Cyclic Groups

Definition

A group G is said to be *cyclic* if $G = \langle a \rangle$ for some $a \in G$.

Examples

1. $(\mathbb{Z}, +)$ is an infinite cyclic group, with 1 as a generator. An alternative generator is -1.
2. For a natural number n, the group of nth roots of unity in $\mathbb{C}^\times$ is a cyclic group of order n, with (for example) $e^{\frac{2\pi i}{n}}$ as a generator. The elements of this group are the complex numbers of the form $e^{k\frac{2\pi i}{n}}$, where $k \in \mathbb{Z}$.
3. For $n \geq 3$, the group of rotational symmetries of a regular n-gon (i.e. a regular polygon with n sides) is a cyclic group of order n, generated (for example) by the rotation through $\frac{2\pi}{n}$ in a counterclockwise direction.

Remark Cyclic groups are always abelian.

"The" cyclic group of order n

It is common practice to denote a cyclic group of order n generically by C_n, and an infinite cyclic group by C_∞. We might write C_n as $\langle x \rangle$ and think of C_n as being generated by an element x. The elements of C_n would then be

$$\mathrm{id}, x, x^2, \ldots, x^{n-1}.$$

Here it is understood that $x^n = \mathrm{id}$, and that multiplication is defined by $x^i \cdot x^j = x^{[i+j]_n}$,
where $[i+j]_n$ denotes the remainder on dividing $i+j$ by n.

Multiplication table for $C_4 = \langle x \rangle$ is given below.

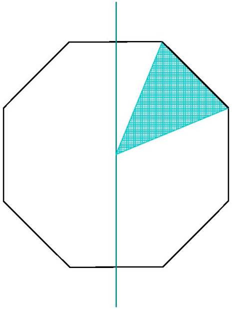
C_4	id	x	x^2	x^3
id	id	x	x^2	x^3
x	x	x^2	x^3	id
x^2	x^2	x^3	id	x
x^3	x^3	id	x	x^2

Generating sets

Let S be any non-empty subset of a group G. Then we can define *the subgroup of G generated by S*. This is denoted by $\langle S \rangle$ and it consists of all the elements of G that can be obtained by starting with the identity and the elements of S and their inverses, and composing these elements in all possible ways under the group operation. So $\langle S \rangle$ is the smallest subgroup of G that contains S.

Definition If $\langle S \rangle$ is all of G, we say that S is a *generating set* of G.

Example In D_{2n}, let $S = \{R_{\frac{360}{n}}, T\}$, where T is any one of the n reflections. Then S generates D_{2n}.
To see why, note that all the rotations arise from composing $R_{\frac{360}{n}}$ with itself repeatedly. All the reflections arise from composing T with the n rotations.



Challenge 2, Week 3

Let C_n be the cyclic group with n elements (think of it abstractly, or as the group of complex nth roots of unity, or the group of rotations of a regular n-gon, or the group of integers modulo n under addition, it doesn't matter).

How many of the n distinct elements of C_n generate n as a cyclic group? Explain your answer.