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 $4 \to 4$ 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 $\mathbb{C}^\times$ (non-zero complex numbers under multiplication), let H be the set of complex numbers whose modulus is a (non-zero) rational number. Is H a subgroup of $\mathbb{C}^\times$?

3 things to check:

1. Is H closed under multiplication? ✓ (non-zero rational numbers)

Let $x, y \in H$. Then $|x| \in \mathbb{Q}$ and $|y| \in \mathbb{Q}$

Is $xy \in H$? i.e. is $|xy| \in \mathbb{Q}$?

Well $|xy| = |x||y|$. Since $|x|$ and $|y|$ are rational, $|x||y|$ is rational. So $xy \in H$

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

Identity element in $\mathbb{C}^\times$ is 1 $(= 1 + 0i)$

Its modulus is 1, which is rational.

So $1 \in H$.

Conclusion: H is a subgroup of $\mathbb{C}^\times$

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

If $x \in H$, then $|x| \in \mathbb{Q}$, and $|x^{-1}| = |1/x| = 1/|x| \in \mathbb{Q}$

So $x^{-1} \in \mathbb{Q}$ and $x^{-1} \in H$

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 $\langle a \rangle$.

Examples

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

$\{\ldots, -5+(-5), -5, 0, 5, 5+5, 5+5+5, \ldots\}$

$= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$

– the additive consisting of all integer multiples of 5.

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

$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$

$A^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ (Id)

Note $A^4 = A$, $A^5 = A^2$, $A^6 = I_2$ etc

$A^{-1} = A^2$

$\langle A \rangle = \{A, A^2, A^3\}$

$= \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\right\}$

A^3 $\quad$ A $\quad$ A^2

Challenge 1, Week 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.