

Lecture 5: Subgroups

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 $4 \rightarrow 4$ 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 reflections 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

$$a, a \star a, a \star a \star a, a \star a \star a \star a, \dots$$

Any subgroup of G that contain 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:

$$\dots a^{-1} \star a^{-1}, a^{-1}, \text{id}_G, a, a \star a, a \star a \star a, \dots$$

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

Examples

1. In $(\mathbb{Z}, +)$, the cyclic subgroup generated by 5 is

2. In $GL(2, \mathbb{Q})$, the cyclic subgroup generated by $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ is

Weekly Challenge 3

Is it possible that a group G could have a subgroup H whose identity element is not the identity element of G itself? Give an example where this occurs, or reason from the group axioms to explain why it never could.