1

Example. Consider $(\mathbb{Z}, +)$, $\langle 5 \rangle = \{\ldots, -5, 0, 5, 10, \ldots\}$. This is called $5\mathbb{Z}$ (integer multiple of 5). Note that this is not $\mathbb{Z}_5$. The latter doesn't even have the same operation.

Is $\mathbb{Z}$ generated by 5? No. But 1 would do.

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

Lemma

The inverse of a generator of a group is also a generator.

Is $\mathbb{Z}$ cyclic? Yes, it is generated by 1 (or -1).

$5\mathbb{Z}$ is a cyclic group generated by 5. $\mathbb{Z}_5$ is generated by 1.

Is $\mathbb{Z}_n$ cyclic? Yes it is generated by 1.

Theorem

Any cyclic group is either isomorphic to $(\mathbb{Z}_n, +_n)$ or to $(\mathbb{Z}, +)$.

Question: Is $(\mathbb{R}, +)$ cyclic?

No. Since $\mathbb{R}$ is uncountable, so there is no bijection between $\mathbb{R}$ and $\mathbb{Z}$ or $\mathbb{Z}_n$.

Definition: greatest common divisors (gcd)

Note. The gcd of a, b can be written as $ra + sb$ with $r, s \in \mathbb{Z}$.

Example. $28r + 40s = 4 \Rightarrow 28 \times 3 + 40 \times (-2) = 4$.

Example. In $\mathbb{Z}_{40}$, what is $\langle 28 \rangle$?

This is controlled by the gcd(28,40). The key is $r = 3$. What else is in $\langle 28 \rangle$? $\{0, 28, 16, 4\}$. So $4 \in \langle 28 \rangle$. Then we have $\{0, 4, 8, \ldots, 36\}$ with $\frac{40}{4} = 10$ elements !

In $\mathbb{Z}_{40}$, $\langle 28 \rangle = \langle 4 \rangle$.

Theorem

In $\mathbb{Z}_n$, the subgroup $\langle r \rangle$ is equal to $\langle d \rangle$, where d=gcd(r, n). Then number of elements in $\langle d\rangle$ is $\frac{n}{d} = \frac{n}{\gcd(r,n)}$.

Theorem

Every subgroup of a cyclic group is cyclic.

Corollary

Every subgroup of $\mathbb{Z}_n$ is of form $\langle r\rangle$, and in fact we can take r to be a divisor of n.

Example. What are the subgroups of $\mathbb{Z}_{18}$?

We just need to choose an appropriate generator from the divisors of 18. $\langle 1\rangle = \mathbb{Z}_{18}$
$\langle 2\rangle = \{0, 2, 4, \ldots\}$ 9 elements.
$\langle 3\rangle = \{0, 3, \ldots\}$ 6 elements.
$\langle 6\rangle = \{0, 6, 12\}$ 3 elements.
$\langle 9\rangle = \{0, 9\}$ 2 elements.
$\langle 18\rangle = \{18\}$ 1 element.
$\langle 10\rangle = \langle 2\rangle$.
$\langle 7\rangle = \langle 1\rangle$ because 7 and 18 are coprime.

See iPad for subgroup lattice.

Example. Subgroup lattice of $\mathbb{Z}_4$. See iPad.

Notation. Let $(G, *)$ be a group, and let $g \in G$. For multiplication, we define $g^2 = g * g, \ldots, g^n = g * \ldots * g$ with n occurrence of gs. $g^0 = e$. g^{-1} is the inverse. $g^{-2} = \left(g^{-1}\right)^2 = \left(g^2\right)^{-1}$ (this is easy to check). $g^{-n} = \left(g^{-1}\right)^n = (g^n)^{-1}$.

The subgroup $\langle g\rangle$ is given by

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

It is true that $g^m * g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$. Caution: m, n are not elements of G.

If the operation is addition. we write $2g = g + g, 0g = e, -1g = g^{-1}, \ldots$ then

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

Theorem

Every cyclic group is abelian.

Note. The converse is false. V_4 is a counterexample.

Proof

If G is cyclic then $G = \{g^n : n \in \mathbb{Z}\}$. For some generator g, let $x, y \in G$. Then $x = g^n$ and $y = g^m$. Then

$$x * y = g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n = y * x.$$

So G is abelian. $\square$