

Cyclic Subgroups

The simplest way to get subgroups of a group is to take an element of the group and all its “powers.”

$$\begin{aligned} a^n &= \underbrace{a \cdots a}_{n \text{ times}} \\ a^{-n} &= \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}} = (a^n)^{-1} \\ a^0 &= e \end{aligned}$$

The collection of all the powers of a is denoted $\langle a \rangle$. It is a subgroup.

Note: In specific examples, the multiplicative notation isn't necessarily used; one usually uses whatever notation is appropriate.

Examples 1) The group $\text{GL}_2(\mathbb{R})$ and

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

2) The group S_3 and $a = (1, 2, 3)$

3) The group \mathbb{Z} and $a = 2$

4) The group \mathbb{Z}_{23}^\times and $a = 2$

5) The group \mathbb{Z}_n and $a = 1$.

Recall that we did exactly this sort of thing with \mathbb{Z}_p^\times back in chapter 1. You may remember that the powers of a eventually repeated. This happens in general.

Lemma: Suppose G is a finite group and $a \in G$. Then there is a smallest positive integer n where $a^n = e$. This smallest n is called the *order* of a , and is denoted $o(a)$. If $n = o(a)$, then

$$\langle a \rangle = \{a^1, \dots, a^n\}.$$

Proof: Suppose G has m elements. Then at least two of a^1, \dots, a^{m+1} are equal. Say $a^i = a^j$ where $1 \leq i < j \leq m+1$. This means that $a^j(a^i)^{-1} = e$. But $(a^i)^{-1} = (a^{-1})^i = a^{-i}$, so $a^{j-i} = e$. Since $j-i$ is positive (and also $< m+1$), the set of all positive integers n where $a^n = e$ is not empty. Thus, this set has a smallest element.

Suppose $n = o(a)$. Using the reasoning above, a^1, \dots, a^n must all be distinct (otherwise a^{j-i} would be e with $0 < j-i < n$). Also, $a^n = e = a^0$.

Suppose $z \in \mathbb{Z}$. By the division algorithm, $z = qn + r$ where $0 \leq r < n$. This implies that

$$a^z = a^{qn+r} = a^{qn}a^r = (a^n)^qa^r = e^qa^r = a^r.$$

Hence, every element of $\langle a \rangle$ is equal to an a^r where $0 \leq r < n$. Since $a^n = a^0$, we're done.

Notice how the subgroup $\langle a \rangle$ is just like \mathbb{Z}_n ; “multiplication” of an a^i and an a^j is just addition of i and j modulo n .