Cyclic Groups

If $G = < a >$; i.e. $G = \{a^n | \ n \in \mathbb{Z}\}$ then G is called a **cyclic group** and a is its generator. If G is finite then the **order** of a is the order of $< a >$. If G is not finite we say a has infinite order.

Ex. If $G = \mathbb{Z}_{10}$ then $a = 1$ generates G and has order 10.

Ex. If $G = \mathbb{Z}$ then $a = 1$ generates G and has infinite order.

Theorem: Every cyclic group is abelian.

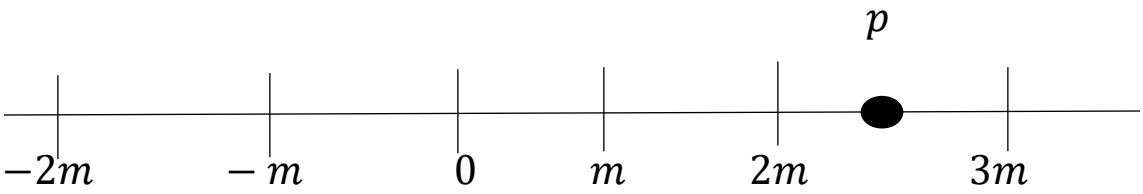
Proof: $G = \{a^n | \ n \in \mathbb{Z}\}$

Let $g_1, g_2 \in G$ then $g_1 = a^k, \ \ g_2 = a^j$.

$g_1 g_2 = a^k \cdot a^j = a^{k+j} = a^{j+k} = a^j \cdot a^k = g_2 g_1$ so G is abelian.

Theorem (Division Algorithm for $\mathbb{Z}$): If m is a positive integer and p is any integer, then there exist unique integers q and r such that

$$p = mq + r \text{ and } 0 \leq r < m.$$



If $p = qm$ for some q then $r = 0$. Otherwise $qm < p < (q+1)m$ for some q and since the distance between qm and $(q+1)m$ is m, $0 < r < m$.

We call q the quotient and r the non-negative remainder when p is divided by m.

Ex. Find q and r when 46 is divided by 7.

$$7, 14, 21, 28, 35, 42, 49, \ldots$$

$$42 < 46 < 49$$

So $46 = 7(6) + 4$

$q = 6$ and $r = 4$.

Theorem: A subgroup H of a cyclic group G is cyclic.

Proof: Let G be generated by a; $G = \{a^n | \, n \in \mathbb{Z}\}$.

If $H = < e > = \{e\}$ then H is cyclic.

If $H \neq \{e\}$ then $a^p \in H$ for some $p \in \mathbb{Z}^+$.

Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

Now let's show that $d = a^m$ generates H.

We must show that every $b \in H$ is a power of d.

Since $b \in H$ and $H \leq G$, we have $b = a^p$ for some p.

Find q, r such that $p = mq + r$ for $0 \leq r < m$.

Then $a^p = a^{mq+r} = (a^m)^q a^r$,

so $a^r = (a^m)^{-q} a^p$.

Now since $a^p \in H, a^m \in H$ and H is a group, both $(a^m)^{-q}$ and a^p are in H thus,

$(a^m)^{-q} a^p \in H$ Thus $a^r \in H$.

Since m is the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus, $p = qm$ and $b = a^n = (a^m)^q = d^q$. Thus b is a power of d.

Ex. $\mathbb{Z}, +$ is a cyclic group. By the previous theorem any subgroup of $\mathbb{Z}$ must also be cyclic. Thus, any subgroup of $\mathbb{Z}$ must be generated by n, an integer (i.e. the subgroups of $\mathbb{Z}$ are precisely $n\mathbb{Z}$ where n is an integer).

Def. Let r and s be two positive integers. $H = \{nr + ms | \, n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}, +$ and thus is cyclic with a generator $d \in \mathbb{Z}^+$. d is called the **greatest common divisor** of r and s. We write: $\boldsymbol{d = GCD(r, s)}$**.** Since $r, s \in H$ and $d \in H$ there must exist integers m, n such that $d = nr + ms$.

