Lectures 5 and 6: Subgroups and generating sets

Definition

Suppose that G is a group with operation $\star$, and let H be a subset of G. Then H is a subgroup of G if H is itself a group under the operation of G.

Examples

1. The set $2\mathbb{Z}$ of even integers is a subgroup of $(\mathbb{Z}, +)$.
2. In the group S_4 of permutations of $\{1, 2, 3, 4\}$, the subset consisting of all those elements that map $4 \to 4$ is a subgroup. It consists of all the permutations of $\{1, 2, 3\}$ (with 4 fixed). It is a "copy" of S_3 inside S_4.
3. In the dihedral group D_{2n} (the symmetries of a regular n-gon), the set of rotational symmetries is a subgroup. The set of relections is not (Why?).

Deciding whether some subset is a subgroup

In $\mathbb{C}^\times$, let H be the set of complex numbers whose modulus is a (non-zero) rational number. Is H a subgroup of $\mathbb{C}^\times$?

1. Is H closed under multiplication?

2. Does H contain the identity element of $\mathbb{C}^\times$?

3. Does H contain the inverse in $\mathbb{C}^\times$ of each of its elements?

Cyclic subgroups

Let $(G, \star)$ be a group, and let a be an element of G. Within G, we can combine a with itself under $\star$ to get a (probably different) element of G. We can repeat this process and build the following sequence of elements of G

$$a,\ a \star a,\ a \star a \star a,\ a \star a \star a \star a, \ldots$$

Any subgroup of G that contains a must be closed under $\star$, so it must contain all these elements (which are not necessarily all distinct). It must also contain id_G, and it must contain a^{-1}, the inverse of a. It must contain all of the following:

$$\ldots a^{-1} \star a^{-1},\ a^{-1},\ \mathrm{id}_G,\ a,\ a \star a,\ a \star a \star a, \ldots$$

Moreover, all these elements do form a group, called the cyclic subgroup of G generated by a, and denoted $\langle a \rangle$.

Lecture 6: Generating Sets

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 C_n of order n

The order of a group is the number of elements in it.
The order of an element is the number of elements in the cyclic subgroup that it generates.
The cyclic group of order 5, generated by an element x, has table

	id	x	x^2	x^3	x^4
id	id	x	x^2	x^3	x^4
x	x	x^2	x^3	x^4	id
x^2	x^2	x^3	x^4	id	x
x^3	x^3	x^4	id	x	x^2
x^4	x^4	id	x	x^2	x^3

This group has manifestations as

- complex 5th roots of unity under $\times$ (with $x = e^{2\pi i/5}$)
- integers modulo 5 under $+$ (with $x = 1$)
- rotational symmetries of a hexagon under $\circ$ (with $x = R_{72}$)

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.