Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism

(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Proof: Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n. Let $\varphi : \langle x \rangle \to \langle y \rangle$ be defined by $\varphi(x^k) = y^k$; we must first prove φ is well defined, that is,

$$\text{if } x^r = x^s, \text{ then } \varphi(x^r) = \varphi(x^s).$$

Since $x^{r-s} = 1$, Proposition 3 implies $n \mid r - s$. Write $r = tn + s$ so

$$\begin{aligned} \varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s = \varphi(x^s). \end{aligned}$$

This proves φ is well defined. It is immediate from the laws of exponents that $\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$ (check this), that is, φ is a homomorphism. Since the element y^k of $\langle y \rangle$ is the image of x^k under φ, this map is surjective. Since both groups have the same finite order, any surjection from one to the other is a bijection, so φ is an isomorphism (alternatively, φ has an obvious two-sided inverse).

If $\langle x \rangle$ is an infinite cyclic group, let $\varphi : \mathbb{Z} \to \langle x \rangle$ be defined by $\varphi(k) = x^k$. Note that this map is already well defined since there is no ambiguity in the representation of elements in the domain. Since (by Proposition 2) $x^a \neq x^b$, for all distinct $a, b \in \mathbb{Z}$, φ is injective. By definition of a cyclic group, φ is surjective. As above, the laws of exponents ensure φ is a homomorphism, hence φ is an isomorphism, completing the proof.

We chose to use the rotation group $\langle r \rangle$ as our prototypical example of a finite cyclic group of order n (instead of the isomorphic group $\mathbb{Z}/n\mathbb{Z}$) since we shall usually write our cyclic groups multiplicatively:

Notation: For each $n \in \mathbb{Z}^+$, let Z_n be the cyclic group of order n (written multiplicatively).

Up to isomorphism, Z_n is the unique cyclic group of order n and $Z_n \cong \mathbb{Z}/n\mathbb{Z}$. On occasion when we find additive notation advantageous we shall use the latter group as

our representative of the isomorphism class of cyclic groups of order n. We shall occasionally say "let $\langle x \rangle$ be the infinite cyclic group" (written multiplicatively), however we shall always use $\mathbb{Z}$ (additively) to represent the infinite cyclic group.

As noted earlier, a given cyclic group may have more than one generator. The next two propositions determine precisely which powers of x generate the group $\langle x \rangle$.

Proposition 5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$.

(2) If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{(n, a)}$.

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \dfrac{n}{a}$.

Proof: (1) By way of contradiction assume $|x| = \infty$ but $|x^a| = m < \infty$. By definition of order

$$1 = (x^a)^m = x^{am}.$$

Also,

$$x^{-am} = (x^{am})^{-1} = 1^{-1} = 1.$$

Now one of am or $-am$ is positive (since neither a nor m is 0) so some positive power of x is the identity. This contradicts the hypothesis $|x| = \infty$, so the assumption $|x^a| < \infty$ must be false, that is, (1) holds.

(2) Under the notation of (2) let

$$y = x^a, \quad (n, a) = d \quad \text{and write} \quad n = db, \ a = dc,$$

for suitable $b, c \in \mathbb{Z}$ with $b > 0$. Since d is the greatest common divisor of n and a, the integers b and c are relatively prime:

$$(b, c) = 1.$$

To establish (2) we must show $|y| = b$. First note that

$$y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = 1^c = 1$$

so, by Proposition 3 applied to $\langle y \rangle$, we see that $|y|$ divides b. Let $k = |y|$. Then

$$x^{ak} = y^k = 1$$

so by Proposition 3 applied to $\langle x \rangle$, $n \mid ak$, i.e., $db \mid dck$. Thus $b \mid ck$. Since b and c have no factors in common, b must divide k. Since b and k are positive integers which divide each other, $b = k$, which proves (2).

(3) This is a special case of (2) recorded for future reference.

Proposition 6. Let $H = \langle x \rangle$.

(1) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

(2) Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-function).

Proof: We leave (1) as an exercise. In (2) if $|x| = n < \infty$, Proposition 2 says x^a generates a subgroup of H of order $|x^a|$. This subgroup equals all of H if and only if $|x^a| = |x|$. By Proposition 5,

$$|x^a| = |x| \quad \text{if and only if} \quad \frac{n}{(a,n)} = n, \quad \text{i.e. if and only if } (a,n) = 1.$$

Since $\varphi(n)$ is, by definition, the number of $a \in \{1, 2, \ldots, n\}$ such that $(a,n) = 1$, this is the number of generators of H.

