Introduction to Group Theory 1

P. Reany

April 25, 2025

Abstract

Just the basics this time.

Wherever groups disclosed themselves, or could be introduced,
simplicity crystallized out of comparative chaos.
— Eric Temple Bell

1 Groups

Definition: A *group* G is a nonempty set of elements on which is defined a binary operator $*$, such that:

1) For any two elements a and b of G, $a * b$ and $b * a$ are elements of G [binary closure]. These elements are not necessarily the same.

2) For any three elements a, b, c of G, $(a * b) * c = a * (b * c)$ [composition associativity].

3) There exists an element e of G, such that for any element a of G, $e*a = a*e = a$ [e being referred to the group's *identity element*].

4) For every element a of G, there exists an element of a^{-1} of G, such that $a^{-1} * a = a * a^{-1} = e$ [a^{-1} being referred to as a's inverse in G].

By the way, the identity element is its own inverse.

Thus, we see from the definition of a group, that a group must contain at least one element, that being its identity element. A group with only one element is called the *trivial group*. However, assuming that the trivial group seems so simple that perhaps we can dispense with it is like the old error of thinking that the zero element of the integers is so simple that it can be dispensed with. Not so for either one.

In the study of abstract algebra, one does not study only specific groups, one also studies properties of abstract groups generally. **The goal of group theory is to unveil the structure of all groups.** To that end, one would like to be able to say meaningful things about generic groups, which might include

statements about their subgroups. A *subgroup* of a group is a subset of a given group which is also a group. And, wouldn't you know it? The trivial group is a subgroup of every group. It doesn't take too much thought to convince oneself that every group is a subgroup of itself. Let H be a subgroup of group G. H is said to be a *proper subgroup* of G if it is neither the full group nor the trivial group.

We need some shorthand way to indicate when an element g is in some group G. For that we write $g \in G$. To indicate that H is a subgroup of G, we write, $H \leq G$. To indicate that H is a subgroup of G but not equal to G, we write $H < G$. There is a very special kind of subgroup called a *normal subgroup* and it is symbolized as $H \trianglelefteq G$ and for a proper normal subgroup of group G: $H \triangleleft G$. We'll discuss normal subgroups presently.

Now, mathematicians prefer to declutter mathematical expressions whenever possible, so, in the definition of a group, they might just drop the $*$ symbol between the binary elements, leading us to rewrite the definition of a group as follows:

Definition: A *group* G is a set of elements on which is defined a binary operation, indicated by justiposition, such that:

1) For any two elements a and b of G, ab and ba are elements of G [binary closure].

2) For any three elements a, b, c of G, $(ab)c = a(bc)$ [composition associativity].

3) There exists an element e of G, such that for any element of a, of G, $ea = ae = a$ [e being referred to the the group's *identity element*].

4) For every element a of G, there exists an element of a^{-1}, of G, such that

$$a^{-1}a = aa^{-1} = e \tag{1}$$

[a^{-1} being referred to as a's *inverse* in G].

Problem: Show that we can weaken the assumption of the two-sided inverse for each element to the assumption of only a one-sided inverse, which establishes a two-sided inverse.

Let's assume that for each element a in G, a has a left inverse a' so that

$$a'a = e\,. \tag{2}$$

But a' also has a left inverse a''. Therefore

$$a''a' = e\,. \tag{3}$$

Multiplying through by a on the right, we get

$$a''a'a = a\,. \tag{4}$$

On using (2) on the LHS, we get

$$a'' = a\,. \tag{5}$$

On substituting this result into (3), we get

$$aa' = e\,. \tag{6}$$

Therefore, element a' is both a left and right inverse to a.

Problem: Let G be a group and let $f : G \longrightarrow G$ given by $f(g) = g^{-1}$ for all $g \in G$. Show that f is one-to-one.

2 Subgroups

When is a subset of a group a subgroup? By definition, a subgroup is a subset of a group which is a group in its own right. But we can simplify the determination of a subset being a subgroup by applying the following theorem:

Theorem: The minimal requirements to show that a nonempty subset S of a group $(G, *)$ is also a subgroup of G are:

a) The elements of S are closed under group composition, and

b) The elements of S are closed under inverses.

Homework Problem: Let H and K be subgroups of G. Show that $H \cap K$ is also a subgroup of G.

Definition: Let Z be the set of elements of group G that commute with all elements of G. This set is referred to as the *center* of G. Let's define it a bit more precisely.

$$Z(G) \equiv \{x \in G \,|\, xg = gx \;\; \forall g \in G\}\,. \tag{7}$$

Homework Problem:. Prove that Z is a subgroup of G.