Groups

The first algebraic structure we will study in details is **groups**. Unlike all the other structures we briefly discussed, groups have *only one operation*. It could be either "sum" or "product". [As you might have seen before in Math 251, what we call sum or product is not necessarily the *usual* notion of such!]
Before we actually see the definition, here are some examples:

- Any ring, field, vector space, module or algebra with its corresponding *sum*. [We just "forget" about the other operation.]
- A field, say F, without its zero element, with its corresponding *product*. This is usually denoted by $F^{\times}$ [or F^{*}].
- The elements of a ring, say R, that are *invertible*, with its corresponding *product*. This is usually denoted by $R^{\times}$. [Note that the previous example is a particular case of this one.]

Main Example

But the archetype of a group is the following example: let S be a set and

$$\mathrm{Perm}(S) \stackrel{\text{def}}{=} \{f : S \to S \ : \ f \text{ is a } \textit{bijection}\}.$$

[Remember, a **bijection** is a function which is both an **injection** [i.e., one-to-one] and a **surjection** [i.e., onto].]

The operation is the *composition* of functions. [Remember that the composition of bijections is a bijection.]

This group is called the **group of permutations of S**. [The elements of $\mathrm{Perm}(S)$ [i.e., the bijections] simply *permute* the elements of S.]

Symmetric Groups

If S has *finitely many elements*, say n, we can think of it simply as $\{1, 2, \ldots, n\}$ [by choosing an order to S]. [Note that S has no underlying structure!]

Thus, we have $\mathrm{Perm}(S) = \mathrm{Perm}(\{1, 2, \ldots, n\})$, and we denote this permutation group by S_n, and refer to it as the **symmetric group of degree n**.

This is the example from which the idea of groups came about, and we will study these in detail!

Getting to the Definition

So, to obtain the definition, we "copy the properties" of $\mathrm{Perm}(S)$ or S_n.

Firstly, unlike the examples coming from "numbers", here we only have **one [natural] operation**: composition. [Note that S has no structure. If S were, say, a ring, then we could add and multiply functions, by adding and multiplying their values, as it is usual.]

We always have the **identity function**: $\mathrm{id} : S \to S$, defined by $\mathrm{id}(s) = s$ for all $s \in S$.

Composition of functions are *always* **associative**: $(f \circ g) \circ h = f \circ (g \circ h)$.

Bijections have **inverse functions**: given $f \in \mathrm{Perm}(S)$, there is $g \in \mathrm{Perm}(S)$ such that $f \circ g = g \circ f = \mathrm{id}$. [Here id is the identity function above.] This function g is usually denoted by f^{-1}.

Binary Operation

Before we give the precise definition of groups, we give a precise definition for the referred "operation". The operations mentioned so far [sums, products, compositions] are all **binary operations**.

Definition

A **binary operation** on a set S is a function from $S \times S$ to S. [So, it produces an element of S from a pair of elements of S. Note that the result is in S *by definition*!]

Definition of a Group

Definition

A **group** is a set G with a binary operation $\cdot$ on G such that:

0. **Closed:** if $g, h \in G$, then $g \cdot h \in G$. [Note we don't need to list this, as it is part of the definition of binary operation, but it is important not to forget to check it!]
1. **Identity Element:** there is $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$. [Thus, G is non-empty!]
2. **Associative:** for all $g, h, k \in G$, we have $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.
3. **Inverse Element:** for all $g \in G$, there is $h \in G$ such that $g \cdot h = h \cdot g = e$. [Here e is the identity element above!]

Check that the previous examples are indeed groups!

Identity and Inverse

Theorem

The identity and inverse of an element are unique.

Proof.

Let e' be another identity [besides e]. Then,

$$
\begin{aligned}
e \cdot e' &= e' && \text{as } e \text{ is an identity,} \\
e \cdot e' &= e && \text{as } e' \text{ is an identity.}
\end{aligned}
$$

Thus $e = e'$.

Let h' be another inverse of g [besides h]. Then,

$$h = eh = (h'g)h = h'(gh) = h'e = h'.$$

$\square$

Notation

Since they are unique, we can refer to them as *the* identity of the group and *the* inverse of g.

