Basics

Prototypical examples of cyclic groups

1. The integers are a group with + as the operation. The integers can be made by starting with 0 and 1 and considering all of the sums

$$1, 1+1, 1+1+1, \ldots$$

together with

$$-1, -1-1, -1-1-1, \ldots$$

We say that 1 *generates* the integers.

$1, 1+1, 1+1+1, \ldots$

$$\left.\begin{matrix} 1, 2, 3, \ldots \\ -1, -2, -3, -4, \ldots \\ 0 \end{matrix}\right\} \text{yields} \rightsquigarrow \mathbb{Z}$$

$-1, -1-1 = -2, -1-1-1 = -3, \ldots$

$1, 1+1, \ldots$

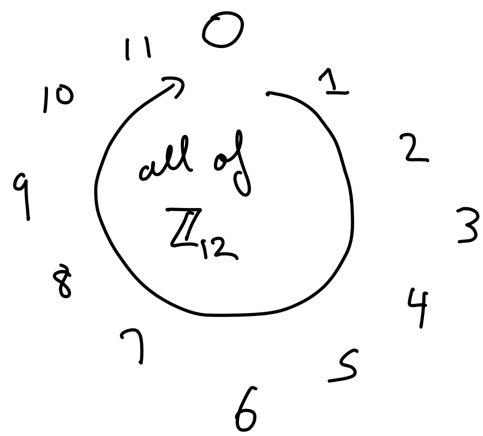
0

-1 generates the integers

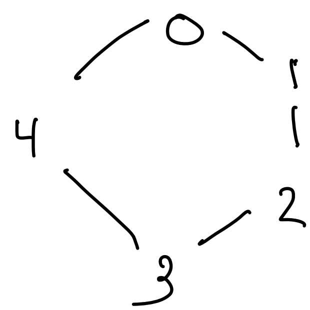
2. Let $G = \mathbb{Z}_n$ for some $n > 1$. G can be made by starting with 0 and 1 and then considering the sums $1, 1+1, \ldots$.

$n = 12$

$11 + 1 = 12 \equiv 0$ in $\mathbb{Z}_{12}$



$\mathbb{Z}_5$



1 generates $\mathbb{Z}_5$

Fundamental definitions

Definition: Let G be a group and let $g \in G$ be an element. Define:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

$\langle g \rangle$ is called the cyclic subgroup of G generated by ~~G~~. g.

Note: if we are writing the group operation using $+$, then

$$\langle g \rangle = \{ng : n \in \mathbb{Z}\}.$$

$\mathbb{Z}_5$: $\langle 1 \rangle$ is the set $\{1, 2, 3, 4, 0\} = \mathbb{Z}_5$

$\mathbb{Z}$: $\langle 1 \rangle$ is the set $\{\underbrace{1, 2, 3, 4, \ldots}_{1\cdot 1,\, 2\cdot 1,\, \ldots}, \ldots, \underbrace{-1\cdot 1}_{-1}, \underbrace{-2\cdot 1}_{-2}, \ldots, 0\cdot 1 = 0\}$

$\langle 1 \rangle = \mathbb{Z}$.

$\mathbb{Z}$: $\langle 2 \rangle = \{2, 4, 6, \ldots, -2, -4, -6, \ldots, 0\} \neq \mathbb{Z}$.

Definition: If there is an element $g \in G$ so that $G = \langle g \rangle$, then we say that G is a *cyclic group* and that g generates G.

$\mathbb{Z}_5$, $\mathbb{Z}$ are cyclic gps $\quad$ $\mathbb{Z}_n$ cyclic $= \langle 1 \rangle$

Examples

The earlier examples $\mathbb{Z}$ and $\mathbb{Z}_N$ are cyclic groups.

If $n \in \mathbb{Z}$, then $\langle n \rangle$ is the cyclic subgroup of $\mathbb{Z}$ consisting of multiples of n. $\langle 2 \rangle \leq \mathbb{Z}$ consists of all even numbers

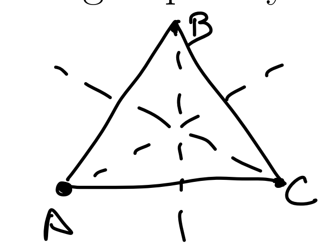
$\langle 5 \rangle = \{5, 10, 15, \ldots, -5, -10, -15, \ldots, 0\}$.

is a subgroup: $\langle 5 \rangle$ is nonempty

if $a \in \langle 5 \rangle$ and $b \in \langle 5 \rangle$ then $a-b \in \langle 5 \rangle$.

Pf: $a = 5n$ $b = 5m$ $a - b = 5\underbrace{(n-m)}_{\in \mathbb{Z}} \in \langle 5 \rangle$

If r is the rotation of the equilateral triangle, then $\langle r \rangle$ is the cyclic subgroup of symmetries of the triangle consisting of 3 rotations.



identity

r rotation to right

r^2 rotation to right 2 times

s_1, s_2, s_3

$\langle r_1 \rangle = \{r_1, r_1^2, r_1^3 = e\}$

$r^{-1} = r^2$ $r^3 = e$

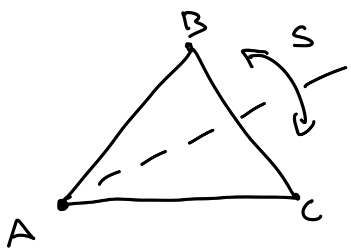
$r^{-2} = r$

$\langle r \rangle$ has 3 elements

in G (which has 6 elements)

More examples

If s is a reflection of the equilateral triangle then $\langle s\rangle$ is the two element cyclic subgroup consisting of 1 and $\langle s\rangle$.



$\langle s\rangle = \{s, s^2 = e\}$

$U(7)$ is cyclic and generated by 3.

$U(7) = \{a \in \mathbb{Z}_7 \mid (a,7) = 1\}$ with $*$.

$U(7) = \{1, 2, 3, 4, 5, 6\}$ 6 elements.

$\underline{3},\ 3^2 = \underline{2},\ 3^3 = 3\cdot 2 = \underline{6},\ 3^4 = 3\cdot 3^3 = 3\cdot 6 = 18 = \underline{4}$

$3^5 = 3\cdot 4 = 12 = \underline{5},\ 3\cdot 5 = 15 = \underline{1} \bmod 7$

$\langle 3\rangle = U(7)$ $U(7)$ is cyclic.

Cyclic groups may have more than one generator.

A look at $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12}$

$\langle 1\rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\} = \mathbb{Z}_{12}$

$\langle 2\rangle = \{2, 4, 6, 8, 10, 0\} \neq \mathbb{Z}_{12}$

$\langle 3\rangle = \{3, 6, 9, 0\}$

$\langle 4\rangle = \{4, 8, 0\}$

$\langle 5\rangle = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} = \mathbb{Z}_{12}$

$\langle 5\rangle = \mathbb{Z}_{12}$

Not every gp is cyclic.

Symmetries of $\triangle$ aren't cyclic.

rotations: $\langle r\rangle$ have 3 elements

reflections $\langle s\rangle$ has 2 elements

identity $\langle e\rangle$ has 1 group.

Quaternions: $\{\pm 1, \pm i, \pm j, \pm k\}$; $i^2 = j^2 = k^2 = -1$

$ij = k$, $ji = -k$

$jk = i$, $kj = -i$

$ki = j$, $ik = -j$

$\langle 1\rangle = \{1\}$

$\langle -1\rangle = \{-1, 1\}$

$\langle i\rangle = \{i, -1, -i, 1\}$

$\langle j\rangle, \langle k\rangle$ have 4 element