§2 - Subgroups

By now we have seen many examples of groups. Some of these groups arise as subsets of a larger group with the same operation.

e.g. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, and all of these sets form groups under addition.

e.g. $\{1,-1\} \subseteq \{1, i, -1, -i\} \subseteq \mathbb{C}^*$, and all of these sets form groups under multiplication.

Definition: Let $(G, \cdot)$ be a group.

If H is a subset of G and $(H, \cdot)$ is a group, we say that H is a subgroup of G, and write $H \leq G$.

Remarks:

(i) For a subset H of a group G to be a subgroup, it must form a group with respect to the same operation as G.

(ii) Every group G is accompanied by two subgroups: $\{e\}$ (the trivial group)

G (the group itself)

A subgroup $H \leq G$ not equal to $\{e\}$ or G

is called a <u>proper subgroup</u> of G.

<u>Ex:</u> Consider the set of even integers

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

sitting inside the additive group $\mathbb{Z}$. It is easy to see that $2\mathbb{Z}$ also forms a group under addition, and hence $2\mathbb{Z} \leq \mathbb{Z}$.

Notice that in every example we have seen, the group G and its subgroup H share the same identity element. This is always the case.

<u>Proposition:</u> If G is a group with identity e_G and $H \leq G$ with identity e_H, then $e_G = e_H$.

Proof: $e_H = e_H^2$, as e_H = identity for H.

Let e_H^{-1} be the inverse of e_H in G. Then

$$e_G = e_H e_H^{-1} = e_H^2 e_H^{-1} = e_H(e_H e_H^{-1}) = e_H e_G = e_H \quad \blacksquare$$

Ex: Is $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ a subgroup of $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$? No!

$\mathbb{Z}_8^* \subseteq \mathbb{Z}_8$, but the operations are different.

Ex: Is $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a subgroup of $\mathbb{Z}$?

No! $\mathbb{Z}_n \not\subseteq \mathbb{Z}_n$ (remember, the elements of $\mathbb{Z}_n$ are really equivalence classes of integers!)

The operations in these groups are also not the same: $\mathbb{Z}$ is a group under addition,

$\mathbb{Z}_n$ is a group under addition mod n.

Theorem (The Subgroup Test):

Let G be a group. A non-empty subset $H \subseteq G$ is a subgroup if and only if

(i) $ab \in H$ for all $a, b \in H$, and

(ii) $a^{-1} \in H$ for all $a \in H$.

Proof: ($\Rightarrow$) Suppose that $H \leq G$.

Since H is a group, it contains the product of any of its elements (i.e., (i) holds) and the inverse of any of its elements (i.e., (ii) holds).

($\Rightarrow$) Now suppose that $\emptyset \neq H \subseteq G$ is such that (i) & (ii) hold.

[Closure] By (i), H is closed under the group operation.

[Associativity] The operation on H is associative because it is the same as the operation on G, which is associative since G is a group.

[Identity] $H \neq \emptyset$, so let $a \in H$. By (ii), $a^{-1} \in H$ and hence $e = aa^{-1} \in H$ (remember, H is closed under the group operation!).

[Inverses] By (ii), every $a \in H$ has an an inverse in H. $\blacksquare$

Exercise [One - Step Subgroup Test]:

Let G be a group. Prove that a non-empty subset $H \subseteq G$ is a subgroup of G if and only if $a^{-1}b \in H$ for all $a, b \in H$.

Ex: Let $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$.

This is called the special linear group.

Is $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ (under matrix mult?)

Let's see!

- $I = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} \in SL_n(\mathbb{R})$, so $SL_n(\mathbb{R}) \neq \emptyset$.

- If $A \in SL_n(\mathbb{R})$, then $\det(A) = 1 \neq 0$. Thus, $A \in GL_n(\mathbb{R})$, so $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$.

It's a non-empty subset.

Now let's use the subgroup test.

- If $A, B \in SL_n(\mathbb{R})$, then $\det(A) = \det(B) = 1$.

  Thus $\det(AB) = \det(A)\det(B) = 1$, so

  $AB \in SL_n(\mathbb{R})$.

- If $A \in SL_n(\mathbb{R})$, then $\det(A^{-1}) = \dfrac{1}{\det(A)} = 1$,

  hence $A^{-1} \in SL_n(\mathbb{R})$.

By the subgroup test, $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

Next we describe the simplest way to construct subgroups within a group G.

Definition: If a is an element of a group G, define $\boxed{\langle a \rangle = \{a^k : k \in \mathbb{Z}\}}$

Note that $\langle a \rangle \subseteq G$ and $\langle a \rangle \neq \emptyset$.

In particular, $e = a^0 \in \langle a \rangle$. Moreover, if $a^n, a^m \in \langle a \rangle$, then $a^{n+m} \in \langle a \rangle$ and $(a^n)^{-1} = a^{-n} \in \langle a \rangle$. Thus, by the subgroup test, $\underline{\langle a \rangle \leq G}$. We call $\langle a \rangle$ the subgroup generated by a.

Exercise: Prove that $\langle a \rangle$ is the smallest subgroup of G containing a (i.e., if $H \leq G$ and $a \in H$, then $\langle a \rangle \leq H$).

Ex: In $\mathbb{Z}_{10}^*$,

$\langle 1 \rangle = \{1\}$,

$\langle 3 \rangle = \{3^k : k \in \mathbb{Z}\} = \{1, 3, 7, 9\} = \mathbb{Z}_{10}^*$,

$\langle 7 \rangle = \{7^k : k \in \mathbb{Z}\} = \{1, 3, 7, 9\} = \mathbb{Z}_{10}^*$,

$\langle 9 \rangle = \{9^k : k \in \mathbb{Z}\} = \{1, 9\}$.

Ex: In $\mathbb{Z}$, for $n \neq 0$,

$$\begin{aligned} \langle n \rangle &= \{n^k : k \in \mathbb{Z}\} \\ &= \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\} \\ &= n\mathbb{Z} \end{aligned}$$

Ex: In D_n,

$\langle R \rangle = \{R^k : k \in \mathbb{Z}\} = \{e, R, R^2, \dots, R^{n-1}\}$

$\langle F \rangle = \{F^k : k \in \mathbb{Z}\} = \{e, F\}$

Definition: If a is an element of a group G, we define the order of a, $|a|$, to be the smallest positive integer k such that $a^k = e$. If no such k exists, we write $|a| = \infty$.

Ex: In $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$,

$|1| = 1$

$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 7, \quad 3^4 = 1 \Rightarrow |3| = 4$

$7^1 = 7, \quad 7^2 = 9, \quad 7^3 = 3, \quad 7^4 = 1 \Rightarrow |7| = 4$

$9^1 = 9, \quad 9^2 = 1 \Rightarrow |9| = 1.$

Ex: In $\mathbb{Z}$, $|0| = 1$ and $|a| = \infty$ for all $a \neq 0$.

Ex: In D_n, what is $|R| = n$, $|F| = 2$.

Notice anything interesting?

It appears that the order of an element $a \in G$ is the same as the order of the group $\langle a \rangle$. This will turn out to be the case, and it's why we call $|a|$ the order of a

Before proving this fact, we investigate the following lemma.

Lemma 2.1: Let a be an element of a group G.

(i) If $|a| = \infty$ then $a^i = a^j \Leftrightarrow i = j$

(ii) If $|a| = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

and $a^i = a^j \iff n \mid i-j$.

Proof: If $|a| = \infty$, then there is no $k \neq 0$ such that $a^k = e$. Thus, if $a^i = a^j$, we have $a^{i-j} = e$ and hence $i-j = 0$. We conclude that $i = j$, thereby proving (i).

Next, suppose that $|a| = n < \infty$. We will show that $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

It is clear that $\supseteq$ holds. But if a^k is an arbitrary element in $\langle a \rangle$, then

$$k = nq + r \quad \text{for some } r \in \{0, 1, \ldots, n-1\}$$

by the division algorithm. We have that

$a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, a^2, \dots, a^{n-1}\}$

This demonstrates $\subseteq$, so $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

It remains to show that $a^i = a^j \Leftrightarrow n \mid i-j$.

($\Leftarrow$) If $n \mid i-j$, then $i-j = nq$ for some $q \in \mathbb{Z}$.

Thus, $a^i = a^{j+nq} = a^j (a^n)^q = a^j e^q = a^j$.

($\Rightarrow$) If $a^i = a^j$, then $a^{i-j} = e$. Using the division algorithm, write

$i-j = nq + r$ for some $r \in \{0, 1, \dots, n-1\}$

Then $e = a^{i-j} = a^{nq+r} = a^r$. Since $r < n$, yet n is the smallest positive integer with $a^n = e$, it must be that $r=0$. Therefore $i-j=nq$, so $n \mid i-j$. This proves (ii). $\blacksquare$

Corollary 1: If a is an element of a group G, then $|a| = |\langle a \rangle|$.

Corollary 2: If a is an element of a group G and $a^k = e$, then $|a|$ divides k.

Proof: If $a^k = e$, then $a^k = a^0$. Thus, by the above lemma, n divides $k-0=k$. $\blacksquare$