset{s_2}{\overset{\shortparallel}{r^2 s}}}_{\text{reflections}} \}$$

<u>Note</u>: • $r^3 = e$ (three $2\pi/3$ rotations

$\iff r^2 = r^{-1}$ give 2π rotation - identity)

• $s^2 = e$ (reflecting twice

$\iff s = s^{-1}$ gives identity).

So from $s_2 = s_2^{-1}$ (since s_2 is a

we get $r^2 s = (r^2 s)^{-1}$ reflection)

$= s^{-1} (r^2)^{-1}$

$= s\,(r^{-1})^{-1} = sr.$

So we have <u>relations</u>

$$\boxed{r^3 = s^2 = e, \quad sr = r^2 s} \quad (*)$$

These determine the whole multiplication table:

Check!

	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

For example:

$$
\begin{aligned}
(rs)(r^2s) &\overset{\text{associativity}}{=} r\,(sr^2)\,s \\
&\overset{\text{assoc}}{=} r\,(sr)(rs) \\
&\overset{\text{relation 3}}{=} r\,(r^2s)(rs) \\
&\overset{\text{assoc.}}{=} r^3\,(sr)\,s \\
&\overset{\text{relation 1}}{=} (sr)\,s \\
&\overset{\text{relation 3}}{=} (r^2s)\,s \\
&\overset{\text{assoc.}}{=} r^2s^2 \\
&\overset{\text{relation 2}}{=} r^2
\end{aligned}
$$

$(rs)(sr) =$
$rs^2r =$
$rer =$
r^2

Similarly for any n, the dihedral group D_n can be defined algebraically as

$$D_n = \{ \underbrace{e, r, \dots\dots, r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, \dots, sr^{n-1}}_{\text{reflections}} \}$$

$r = \mathrm{rot}\, 2\pi/n$

where r and s satisfy the relations

$$r^n = s^2 = e, \qquad sr = r^{n-1}s.$$

$(sr)^2 = srsr = \underbrace{s^2}_{e} r^{n-1} r = r^n = e$

$(sr^k)^2 = e$ for $0 \leq k \leq n-1$

Prove this :)