Ex. Find $GCD(60, 96)$

Positive divisors of 60 are $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

Positive divisors of 96 are 1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96.

$GCD(60, 96) = 12$.

The easiest way to find the GCD is to prime factor the numbers and take the common factors:

$60 = 2^2 \times 3 \times 5, \quad 96 = 2^5 \times 3,$ so $GCD(60, 96) = 2^2 \times 3 = 12$.

If 2 numbers r, s are relatively prime (i.e. have only 1 as a common factor) then $GCD(r, s) = 1$.

Def. Two groups $< S,* >$ and $< S',*' >$ are **isomorphic** if there exists a 1-1 function ϕ (called an **isomorphism**) of S onto S' such that:

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S.$$

Ex. Show the group of roots of $x^4 = 1$, $G = \{1, i, -1, -i\} = \{i^0, i^1, i^2, i^3\}$, where $i = \sqrt{-1}$, is isomorphic to $\mathbb{Z}_4$.

Let $\phi: G \to \mathbb{Z}_4$, by $\phi(i^k) = k$.

By definition, ϕ is 1- 1 if $\phi(x) = \phi(y) \implies x = y$ for any $x, y \in G$.

$$\phi(i^j) = \phi(i^k)$$

$$j = k \implies i^j = i^k.$$

ϕ is onto $\mathbb{Z}_4$ because if $x \in \mathbb{Z}_4$, then $\phi(i^x) = x$, and $i^x \in G$.

Now we must show that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in G$.

In this case: $*=$ usual multiplication

$*'=$ addition modulo 4.

$$\phi(i^j * i^k) = \phi(i^j \cdot i^k) = \phi(i^{j+k})$$

$$= j +_4 k$$

$$= \phi(i^j) +_4 \phi(i^k) = \phi(i^j) *' \phi(i^k).$$

So ϕ is an isomorphism from G to $\mathbb{Z}_4$.

Theorem: Let G be a cyclic group with generator a.

1. If the order of G is infinite, then G is isomorphic to $< \mathbb{Z}, + >$.
2. If G has finite order n, then G is isomorphic to $< \mathbb{Z}_n, + >$.

Proof:

1. Assume for all positive integers $s, a^s \neq e$.
   In this case, no two distinct exponents j and k can give equal elements a^j and a^k of G.
   Suppose that $a^j = a^k$ and say $j > k$ then, $a^j a^{-k} = a^{j-k} = e$ but this contradicts the assumption $a^s \neq e$ for $s \in \mathbb{Z}^+$. Hence every element of G can be expressed as a^s for a unique $s \in \mathbb{Z}$.

   Define ϕ by: $\phi: G \to \mathbb{Z}$; $\phi(a^i) = i$.

   This maps G onto $\mathbb{Z}$, and is 1-1 since:

   $$\phi(a^i) = \phi(a^j)$$

   means $i = j$ and thus $a^i = a^j$.

Now we must show $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in G$.

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j).$$

Thus ϕ is an isomorphism.

2. Assume $a^s = e$ for some positive integer s, let n be the smallest possible integer such that $a^n = e$.

   If $t \in \mathbb{Z}$ and $t = nq + r$ for $0 \leq r < n$.

Then $a^t = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$.

If $0 < k < h < n$ and $a^h = a^k$

then $a^{h-k} = e$ and $0 < h - k < n$, which contradicts that n is the smallest positive integer with $a^n = e$. Thus $h = k$.

Thus $a^0 = e, a, a^2, \ldots a^{n-1}$ are distinct elements of G.

Define ψ: $G \to \mathbb{Z}_n$ by $\psi(a^i) = i$.

ψ is 1-1 (as in part 1.) and onto.

And $\psi(a^i a^j) = \psi(a^{i+j}) = i +_n j = \psi(a^i) +_n \psi(a^j)$

So ψ is an isomorphism.

