Group Theory

Varsity Practice 09/28/2025

Jeremy Beard

Groups are a kind of structure that pops up in pretty much every field of mathematics. While we can describe them by a relatively small list of axioms (rules), they have a rich theory, and often behave in strange ways you might not expect.

1 Basics of groups

Definition 1. Let G be a set, and $* : G \times G \to G$ be a binary function (that is, $*$ takes in two inputs (a, b) from G and outputs $*(a, b)$, a new element of G). Use the shorthand $a * b$ instead of $*(a, b)$.

We say $(G, *)$ is a *group* if it satisfies the following 3 axioms:

1. **Associativity:** for any $a, b, c \in G$, we have that $(a * b) * c = a * (b * c)$ (that is, the order in which we apply $*$ does not matter)
2. **Identity:** there is a special element $e \in G$ such that for all $a \in G$, we have

   $$a * e = a = e * a$$

   We call e an *identity* of $(G, *)$.
3. **Inverses:** for all $a \in G$ there exists some $b \in G$ such that

   $$a * b = e = b * a$$

   We call b an *inverse* of a.

These might be a little easier to process with an example.

Example 2. $(\mathbb{R}, +)$, that is, the real numbers $\mathbb{R}$ with addition $+$, form a group.

Associativity says that the order in which we add numbers doesn't matter - for example, $1+(2+3) = 1 + 5 = 6 = 3 + 3 = (1 + 2) + 3$.

The **identity** of $(\mathbb{R}, +)$ is 0, since adding 0 never changes the number (e.g. $0 + 2 = 2 = 2 + 0$).

The **inverse** of a number is just it's negative - e.g. $3 + (-3) = 0 = (-3) + 3$.

In similar ways, we can see that the following are groups:

Example 3.
1. $(\mathbb{R}, +)$, as described above.
2. $(\mathbb{R}\backslash\{0\}, \cdot)$, where $\cdot$ is multiplication.

3. (1) but with $\mathbb{R}$ replaced by $\mathbb{Q}$ or $\mathbb{Z}$.
4. (2), but with $\mathbb{R}$ replaced by $\mathbb{Q}$.
5. For any integer $n \geqslant 1$, let $C_n = \{0, 1, 2, \ldots, n-1\}$, and let $+_{\mod n}$ be addition modulo n (e.g. $-1 = 4 = 9 \mod 5$).Then $(C_n, +_{\mod n})$ is a group.

Question 1.1.
1. What are the identities in the examples (1)-(5)? What are the inverses?
2. Why is $(\mathbb{N}, +)$ not a group? Why is $(\mathbb{R}, \cdot)$ not a group? Why is $(\mathbb{Z}\backslash\{0\}, \cdot)$ not a group?
3. Show that $(\mathbb{Z}, -)$ does not satisfy the associativity axiom (and is therefore not a group).
4. Let $G = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. Why is $(G, +)$ not a group?

One useful fact is that the identity of a group is unique (note the identity axiom does not say there is *exactly* one identity explicitly!) Thus it makes sense to talk about *the* identity of $(G.*)$, rather than *an* identity.

Proposition 4. Let $(G, *)$ be a group. If e and f are both identities of $(G, *)$, then $e = f$.

Proof. Note that since f is an identity,

$$e * f = e$$

On the other hand, since e is an identity,

$$e * f = f$$

So $e = e * f = f$. □

The following fact will be an exercise later, and has a similar proof.

Fact 5. Let $(G, *)$ be a group. If $a, b, c \in G$ and b, c are both inverses of a, then $b = c$. That is, inverses are unique.

Notation 1.1. We denote the unique inverse of a by a^{-1}.

