Groups of order 1

Let $G=\{g\}$. There is only one possible binary operation $*: G\times G \to G$, which is given by $g*g=g$.

- associativity ✓

$$(g*g)*g = g*g = g*(g*g).$$

- identity $= g$ ✓
- inverses: $g*g = \overset{=e}{g} \Rightarrow g^{-1}=g$. ✓

Conclusion: There is one group of order 1, up to "isomorphism".

Ex: $(\{g\},*)$, $(\{1\},\cdot)$, $(\{0\},+)$

The sets and binary ops. here are all different, but these are all groups of order 1. However, after relabelling they are essentially the same as algebraic objects.

Def: Two groups $(G, *)$ and $(H, \circ)$ are <u>isomorphic</u> if there is a bijection $\varphi: G \to H$ satisfying

$$\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2), \quad \forall g_1, g_2 \in G.$$

(<u>isomorphism</u>) Notation: $G \cong H$.

<u>Multiplication tables for binary operations</u>

Suppose that $S = \{s_1, \ldots, s_n\}$ and that $*$ is a binary operation on S. The <u>multiplication table</u> for $*$ is the $n \times n$ table whose $(i,j)^{th}$ entry is $s_i * s_j$.

	s_1	s_2	$\cdots$	s_n
s_1	$s_1 * s_1$	$s_1 * s_2$	$\cdots$	$s_1 * s_n$
s_2	$s_2 * s_1$	$s_2 * s_2$	$\cdots$	$s_2 * s_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
s_n	$s_n * s_1$	$s_n * s_2$	$\cdots$	$s_n * s_n$

Two finite groups G_1 and G_2 with $|G_1| = |G_2|$ are isomorphic if, after bijectively identifying the elements of one with the other, the corresponding elements in the multiplication tables are the same.

Groups of order 2 (written multiplicatively)

Suppose G is a group with $|G|=2$.

Write $G=\{e,x\}$, consider the multiplication table:

	e	x
e	e	x
x	x	e

- e is the identity:
  $e^2=e$
  $ex=xe=x$
- x has an inverse:
  forces $x^2=e$ $(x^{-1}=x)$

Conclusion: Only one group of order 2, up to isomorphism.

"Another" group of order 2:

$(\{-1,1\},\cdot)$

	1	-1
1	1	-1
-1	-1	1

(isomorphic to the group above)

Groups of order 3

Suppose G is a group with $|G|=3$.

Write $G=\{e,x,y\}$

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

- e is the identity

- If $xy=y$ then $x=e$ (cancellation law)

  This can't happen, b/c of uniqueness of e.

  If $xy=x$ then $y=e$, which also can't happen.

  Therefore $xy=e$.

  By a similar argument, $yx=e$

- If $x^2=e$ then $x^{-1}=x$, which contradicts uniqueness of inverses.

  If $x^2=x$ then $x=e$, which contradicts uniqueness of identity.

  Therefore $x^2=y$.

  Similarly, $y^2=x$.

Conclusion: There is one group of order 3, up to isomorphism.

Some comments:

1) All of the groups we have just listed are Abelian: their multiplication tables are symmetric about the main diagonal, so $g_i g_j = g_j g_i$, for all i, j.

2) All of these groups are also examples of <u>cyclic groups</u>: groups G with the property that

$$\exists\, g \in G \text{ s.t. } \forall\, h \in G,\ \exists\, n \in \mathbb{Z} \text{ s.t. } h = g^n.$$

generator or generating element for G

Notation:

$\forall\, x \in G$, $\langle x \rangle = \{ x^n : n \in \mathbb{Z} \}$ (if G is written multiplicatively)

(or $\{ nx : n \in \mathbb{Z} \}$ if G is written additively)

With this notation, G is cyclic iff

$\exists g \in G$ s.t. $G = \langle g \rangle$ (G is generated by g)

Exs:

1) Group with 1 element: $(G \cong C_1)$

$G = \{g\} = \langle g \rangle \qquad (g^n = g, \ \forall n \in \mathbb{Z})$

2) Group with 2 elements: $(G \cong C_2)$

$G = \{\underset{x^2}{e}, \underset{x^1}{x}\} = \langle x \rangle$

	e	x
e	e	x
x	x	e

$$\cdots = x^{-4} = x^{-2} = \overset{e}{\overset{\shortparallel}{x^0}} = x^2 = x^4 = \cdots$$

$$\cdots = x^{-3} = x^{-1} = \overset{x}{\overset{\shortparallel}{x^1}} = x^3 = x^5 = \cdots$$

3) Group with 3 elements: $(G \cong C_3)$

$G = \{\underset{x^3}{e}, \underset{x^1}{x}, \underset{x^2}{y}\} = \langle x \rangle$

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Note:

$$\cdots = x^{-6} = x^{-3} = \overset{e}{\overset{\shortparallel}{x^0}} = x^3 = x^6 = \cdots$$

