1. Cyclic groups and cyclic subgroups

Definition 1.1. A group H is cyclic if H can be generated by a single element, i.e., there exists $a \in H$ such that

$$H = \{a^n \mid n \in \mathbb{Z}\}.$$

In this case, we denote $H = \langle a \rangle$.

Example 1. In additive notation $\mathbb{Z}/n\mathbb{Z}$ is cyclic and $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

Remark 1.1.1.

(i) In additive notation $H = \{na \mid n \in \mathbb{Z}\}$.

(ii) If $H = \langle x \rangle$ then $H = \langle x^{-1} \rangle$ also. This means x, the generator, is not unique.

(iii) We could have $x^n = x^m$ even if $n \neq m$. For instance, in the example above, $2 \cdot \bar{1} = (n+2) \cdot \bar{1}$

(iv) Every cyclic subgroup H is Abelian. For example, if $H = \langle r \rangle$ in $G = D_n$, then H is Abelian, but D_n is not cyclic.

(v) By convention, $x^0 = 1$ for any element x.

Exercise 1. If $G = D_{2n}$ and $H \leq G$ the subgroup consisting of rotations, then $H = \langle r \rangle$ and $r^k = r^m$ if and only if $k \equiv m (\bmod n)$.

Proposition 1.2. *If $H = \langle x \rangle$ then $|H| = |x|$. More specifically:*

(i) If $|H| = n < \infty$, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all distinct elements of H.

(ii) If $|H| = \infty$, then $x^n \neq 1$ for $n \neq 0$ and $x^a \neq x^b$ for $a \neq b$ in $\mathbb{Z}$.

Proposition 1.3. *Let G be a group, $x \in G$, and $m, n \in \mathbb{Z} \backslash \{0\}$.*

- *If $x^m = 1$ and $x^n = 1$, then $x^d = 1$ where $d = (m, n)$.*
- *In particular, if $x^m = 1$, then $x^{|m|} = 1$.*

Proof. There exist $r, s \in \mathbb{Z}$ such that $d = mr + ns$ where $d = (m, n)$. Therefore,

$$x^d = (x^m)^r \cdot (x^n)^s = 1^r \cdot 1^s = 1.$$

If $x^m = 1$, let $n = |x|$. If $m = 0$, certainly $n \mid m$, so we may assume $m \neq 0$. Since some nonzero power of x is the identity, $n < \infty$. Let $d = (m, n)$ so by the preceding result $x^d = 1$. Since $0 < d \leq n$ and n is the smallest positive power of x which gives the identity, we must have $d = n$, that is, $n \mid m$ as asserted.

□

Theorem 1.4. *Any two cyclic groups of the same order are isomorphic.*

Proof. (i) **Finite case.** Let $H_1 = \langle x \rangle$ and $H_2 = \langle y \rangle$ where $|x| = |y| = n$. Define $\varphi : \langle x \rangle \to \langle y \rangle$ by $\varphi(x^k) = y^k$. Then φ is a well-defined isomorphism. Indeed, If $x^k = x^l$ then $x^{k-l} = 1$, whence $n \mid k - k$. Hence $nt = k - l$ for some $t \in \mathbb{Z}$. Thus $1 = y^{nt} = y^{k-l}$, whence $y^k = y^l$ and it follows that $\varphi(x^k) = \varphi(x^l)$. Note φ is a homomorphism because

$$\varphi(x^k \cdot x^l) = \varphi(x^{k+l}) = y^{k+l} = y^k \cdot y^l = \varphi(x^k) \cdot \varphi(x^l).$$

Moreover, φ is surjective since if $y^k \in \langle y \rangle$ then $\varphi(x^k) = y^k$. Recall that every surjective function between finite sets of the same cardinality is bijective (prove this if you have not seen it).

(ii) **Infinite case.** If $H = \langle x \rangle$ with $|H| = \infty$, then define $\varphi \colon \mathbb{Z} \to \langle x \rangle$ by $\varphi(k) = x^k$. It is clear that φ is an isomorphism. (If it is not clear for you, prove it.)

□

Remark 1.4.1. The second part of this proof tell us that, up to isomorphism, there exists a unique cyclic group of finite order n, namely $\mathbb{Z}/n\mathbb{Z}$, and a unique cyclic group of infinite order, namely $\mathbb{Z}$.

Proposition 1.5. *Let G be a group, let $x \in G$, and let $a \in \mathbb{Z} \setminus \{0\}$.*

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

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

(iii) If $|x| = n < \infty$ and $a > 0$ is such that $a \mid n$, then $|x^a| = \frac{n}{a}$.

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

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

Also,

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

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. The result is is established.

(ii) Let

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

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, $(b,c) = 1$. We must show $|y| = b$. First note that

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

so, we see that $|y|$ divides b. Let $k = |y|$. Then

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

so $n \mid ak$, 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, $b = k$.

(iii) This is a special case of the last item.

$\square$

Proposition 1.6. *Let $H = \langle x \rangle$.*

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

(ii) 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 $\phi(n)$ (where ϕ is Euler's ϕ-function).

Proof. We leave (i) as an exercise. In (ii) if $|x| = n < \infty$, note x^a generates a subgroup of H of order $|x^a|$. This subgroup equals all of H if and only if $|x^a| = |x|$. Thus

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

Since $\phi(n)$ 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.

$\square$

Theorem 1.7 (Complete structure of a cyclic group)**.** *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, $x^a \neq x^b$. Furthermore, for every integer m, $x^m = x^{|m|}$, 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, $x^m = x^{(n,m)}$, so that the subgroups of H correspond bijectively with the positive divisors of n.*

Proof. Classwork. $\square$

Remark 1.7.1. In $\mathbb{Z}/n\mathbb{Z}$,

(i) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{m} \rangle$ if and only if $(m, n) = 1$ for $m \in \mathbb{Z}$.

(ii) $\langle \overline{s} \rangle \leq \langle (\overline{s}, \overline{m}) \rangle$.

(iii) $\langle \overline{a} \rangle \leq \langle \overline{b} \rangle$ if and only if $(b, n) \mid (a, n)$ where $1 \leq a, b \leq n$.

Exercise 2. Find $a \in \mathbb{Z}$ such that $\mathbb{Z}/48\mathbb{Z} = \langle \overline{a} \rangle$. Find the order of $\overline{a}$ and the inclusion between the subgroups of $\mathbb{Z}/48\mathbb{Z}$. Notice that $48 = 2^4 \cdot 3$ and $\varphi(48) = 16$.