Example

Proposition 6 tells precisely which residue classes mod n generate $\mathbb{Z}/n\mathbb{Z}$: namely, $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $(a,n) = 1$. For instance, $\bar{1}, \bar{5}, \bar{7}$ and $\overline{11}$ are the generators of $\mathbb{Z}/12\mathbb{Z}$ and $\varphi(12) = 4$.

The final theorem in this section gives the complete subgroup structure of a cyclic group.

Theorem 7. Let $H = \langle x \rangle$ be a cyclic group.

(1) Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

(2) If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the nontrivial subgroups of H correspond bijectively with the integers $1, 2, 3, \ldots$.

(3) If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

Proof: (1) Let $K \leq H$. If $K = \{1\}$, the proposition is true for this subgroup, so we assume $K \neq \{1\}$. Thus there exists some $a \neq 0$ such that $x^a \in K$. If $a < 0$ then since K is a group also $x^{-a} = (x^a)^{-1} \in K$. Hence K always contains some positive power of x. Let

$$\mathcal{P} = \{b \mid b \in \mathbb{Z}^+ \text{ and } x^b \in K\}.$$

By the above, $\mathcal{P}$ is a nonempty set of positive integers. By the Well Ordering Principle (Section 0.2) $\mathcal{P}$ has a minimum element — call it d. Since K is a subgroup and $x^d \in K$, $\langle x^d \rangle \leq K$. Since K is a subgroup of H, any element of K is of the form x^a for some integer a. By the Division Algorithm write

$$a = qd + r \qquad 0 \leq r < d.$$

Then $x^r = x^{(a-qd)} = x^a(x^d)^{-q}$ is an element of K since both x^a and x^d are elements of K. By the minimality of d it follows that $r = 0$, i.e., $a = qd$ and so $x^a = (x^d)^q \in \langle x^d \rangle$. This gives the reverse containment $K \leq \langle x^d \rangle$ which proves (1).

We leave the proof of (2) as an exercise (the reasoning is similar to and easier than the proof of (3) which follows).

(3) Assume $|H| = n < \infty$ and $a \mid n$. Let $d = \dfrac{n}{a}$ and apply Proposition 5(3) to obtain that $\langle x^d \rangle$ is a subgroup of order a, showing the existence of a subgroup of order a. To show uniqueness, suppose K is any subgroup of H of order a. By part (1) we have

$$K = \langle x^b \rangle$$

where b is the smallest positive integer such that $x^b \in K$. By Proposition 5

$$\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n, b)},$$

so $d = (n, b)$. In particular, $d \mid b$. Since b is a multiple of d, $x^b \in \langle x^d \rangle$, hence

$$K = \langle x^b \rangle \leq \langle x^d \rangle.$$

Since $|\langle x^d \rangle| = a = |K|$, we have $K = \langle x^d \rangle$.

The final assertion of (3) follows from the observation that $\langle x^m \rangle$ is a subgroup of $\langle x^{(n,m)} \rangle$ (check this) and, it follows from Proposition 5(2) and Proposition 2 that they have the same order. Since (n, m) is certainly a divisor of n, this shows that every subgroup of H arises from a divisor of n, completing the proof.

Examples

(1) We can use Proposition 6 and Theorem 7 to list all the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given n. For example, the subgroups of $\mathbb{Z}/12\mathbb{Z}$ are

(a) $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle$ (order 12)
(b) $\langle \bar{2} \rangle = \langle \overline{10} \rangle$ (order 6)
(c) $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ (order 4)
(d) $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ (order 3)
(e) $\langle \bar{6} \rangle$ (order 2)
(f) $\langle \bar{0} \rangle$ (order 1).

The inclusions between them are given by

$$\langle \bar{a} \rangle \leq \langle \bar{b} \rangle \quad \text{if and only if } (b, 12) \mid (a, 12), \quad 1 \leq a, b \leq 12.$$

(2) We can also combine the results of this section with those of the preceding one. For example, we can obtain subgroups of a group G by forming $C_G(\langle x \rangle)$ and $N_G(\langle x \rangle)$, for each $x \in G$. One can check that an element g in G commutes with x if and only if g commutes with all powers of x, hence

$$C_G(\langle x \rangle) = C_G(x).$$

As noted in Exercise 6, Section 2, $\langle x \rangle \leq N_G(\langle x \rangle)$ but equality need not hold. For instance, if $G = Q_8$ and $x = i$,

$$C_G(\langle i \rangle) = \{\pm 1, \pm i\} = \langle i \rangle \quad \text{and} \quad N_G(\langle i \rangle) = Q_8.$$

Note that we already observed the first of the above two equalities and the second is most easily computed using the result of Exercise 24 following.