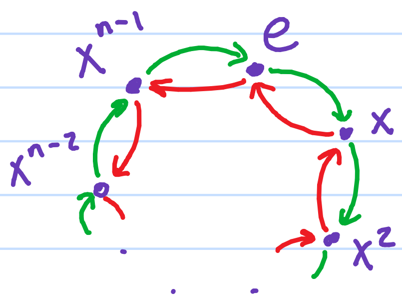
$$\cdots = x^{-5} = x^{-2} = \overset{x}{\overset{\shortparallel}{x^1}} = x^4 = x^7 = \cdots$$

$$\cdots = x^{-4} = x^{-1} = \overset{y}{\overset{\shortparallel}{x^2}} = x^5 = x^8 = \cdots$$

4) For each $n \in \mathbb{N}$, there is exactly one cyclic group G of order n, up to isomorphism.

$(C_n = Z_n = \mathbb{Z}_n)$

$$C_n = \langle x \rangle = \{ \underset{}{x^0}^{\,=e}, x^1, x^2, \ldots, x^{n-1} \}$$



$\longrightarrow$ = mult. by x

$\longrightarrow$ = mult. by x^{-1}

$$\cdots = x^{-2n} = x^{-n} = \overset{=e}{x^0} = x^n = x^{2n} = \cdots$$

$$\cdots = x^{1-2n} = x^{1-n} = x^1 = x^{1+n} = x^{1+2n} = \cdots$$

$$\cdots = x^{2-2n} = x^{2-n} = x^2 = x^{2+n} = x^{2+2n} = \cdots$$

$$\vdots$$

$$\cdots = x^{-1-n} = x^{-1} = x^{n-1} = x^{(n-1)+n} = x^{(n-1)+2n} = \cdots$$

Note: $x^{-1} = x^{n-1}$ $\quad (x x^{n-1} = x^n = e)$

$x^{-2} = x^{n-2}$ $\quad (x^2 x^{n-2} = x^n = e)$

$\vdots \qquad \vdots$

$x^{-k} = x^{n-k}$ $\quad (x^k x^{n-k} = x^n = e)$

Other common isomorphic versions of this group:

- $(\mathbb{Z}/n\mathbb{Z}, +)$ (integers modulo n under addition)
- $(\{z \in \mathbb{C} : z^n = 1\}, \cdot)$ (nth roots of unity in $\mathbb{C}$ under multiplication)
- $n \geq 3$:

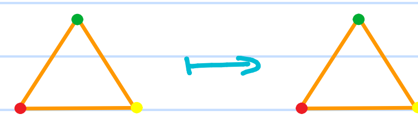
$$\left(\left\{ \begin{array}{l} \text{rotations in the plane preserving} \\ \text{a regular } n\text{-gon centered at } (0,0) \end{array} \right\}, \circ \right)$$

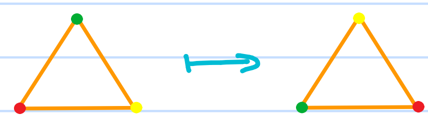
composition of maps

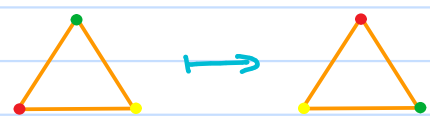
Ex: $n = 3$, $G = \{r_0, r_{2\pi/3}, r_{4\pi/3}\}$

$r_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ is rotation counterclockwise by θ about $(0,0)$

- Check that $(G, \circ)$ is a group:

r_0 : 

$r_{2\pi/3}$: 

$r_{4\pi/3}$: 

Associativity ✓

(Composition of functions $f: S \to S$ is associative)

Identity $= r_0$ ✓

$(r_0 \circ r_\theta = r_\theta \circ r_0 = r_\theta, \ \forall \theta \in \mathbb{R})$

Inverses: $r_0^2 = r_0 \Rightarrow r_0^{-1} = r_0$

$r_{2\pi/3} r_{4\pi/3} = r_{4\pi/3} r_{2\pi/3} = r_0 \Rightarrow \begin{array}{l} r_{2\pi/3}^{-1} = r_{4\pi/3} \\ r_{4\pi/3}^{-1} = r_{2\pi/3} \end{array}$ ✓

Write $r = r_{2\pi/3}$. Then $r^0 = e = r_0$ and $r^2 = r_{4\pi/3}$,

so $G = \{r^0, r^1, r^2\}$, and $G \cong C_3$.

5) While we're talking about this, one more cyclic group: $(\mathbb{Z},+)$ (infinite)

$\mathbb{Z} = \{n \cdot 1 : n \in \mathbb{Z}\} = \langle 1 \rangle$ (additive notation)

Final comment:

3) Trying to classify groups of order n by looking at multiplication tables is computationally unfeasible, for large n. (e.g. there are n^{n^2} binary operations on a set of cardinality n)