Ex. Find the order of the cyclic subgroup H of $\mathbb{Z}_{30}$ generated by 12.

Notice that: $a = 12$

$$a^2 = 12 + 12 = 24$$

$$a^3 = 12 + 12 + 12 = 36\ (mod\ 30) = 6$$

$$a^4 = 12 + 12 + 12 + 12 = 48\ (mod\ 30) = 18$$

$$a^5 = 12 + 12 + 12 + 12 + 12 = 60\ (mod\ 30) = 0.$$

So $H =< 12 >= \{0, 6, 12, 18, 24\}$.

Thus $|H| = 5$.

Notice that $|H| = \frac{|\mathbb{Z}_{30}|}{GCD(12,30)} = \frac{30}{6} = 5$.

This leads us to:

Theorem: Let G be a cyclic group with n elements and generated by a.

Let $c = a^t$. Then c generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements, where d is the greatest common divisor of n and t. Also $< a^t > = < a^p >$ if and only if

$$GCD(t, n) = GCD(p, n).$$

Corollary: If a is a generator of a finite cyclic group G of order n, then the other generators of G are elements of the form a^r, where r is relatively prime to n.

E x. Find the order of the subgroup $\mathbb{Z}_{18}, +$ generated by:

a) 6
b) 15.

a) $GCD(6,18) = 6$ so the order of the group generated by 6 is

$$\frac{18}{GCD(6,18)} = \frac{18}{6} = 3.$$

b) $GCD(15,18) = 3$ so the order of the group generated by 15 is

$$\frac{18}{GCD(15,18)} = \frac{18}{3} = 6.$$

Ex. Find all the subgroups of $\mathbb{Z}_{24}$ and draw a subgroup diagram.

The subgroup generated by 1 is the entire group $\mathbb{Z}_{24}$. Any other positive integer less than 24 and relatively prime to 24 will also generate $\mathbb{Z}_{24}$. Those numbers are $1, 5, 7, 11, 13, 17, 19,$ and 23.

Now let's take 2 as a generator:

$< 2 > = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$ is a group of order

$12 = \frac{24}{GCD(2,24)}$. Any other integer in $\mathbb{Z}_{24}$ of the form $b = 2h$, where h is relatively prime to 12 will also generate this subgroup.

So $b = 10, 14,$ and 22 i.e. $GCD(b, 24) = 2$.

$< 3 > = \{0, 3, 6, 9, 12, 15, 18, 21\}$ is a group of order $8 = \frac{24}{GCD(3,24)}$.

$GCD(b, 24) = 3$ if $b = 3h$ and h is relatively prime to 8,

i.e. $b = 9, 15$ and 21. Thus $9, 15,$ and 21 generate the same subgroup.

$< 4 > = \{0, 4, 8, 12, 16\ \ 20\}$ is a group of order $6 = \frac{24}{GCD(4,24)}$.

$GCD(b, 24) = 4$ if $b = 4h$ and h is relatively prime to 6,

i.e. $b = 20$. Thus 20 generates the same subgroup.

So far we have all subgroups generated by positive integers ≤ 23 except $6, 8, 12, 16,$ and $18.$

$< 6 > = \{0, 6, 12, 18\}$ is a subgroup of order $4 = \frac{24}{GCD(6,24)}$.

$GCD(b, 24) = 6$ if $b = 6h$ and h is relatively prime to 4,

i.e. $b = 18.$ Thus 18 generates the same subgroup.

$< 8 > = \{0, 8, 16\}$ is a subgroup of order $3 = \frac{24}{GCD(8,24)}$.

$GCD(b, 24) = 8$ if $b = 8h$ and h is relatively prime to 3,

i.e. $b = 16.$ Thus 16 generates the same subgroup.

$< 12 > = \{0, 12\}$ is a subgroup of order $2.$

$< 0 > = \{0\}$ is a subgroup of order $1.$

The subgroup diagram is: