Introduction to Groups

1.1 Groups

Consider past experiences with basic algebra. Beyond simple computation, computation would be used to solve equations. The simplest possible equations done would be linear equations of the form $a + x = b$. Condsider the example equation $5 + x = 3$. Then one would solve it by doing

$$\begin{aligned}
5 + x &= 3 \\
-5 + (5 + x) &= -5 + 3 \\
(-5 + 5) + x &= -5 + 3 \\
0 + x &= -5 + 3 \\
x &= -5 + 3 \\
x &= -2.
\end{aligned}$$

What was required to solve this equation? There were 3 mains things. Firstly associativity had to be utilized in order to group the -5 and 5 numbers together. Second, there needed to be a *neutral* element, in this instance 0. Thirdly, there needed to be an inverse element, in this instance -5. Therefore this shall be the motivation behind the definition of a group.

Definition 1.1 (Group). A group $\langle G, * \rangle$ is a set G closed under the binary operation $*$ such that it follows three axioms.

1. For all $a, b, c \in G$, we have
$$(a * b) * c = a * (b * c).$$
2. There exists an element $e \in G$ such that for all $x \in G$, we have
$$e * x = x * e = x.$$
3. For each element $a \in G$, there is an element $a' \in G$ such that
$$a * a' = a' * a = e.$$

Example 1.1. Take the structure $\langle Z, * \rangle$ where $a * b = a \cdot b$. The structure is not a group since there is no inverse element for *any* of the elements, therefore it certianly cannot be a group

1.2 Subgroups

Definition 1.2 (Subgroup). A subset H of a group G is a subgroup if it is

1. Closed under the binary operation of G
2. H with the induced operation of G is a group

The notation $H \leq G$ and $G \geq H$ denotes that H is a subgroup of G, and additionally $H < G$ and $G > H$ denote that H is a subgroup of G where $H \neq G$.

To show that a given subset of G is a subgroup over its induced binary operation, one can follow a simple 3 condition process. This process can be shrunken down to one condition as proved in Theorem 1.3.

Theorem 1.1 (Subgroup). A subset H of G is a subgroup of G if and only if

1. H is closed under the binary operation of G
2. The identity element e of G is in H
3. For all $a \in H$ it is true that $a^{-1} \in H$

Example 1.2. Consider the subset of $M_n(\mathbb{R})$ defined as

$$S = \left\{A \in M_n(\mathbb{R}) : A^\intercal A = I_n\right\}.$$

under the binary operation of matrix multiplication. Check the conditions that S is a subgroup of $M_n(\mathbb{R})$.

(Closure) Let $A, B \in S$. Then

$$\begin{aligned} (AB)^\intercal AB &= B^\intercal A^\intercal AB \\ &= B^\intercal I_n B \\ &= B^\intercal B \\ &= I_n. \end{aligned}$$

Therefore $AB \in S$.

(Identity) The identity matrix I_n is in S since $I_n = I_n^\intercal$, therefore

$$I_n^\intercal I_n = I_n I_n = I_n.$$

Therefore S has an identity element.

(Inverse) Let $A \in S$.

1.3 Generators and Cyclic Subgroups

Consider the group $\mathbb{Z}_n$ under modular addition. Something of interest to note is that every element in $\mathbb{Z}_n$ can be written as the repeated addition of 1. Take for example $\mathbb{Z}_3 = \{0, 1, 2\}$.

It follows then that

$$\begin{aligned} 1 &= 1 \\ 1 +_3 1 &= 2 \\ 2 +_3 1 &= 0. \end{aligned}$$

In this instance, the repeated operation of 1 produced all the elements of $\mathbb{Z}_3$. In a sense, the element 1 *generated* the entire group. This idea can be cautified abstractly.

Definition 1.3 (Generator). An element g of a group G is a generator for G if the set

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Is equivalent to G. That is

$$\langle g \rangle = G.$$

Example 1.3. Consider the cyclic subgroup of $GL(2, \mathbb{R})$ with the generator

$$\left\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\rangle.$$

For simplicity, denote the matrix as a and the identity matrix as e. Note that then

$$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

meaning that $a^2 = e$, implying that $a^{2n} = e$ and $a^{2n+1} = a$. Additionally, since $a^2 = e$, it follows that $a = a^{-1}$. therefore

$$\left\langle \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \leq GL(2, \mathbb{R}).$$

Example 1.4. Consider the cylic subgroup of $GL(2, \mathbb{R})$ with the generator

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Note that multiplaction of the matrix results in

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

In general,

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix}.$$

Therefore if a denotes the generating elements

$$a^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Additionally, $a^{-n} a^n = e$, meaning

$$a^{-n} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

Hence the group generated by a is

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} : k \in \mathbb{Z} \right\}.$$

Example 1.5. Is the following group cyclic?

$$G = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Z} \right\}.$$

The group is not cylic.

Proof. Assume towards contradiction that G is cylic. Consider two cases for a choice of generator. Assume that $b = 0$. Then all possible generators are in the form a where $a \in \mathbb{Z}$. However $a \neq \sqrt{2} \in G$, hence b cannot be zero. Assume then that $b \neq 0$. Then all generators are of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$. However, the generator will never result in any integers since $a + b\sqrt{2} \notin \mathbb{Z}$. Therefore the group cannot be cylic since there are no possible generators of the group. ■

Theorem 1.2. A group with no proper non-trivial subgroups is cyclic

Proof. Let G be a group and assume that it has no proper non-trivial subgroups, meaning that the only subgroups of G are $\{e\}$ and G. The case where $G = \{e\}$ is trivial. Therefore let $g \in G$ such that $g \neq e$. Then $\langle g \rangle \leq G$. However since G has no proper non-trivial subgroups, $\langle g \rangle \neq G$ and hence $\langle g \rangle = G$ ■

Theorem 1.3 (Singular Subgroup Condition). *H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.*

Proof. Let G be a group and $H \subseteq G$. Assume that $\forall a, b \in H$ that $ab^{-1} \in H$. Consider the three conditions (out of order in this case) in Theorem 1.1

2.) Let $a \in H$. Then $aa^{-1} \in H$, or equivalently $e \in H$. Therefore H contains the identity element of G.

3.) Let $b \in H$. Since $e \in H$, it follows that $eb^{-1} \in H$, or equivalently $b^{-1} \in H$. Therefore H has an inverse for every element within itself.

1.) Let $a, b \in H$. Since H contains inverses for every element, $b^{-1} \in H$ and also $\left(b^{-1}\right)^{-1} \in H$. Therefore $a\left(b^{-1}\right)^{-1} \in H$ or equivalently $ab \in H$. Hence H is closed under the binary operation of G.

Since H satisfies the 3 condition of Theorem 1.1, it follows that $H \leq G$. ■