We can formalise the strategy for proving $(G, *)$ is a group with the process below:

- Check that $(G, *)$ is *closed* - that is, check that whenever $a, b \in G$, that $a * b$ in G.
- Check that $(G, *)$ is associative - that is, take $a, b, c \in G$ arbitrary, and show why $(a * b) * c = a * (b * c)$.
- Check that $(G, *)$ has an identity - that is, find the $e \in G$ that you think is the identity, take $a \in G$ arbitrary, and prove that $a * e = a$ and $e * a = a$.
- Check that $(G, *)$ has inverses - that is, take an arbitrary $a \in G$, and find some $b \in G$ such that $a * b = e$ and $b * a = e$.

To prove that $(G, *)$ is *not* a group, try to find a counterexample to closure, associativity, or existence of inverses, or show that there is no identity element.

Question 1.2. Where does the 'closed' condition appear in the definition of groups?

All the groups we have seen so far satisfy an extra assumption:

Definition 6. Let $(G, *)$ be a group. We say that $*$ is *commutative* if for every $a, b \in G$, $a * b = b * a$ (that is, the order of the elements does not matter).

We say the group $(G, *)$ is *Abelian* if $*$ is commutative.

This is a nice property - but one problem that can mess with our intuition of groups is that *not all groups are commutative!* Let's see an example.

Definition 7. Let $f : X \to Y$ be a function from set X to set Y. We say f is a *bijection* if whenever $x_1 \neq x_2 \in X$, $f(x_1) \neq f(x_2)$, and for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

That is, f maps X onto everything in Y in such a way that it never uses different inputs for the same output.

Definition 8. Let X be a set. Then the *symmetric group on* X is the group $(S^X, \circ)$ where

- S^X is the set of all bijections $f : X \to X$
- given $f, g \in S^X$, $g \circ f : X \to X$ is the function where $g \circ f(x) = g(f(x))$ for all $x \in X$.

For now, let's take on faith that this is a group. Let's see an example to make it less scary.

Example 9. Say $X = \{1, 2, 3\}$. Then say $f : X \to X$ is the function given by

$$f(1) = 2, f(2) = 3, f(3) = 1$$

Then $f \in S^X$, since it is a bijection (that is, 1, 2, and 3 all get mapped to different places, and something maps onto 1, 2, and 3). We could take $g : X \to X$ to be

$$g(1) = 2, g(2) = 1, g(3) = 3$$

Again, $g \in S^X$. In this case, we have

$$g \circ f(1) = g(f(1)) = g(2) = 1$$

$$g \circ f(2) = g(f(2)) = g(3) = 3$$

$$g \circ f(3) = g(f(3)) = g(1) = 2$$

which we can see is again a bijection.

We also can define $e : X \to X$ by

$$e(x) = x \text{ for } x = 1, 2, 3$$

which is the identity of this group.

Question 1.3. Let $X = \{1, 2, 3\}$ and let $f, g, e \in S^X$ be from the above example. Find $f \circ g$ and explain why it shows $(S^X, \circ)$ is *not* Abelian.

Now we have some intuition (or some idea of how strange groups can be!) we can tackle some exercises.

2 Exercises Part 1

Question 2.1. Is it possible for a group to have no elements? Why/why not?

Question 2.2. Let $n \geqslant 1$ be an integer. Let $C_n = \{0, 1, 2, 3, \ldots n-1\}$, and let $+_{\mod n}$ be addition modulo n. It is a fact that $(C_n, +_{\mod n})$ forms a group (you do not have to prove this). What is the identity, and for arbitrary $i \in C_n$, what is the inverse of i?

Question 2.3. Let $p \in \mathbb{N}$ be a prime number, and $\cdot$ be multiplication modulo p. It is a fact that $(C_p \backslash \{0\}, \cdot)$ forms a group, where $C_p \backslash \{0\} = \{1, 2, 3, \ldots p-1\}$ (you do not have to prove this). What is the identity?

Question 2.4. Using the notation from Question 2.3 above, why is $(C_4 \backslash \{0\}, \cdot)$ not a group?

