The integers mod N and relatively prime to N with multiplication are an abelian group

$\mathbb{Z}/N$ N integer >0. $N=3$

$[a][b] = [ab]$ $[1][2]=[2]$

$[2][2] = [4] = [1]$.

- multiplication is associative.

$([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)]$
$= [a][bc]$
$= [a]([b][c])$

- there is an identity element.

$[1][a] = [a][1] = [a]$ for all a.

- inverses. $[a][b] = 1$.

If $a=0$ there is no b so that $[0][b]=[1]$

$\mathbb{Z}/N$ is not a group because 0 has no inverse.

- $(\mathbb{Z}/N\mathbb{Z}) \setminus \{[0]\}$? $N=4$.

$[2][2] = [4] = [0]$

if $[2][x] = [1]$

$[0] = [2][2][x] = [2]$ a contradiction.

$U(N) = \{[a] \in \mathbb{Z}/N \mid \gcd(a,N)=1\}$. $U(N)$ is a group. $[1]$ is the identity

$[a] \in U(N)$. Find x so that $[a][x] = 1$.

Solve $\boxed{au+Nr=1}$ by Euclid's algorithm.

$au \equiv 1 \bmod N$

$[a][u]=[1]$

u is the inverse of a.

$\mathbb{Z}/4$ $\quad \cancel{[0]}, [1], \cancel{[2]}, [3]$ $\qquad U(N) = \{[1],[3]\}$ $\qquad [9] = [1]$

	1	3
1	1	3
3	3	1

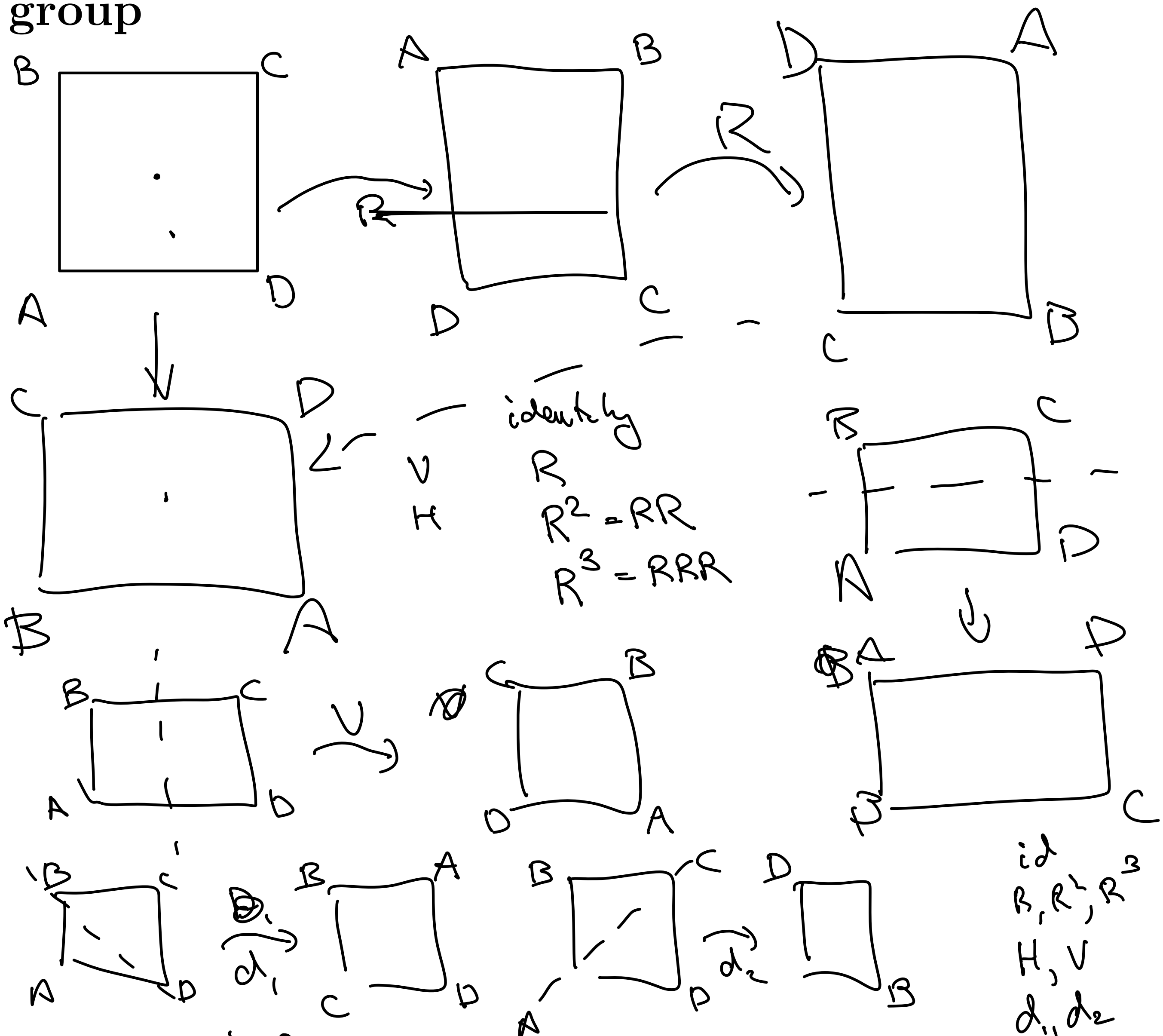
$\mathbb{Z}/10\mathbb{Z}$ $\quad \cancel{[0]}\ [1]\ \cancel{[2]}\ [3]\ \cancel{[4]}\ \cancel{[5]}\ \cancel{[6]}\ [7]\ \cancel{[8]}\ [9]$

$U(N) = \{[1],[3],[7],[9]\}$

$U(10)$ $\qquad [21] = [1]$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The symmetries of a square are a nonabelian group



identity

V $\quad R$

H $\quad R^2 = RR$

$R^3 = RRR$

id

R, R^2, R^3

H, V

d_1, d_2

- associative
- identity = identity symmetry
- inverses:

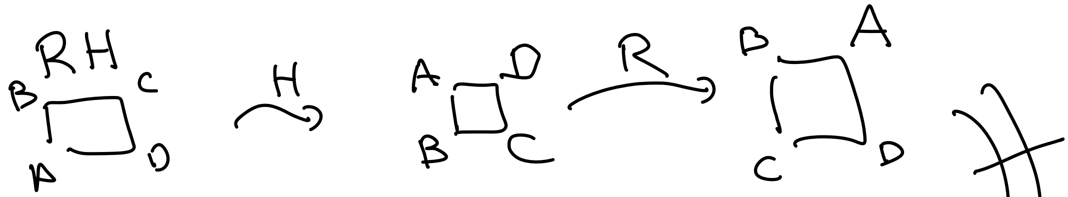
$H^2 = id$ $\qquad d_1^2 = id$

$V^2 = id$ $\qquad d_2^2 = id$

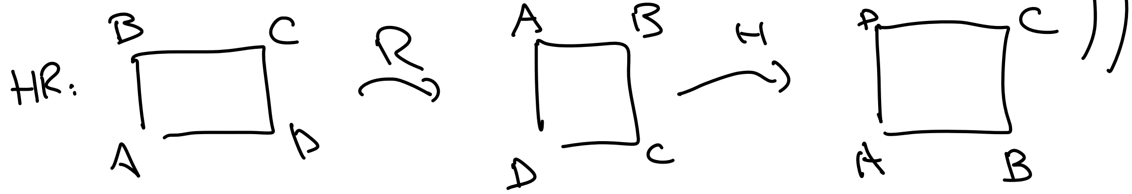
R^3 = left rotation

$R^3 \cdot R$ = identity

$R^2 \cdot R^2$ = identity



Non-abelian group.



2 by 2 real matrices under addition are an abelian group

$$M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,b,c,d \in \mathbb{R} \right\}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}$$

These form a group.

•) $$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) + \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

$$= \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix} + \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} (a+x)+r & (b+y)+s \\ (c+z)+t & (d+w)+u \end{bmatrix}$$

$$= \begin{bmatrix} a+(x+r) & b+(y+s) \\ c+(z+t) & d+(w+u) \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} + \begin{bmatrix} r & s \\ t & u \end{bmatrix}\right)$$

so addition of matrices is associative.

