# Orders of elements in finite cyclic groups

**Thm** If $G = \langle g \rangle$ is a cyclic group of order $n$, then

$$|g^k| = n/d, \quad \text{where } d = \gcd(n,k),$$

for any $1 \le k \le n$.

exercise

**Recall**: $|a| = |\langle a \rangle| = \min_m \{a^m = e \mid m \ge 1\}$.

(Proof.) **Claim**: $g^m = e$ for a positive integer $m$ iff $n \mid m$.

Proof of claim:

If $n \mid m$, then $m = nq$, so

$$g^m = g^{nq} = (g^n)^q = e^q = e.$$

If $g^m = e$, then write $m = nq + r$, with $0 \le r < n$.

Then

$$e = g^m = g^{nq+r} = g^{nq} g^r = e g^r = g^r.$$

So $r = 0$, since $|g| = n$.

This proves the claim.

To compute $|g^k|$. Let $m = |g^k|$. So $m$ is the smallest pos. integer s.t. $(g^k)^m = e$.

$\longleftrightarrow$ smallest pos. integer s.t. $g^{km} = e$

$\longleftrightarrow$ smallest pos. integer s.t. $n \mid km$.

Let $d = \gcd(n,k)$. Then

$$n \mid km \iff (n/d) \mid (k/d)\, m.$$

But $n/d$ & $k/d$ are relatively prime, so $(n/d) \mid m$. So $|g^k|$ is the smallest positive integer $m$ divisible by $n/d$.

$$\therefore\ m = n/d.$$

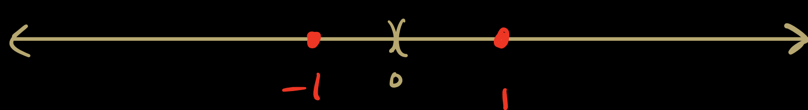
$\blacksquare$

<u>Cor</u>. The generators of $\mathbb{Z}_n$ are the integers $1 \le k < n$ which are relatively prime to $n$.

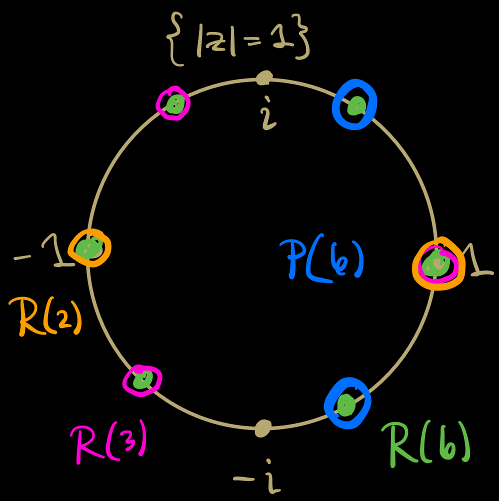
<u>Cyclic subgroups of $\mathbb{C}^*$</u>

$\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

$(\mathbb{R}^*, \times)$ has exactly one nontrivial finite cyclic subgroup: $\langle -1 \rangle = \{-1, 1\}$.




$(\mathbb{C}^*, \times)$ has infinitely many nontrivial finite cyclic subgroups. In fact, for any $n \geq 1$, $(\mathbb{C}^*, \times)$ contains a cyclic subgroup of order $n$.




If $z \in \mathbb{C}^*$ has order $n$, then $z^n = 1$. We call solutions to $z^n = 1$ **$n^{th}$ roots of unity.**

exercise

$$R(n) = \{e^{2\pi i k/n} \mid 0 \le k \le n-1\}.$$

__Check:__ $(R(n), \times)$ is a cyclic subgroup of order $n$.

The elements of $R(n)$ which have order $n$ are called **primitive $n^{th}$ roots of unity.**

$$P(n) = \{e^{2\pi i k/n} \mid 0 \le k \le n-1 \;\&\; \gcd(n,k) = 1\}.$$

__Exercise.__ Let $R =$ __all__ roots of unity, of any order.

Is $R$ a group? If so, is it cyclic?

Can you describe $R$ geometrically?

---

## __Subgroups of $S_n$__

__Vocabulary__

A **permutation** of a set $X$ is a bijection $\sigma : X \to X$.

Denote by $S_n$ the collection of all permutations of $X = \{1, 2, \ldots, n\}$.

Fact: $|S_n| = n!$ Also, $(S_n, \circ)$ forms a group.

We call $(S_n, \circ)$ the symmetric group on $n$ letters.

Subgroups of $S_n$ are called permutation groups.

## Notation

We read our binary operation right-to-left:

$\sigma, \tau \in S_n \Rightarrow \sigma\tau =$ "$\tau$, then $\sigma$".

We can rep. $\sigma \in S_n$ with a $2 \times n$ matrix:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \rightsquigarrow \begin{matrix} \sigma(1) = 3 & \sigma(3) = 1 \\ \sigma(2) = 2 & \sigma(4) = 4 \end{matrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \rightsquigarrow \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Better: cycle notation.

A cycle of length $k$ is $\sigma \in S_n$ s.t. $\exists$ distinct integers $a_1, a_2, \ldots, a_k$ s.t.

$$\sigma(a_1) = a_2, \ \ldots, \ \sigma(a_{k-1}) = a_k, \ \sigma(a_k) = a_1,$$

with $\sigma(i) = i$ for all other integers $1 \le i \le n$.

Notation: $\sigma = (a_1 a_2 \cdots a_k)$

Ex $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\,3)$

$\sigma\tau$ is NOT a cycle

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$$

Call a pair of cycles **disjoint** if the subsets that they permute are disjoint.

Ex $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ is disjoint from $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

Thm Every permutation of $S_n$ can be written as a product of disjoint cycles.

(Proof.) Fix $\sigma \in S_n$, let $X = \{1, 2, \dots, n\}$.

Set $X_1 = \{1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots\} \subseteq X$.

Next, let $i \in X \setminus X_1$ be smallest integer in $X \setminus X_1$ and set

$$X_2 = \{i, \sigma(i), \sigma^2(i), \sigma^3(i), \dots\} \subseteq X \setminus X_1.$$

Repeat this process until we've exhausted $X$:

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_r.$$

For each $1 \leq i \leq r$, define a cycle $\sigma_i : X \to X$ by

$$\sigma_i(x) := \begin{cases} \sigma(x), & x \in X_i \\ x, & x \in X \end{cases}.$$

The cycles $\sigma_1, \dots, \sigma_r$ are disjoint, and

$\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$.

<u>Example</u>. Apply the proof technique to a random permutation.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 5 & 1 & 2 & 4 & 6 \end{pmatrix}$$

$$\sigma_1 = (1\,7\,6\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$$

$$\sigma_2 = (2\,3\,5)$$

$$\sigma = \sigma_1 \sigma_2 = (1\,7\,6\,4)(2\,3\,5)$$

cycles

permutation, but not a cycle