(Hint: have a go multiplying together different elements from C_4. Do you break any of the 4 group conditions?)

Question 2.5. What about $(C_6 \backslash \{0\}, \cdot)$? More generally, is not a prime, why is $(C_n \backslash \{0\}, \cdot)$ not a group?

(Hint: we know that $n = ab$ for some $a, b \in C_n \backslash \{0\}$.)

Question 2.6. Let $(G, *)$ be a group, and $a, b, c \in G$. Show that if b and c are both inverses of a, then $b = c$ (that is, inverses are unique, so the notation a^{-1} makes sense).

(Hint: the argument should be a formal proof that shows inverses are unique for any *group. It might be helpful to look at Proposition 4 if you aren't used to these kinds of arguments.)*

Question 2.7. Given a set X, let X^X be the set of functions $f : X \to X$ (not just bijections). As before, we can define compositions $g \circ f$ for $f, g \in X^X$.

Let $X = \{1, 2\}$. Explain why $(X^X, \circ)$ is not a group. More generally, explain why if X has at least two elements, then $(X^X, \circ)$ is not a group.

Question 2.8. Let X be a set, and consider $(X^X, \circ)$. Following on from Question 2.7,

1. Is $(X^X, \circ)$ a group when X has size 1?
2. What about when X has size 0?

(Hint: if X is empty, what is X^X? How does this mesh with the identity axiom?)

Question 2.9. Let X be an arbitrary set this time. Use the process described earlier to explain why $(S^X, *)$ is a group with identity $e : X \to X$ given by $e(x) = x$ for all $x \in X$.

(Hint: when showing $(S^X, \circ)$ is closed, note that if $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f : A \to C$ is a bijection).

Question 2.10. (Tricky) Read Definition 12 ahead to learn what a subgroup is. Suppose $(G, *)$ is a finite group with subgroup $(H, *)$, and that $a \in G$. We define the *coset of a and H* to be

$$aH = \{a * h : h \in H\}$$

Note this is a subset of G, but may not be a subgroup.

1. Show that for all $a \in G$, $|aH| = |H|$ *(Hint: find a bijection from H to aH)*
2. Recall $\varnothing$ is the empty set. Show that if $aH \cap bH \neq \varnothing$, then $ah = b$ for some $h \in H$.
3. (Tricky) Show that for $a, b \in G$, either $aH = bH$ or $aH \cap bH = \varnothing$
4. Deduce why $|H|$ divides $|G|$ *(Hint: show that $|H| \cdot |\{aH : a \in G\}| = |G|$)*

3 Moving between groups

So far we have looked at groups in isolation, but often we need to consider how they interact. The most simple interaction might be a *homomorphism*, which is basically putting a group into another one while preserving the $*$ operation.

Definition 10. A *homomorphism* from group $(G, *)$ to a group $(H, \bigstar)$ is a function $f : G \to H$ such that for all $a, b \in G$, we have $f(a * b) = f(a) \bigstar f(b)$. We will sometimes write $f : (G, *) \to (H, \bigstar)$ for short.

Example 11.
1. If $(G, *)$ is a group, then the identity map $f : G \to G$ given by $f(x) = x$ is a homomorphism from $(G, *)$ to $(G, *)$.
2. If $(G, *)$ and $(H, \bigstar)$ are groups and H has identity e_H, then $f : G \to H$ given by $f(x) = e_H$ for all $x \in G$ is a homomorphism.
3. The function $f : \mathbb{Z} \to \mathbb{R}$ given by $f(x) = 2x$ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{R}, +)$, since
$$f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$$
This also works if we replace $\mathbb{Z}$ by $\mathbb{Q}$ or $\mathbb{R}$.
4. $f : (\mathbb{Z}, +) \to (\{0, 1\}, +_{\text{mod}2})$ given by $f(x) = x \bmod 2$ is a homomorphism.
5. $f : (\mathbb{R}\backslash\{0\}) \to (\mathbb{R}\backslash\{0\})$ given by $f(x) = 2x$ is *not* a homomorphism from $(\mathbb{R}\backslash\{0\}, \cdot)$ to $(\mathbb{R}\backslash\{0\}, \cdot)$ - for example, $f(2 \cdot 2) = f(4) = 8$, but $f(2) \cdot f(2) = 4 \cdot 4 = 16$, so $f(2 \cdot 2) \neq f(2) \cdot f(2)$.