When using the multiplicative notation [as above], we denote the inverse of g by g^{-1}. The identity is often denoted by 1.

Note that groups are not necessarily commutative [i.e., gh might be different from hg – this is the case for permutations!]. Commutative groups are called **Abelian groups**.

Sometimes, when dealing with *abstract Abelian groups*, one can denote the operation by "$+$". [We *never* us $+$ for non-commutative groups!] In this case, the inverse of g is denoted by $-g$ and the identity by 0.

Powers

Definition

Let a be an element of a group G.

Multiplicative Notation:

- $a^0 = 1$;
- $a^n = \underbrace{a \cdot a \cdots a}_{n \text{ factors}}$ for $n \in \mathbb{Z}_{>0}$;
- $a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ factors}}$ for $n \in \mathbb{Z}_{>0}$.

Additive Notation (for Abelian groups):

- $0 \cdot a = 0$;
- $n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ summands}}$ for $n \in \mathbb{Z}_{>0}$;
- $(-n) \cdot a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ summands}}$ for $n \in \mathbb{Z}_{>0}$.

Properties of Powers

Theorem

Let G be a group and $a, b \in G$. Then:

- $a^m \cdot a^n = a^{m+n}$ *for all* $m, n \in \mathbb{Z}$;
- $(a^m)^n = a^{mn}$ *for all* $m, n \in \mathbb{Z}$;
- $(ab)^{-1} = b^{-1}a^{-1}$.

Note that $(ab)^2 = abab$, *not* [necessarily] a^2b^2, as our groups are not necessarily commutative!

For *Abelian* groups with additive notation, we have:

- $(m \cdot a) + (n \cdot a) = (m + n) \cdot a$ for all $m, n \in \mathbb{Z}$;
- $n \cdot (m \cdot a) = (nm) \cdot a$ for all $m, n \in \mathbb{Z}$;
- $-(a + b) = (-a) + (-b)$.

In *this case*, $2(a + b) = 2a + 2b$.

Invertible Matrices

We denote by $\mathrm{GL}_n(\mathbb{R})$ the set of *invertible* matrices in $M_n(\mathbb{R})$. [**Remember:** a matrix $A \in M_n(\mathbb{R})$ is invertible if there is $B \in M_n(\mathbb{R})$ such that $BA = AB = I_n$, where I_n is the $n \times n$ *identity matrix*. You've seen that $A \in M_n(\mathbb{R})$ is invertible if, and only if, $\det(A) \neq 0$.] This is a group with the usual multiplication of matrices. [Check it! It might be helpful to use properties of the determinant.]

Similarly, $\mathrm{GL}_n(\mathbb{Z})$ is the set of invertible matrices in $M_n(\mathbb{Z})$. Is there a simple way to check if a matrix is invertible there [like the determinant in $\mathrm{GL}_n(\mathbb{R})$]? *Yes!* $A \in M_n(\mathbb{Z})$ is invertible if, and only if, $\det(A) = \pm 1$. [Can you see why? Think about the formula to invert a matrix and remember that we cannot have fractions in the entries of the inverse!]

$\mathrm{GL}_n(\mathbb{Z})$ is also a group [with the usual matrix multiplication]. In general, we call $\mathrm{GL}_n(R)$ the **general linear group of $n \times n$ matrices over R**.

Solving Equations

Theorem

Let G be a group [with operation denoted as multiplication]. If $a, b, x \in G$ and $ax = b$, then $x = a^{-1}b$.

Proof.

Since we have $a^{-1} \in G$, we have that

$$ax = b \Rightarrow a^{-1}(ax) = a^{-1}b \Rightarrow$$
$$(a^{-1}a)x = a^{-1}b \Rightarrow 1x = a^{-1}b \Rightarrow x = a^{-1}b.$$

□

This works then when G is either a groups of invertible matrices or a group of invertible "numbers" [both with multiplication].

Further Reading

Please read Section 2.1 from the text for extra examples and details!