•) identity element = $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

•) <u>inverses</u> inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Invertible 2x2 matrices with real entries under multiplication ($\underbrace{\mathrm{GL}_2(\mathbb{R})}$) are a nonabelian group

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{matrix} ad-bc \neq 0 \\ a,b,c,d \in \mathbb{R} \end{matrix} \right\}.$

$$\underset{A}{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \underset{B}{\begin{pmatrix} x & y \\ z & w \end{pmatrix}} = \underset{AB}{\begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}}$$

- matrix mult. is associative. $(AB)C = A(BC)$
- identity $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- inverses.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $ad-bc \neq 0$

A^{-1} exists so $AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -\frac{c}{\Delta} & a/\Delta \end{pmatrix}$

$\Delta = ad-bc \neq 0$

$$AA^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix} = \begin{pmatrix} \frac{ad-bc}{\Delta} & \frac{-ab+ab}{\Delta} \\ \frac{cd-cd}{\Delta} & \frac{-bc+ad}{\Delta} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

If $\Delta = 0$ then there is no inverse to a matrix

NOT abelian

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \underline{\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \underline{\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}}$$

The quaternion group with 8 elements is a non-abelian group

$Q = \{\pm 1, \pm i, \pm j, \pm k\}$

$i^2 = j^2 = k^2 = -1$

$(-1)^2 = 1^2 = 1$

$(-i)^2 = (-1)^2(i^2) = 1 \cdot (-1) = -1$

$$\boxed{\begin{array}{ll} i \cdot j = k & j \cdot k = i \\ j \cdot i = -k & k \cdot j = -i \\ k \cdot i = j & i \cdot k = -j \end{array}}$$

- Associative $(ij)(k) = (k)(k) = k^2 = -1$
  $(i)(jk) = (i)(i) = i^2 = -1$
  $(ki)j = j \cdot j = j^2 = -1$
  $k(ij) = k \cdot k = k^2 = -1$
- identity: 1 $\quad 1 \cdot j = j \quad 1 \cdot i = i \ldots$
- inverses:
  $1 \cdot 1 = 1$ $\quad j \cdot (-j) = +1 \quad k(-k) = +1$
  $-1 \cdot -1 = 1$ $\quad i \cdot (-i) = +1$
- Not Abelian: $i \cdot j \neq j \cdot i$ for example.

The nonzero complex numbers with multiplication are an abelian group

$\mathbb{C}^* = \{x \in \mathbb{C} \mid x \neq 0\}.$

$x = a + bi \quad a, b \in \mathbb{R}, \quad i^2 = -1$

- associative $\quad ((a+bi)(c+di))(u+vi) \stackrel{?}{=}$

  $(a+bi)((c+di)(u+vi))$

- identity element is 1.

- inverses: $\quad (a+bi)^{-1} = \dfrac{a-bi}{a^2+b^2}$

  $(a+bi)\dfrac{(a-bi)}{a^2+b^2} = 1 \quad \checkmark$

abelian $\quad (a+bi)(c+di) = (ac-bd) + (bc+ad)i$

$(c+di)(a+bi) = (ac-bd) + (ad+bc)i$

The complex numbers of norm 1 with multiplication are an abelian group

$$S = \{ x \in \mathbb{C} \mid \|x\|^2 = 1 \}$$

$$= \{ a+bi \mid a, b, \in \mathbb{R}, \ a^2+b^2 = 1 \}.$$

- $\|(a+bi)(c+di)\|^2 = \|a+bi\|^2 \|c+di\|^2 = 1$
  $a+bi, c+di \in S$
- $1 \in S$
- $(a+bi)^{-1} = \dfrac{(a-bi)}{a^2+b^2} = (a-bi)$
  $\|a-bi\|^2 = 1 \in S.$

$$e^{i\theta} = \cos\theta + i\sin\theta \qquad \|re^{i\theta}\|^2 = r^2$$

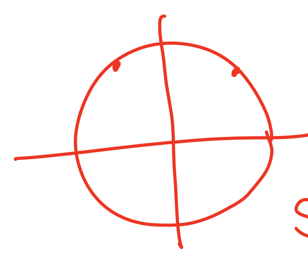
$$re^{i\theta} = r\cos\theta + i r\sin\theta \qquad \|r e^{i\theta}\|^2 = 1$$

$$\Rightarrow r = \pm 1$$

$$e^{i\pi} = -1$$

$$-e^{i\theta} = e^{i\pi} \cdot e^{i\theta} = e^{i(\theta+\pi)}$$

$$S = \{ e^{i\theta} \mid \theta \in [0, 2\pi) \}.$$



S

$$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$