Math 403 Chapter 2: Groups

---

1. **Introduction:** An extremely basic notion of a group is a collection of objects and a way to combine them. There is of course a more formal definition as well as requirements but before nailing down the specifics here are some examples:
   Example: We could take the integers with addition. If we add two integers we get another integer.
   Example: We could take the various ways to switch the objects in three boxes with the notion of doing one switch and then another. If we do two switches the result is a switch.

2. **Definition(s):** A *group* G is a set of objects (sometimes also sloppily denoted G) and a binary operation $*$ (not necessarily multiplication) which takes two objects in G, say a and b, and creates a new object $a * b$ which is also in G (this is called *closure*). Moreover we must have:

   (a) *Associativity:* For any $a, b, c \in G$ we have $(a * b) * c = a * (b * c)$.

   (b) *Identity:* There is some $e \in G$ such that for all $a \in G$ we have $e * a = a * e = a$. There is no assumption that this is unique!

   (c) *Inverses:* For every $a \in G$ there is some $b \in G$ with $a * b = b * a = e$. There is no assumption that this is unique!

   A word on notation. Often in the abstract we write ab instead of $a * b$ and this is usually fine, especially when $*$ is actually multiplication or something unambiguous. However if $*$ is addition then we should write $a + b$ instead of ab. When we do use ab notation then sometimes instead of e we write 1 but this only sometimes makes sense.

3. **Abelian Groups:** Note that there is no guarantee that $a * b = b * a$ for all $a, b \in G$. When this is true we say the group is *Abelian*, or *commutative*.

4. **Examples and Non-Examples:** Here are some examples and non-examples:
   Example: The structure $G = (\mathbb{Z}, +)$ is an Abelian group.
   Example: The structure $(\mathbb{Z}, -)$ is not a group. Why not?
   Example: The structure $G = (\{1, 3, 5, 7\}, \cdot \bmod 8)$ is an Abelian group.
   Example: The structure $G = (GL_2\mathbb{R}, \cdot)$ is a group but is not Abelian.
   Example: The structure $(\mathbb{R}, \cdot)$ is not a group.
   Example: The structure $G = (\mathbb{R} - \{0\}, \cdot)$ is an Abelian group.

5. **Elementary Properties:** The following are properties of a group. Notice that they're not part of the definition, rather they follow automatically from the definition.

   (a) **Theorem:** The identity is unique.
   Proof: Suppose e_1, e_2 are both identities. Then $e_1e_2 = e_1$ and $e_1e_2 = e_2$ so then $e_1 = e_2$. $\mathcal{QED}$

   (b) **Theorem:** The left and right cancellation laws hold.
   Proof: Suppose $ab = ac$. Left multiply by *an* inverse of a. Note that sometimes this is stated for non-identity a but it's fine for $a = e$ too, the point being that if $a = e$ then $ab = ac$ becomes $b = c$ without any cancellation at all. $\mathcal{QED}$

   (c) **Theorem:** Inverses are unique.
   Proof: Suppose b_1, b_2 are both inverses of a. Then $ab_1 = e = ab_2$ then cancel the a. $\mathcal{QED}$
   Note: Now we can use a^{-1} for *the* inverse of a.

(d) **Theorem:** The shoes-socks property holds: For $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$.
Proof: We wish to solve $(ab)(?) = e$. Note $abb^{-1}a^{-1} = e$. $\mathcal{QED}$
Note: We know that things like $(a^2)^3 = (a^3)^2$ because both are a^6. The Shoes-Socks property allows us to extend this to inverses and write things like $(a^2)^{-1} = (a^{-1})^2$. This is because:

$$(a^2)^{-1} = (aa)^{-1} = a^{-1}a^{-1} = (a^{-1})^2$$

Without ambiguity we can then also write a^{-2}.

6. **Closing Note:** When the operation is obvious we'll sometimes not bother to write it. For example when talking about the set $\mathbb{Z}$ the standard way to create a group is to use $+$ so often we'll write $G = \mathbb{Z}$ instead of $G = (\mathbb{Z}, +)$.