Question 3.1. Let $f : G \to H$ be a homomorphism from $(G, *)$ to $(H, \bigstar)$. Say $e \in G$ and $e' \in H$ are the respective identity elements of the groups. Show that $f(e) = e'$.

(Hint: from Question 4, we know there is only one identity for H - so it is enough to show that $f(e)$ is an identity for H, that is, $f(e) \bigstar a = a = a \bigstar f(e)$ for all $a \in H$.)

Definition 12. Let $(G, *)$ be a group. $(H, \bigstar)$ is a *subgroup* of $(G, *)$ if $(H, \bigstar)$ is a group, $H \subseteq G$, and $a \bigstar b = a * b$ for all $a, b \in H$ (so $\bigstar = *$ on H).

Example 13.
1. If $(G, *)$ is a group, then $(G, *)$ is a subgroup of itself, as is $(\{e\}, *)$ where e is the identity element.
2. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, which is a subgroup of $(\mathbb{R}, +)$
3. $(\mathbb{Z}\backslash\{0\}, \cdot)$ is a subgroup of $(\mathbb{Q}\backslash\{0\}, \cdot)$, which is a subgroup of $(\mathbb{R}\backslash\{0\}, \cdot)$
4. If $2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ is the set of all even numbers, then $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Question 3.2. Why is $(\{0,1\}, +_{\text{mod2}})$ not a subgroup of $(\mathbb{Z}, +)$?

Definition 14. The *kernel* of a group homomorphism $f : (G, *) \to (H, \bigstar)$ is the set $\ker(f) = \{x \in G : f(x) = e_H\}$, where e_H is the identity of $(H, \bigstar)$.

Fact 15. If $f : (G, *) \to (H, \bigstar)$ is a homomorphism, then $(\ker(f), *)$ is a subgroup of $(G, *)$.

Example 16.
1. If $f : (G, *) \to (G, *)$ is $f(x) = x$, then $\ker(f) = \{e\}$ where e is the identity. If $f(x) = e$ for all $x \in G$, then $\ker(f) = G$.
2. Let $f : (\mathbb{Z}, +) \to (\{0,1\}, +_{\text{mod2}})$ be $f(x) = x \bmod 2$. Then $f(x) = 0$ if and only if $x = 0 \bmod 2$, if and only if $x = 2y$ for some $y \in \mathbb{Z}$, that is, x is even. So $\ker(f) = \{2y : y \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \text{ is even}\} = \{\cdots -6, -4, -2, 0, 2, 4, 6 \dots\}$.

Now we have a few more tools, let's finish with some more exercises.

4 Exercises Part 2

Question 4.1. Suppose $(G, *)$ has subgroup $(H, *)$. Prove the identity of $(G, *)$ is in H. What is the identity of $(H, *)$?

Question 4.2. Let $(G, *)$ and $(H, \bigstar)$ be groups. Show that (no matter which groups these are) there is a homomorphism between G and H.

Question 4.3. Suppose that $f : (G, *) \to (H, \bigstar)$ is a homomorphism between groups. Show that $(\ker(f), *)$ is a subgroup of $(G, *)$.

(Hint: since $\ker(f) \subseteq G$ *and uses the same binary function* $*$*, you only need to show that* $(\ker(f), *)$ *is a group - that is, closed, associative, and has identity and inverses. For example, for closure, you have to show why* $a, b \in \ker(f)$ *implies* $a * b \in \ker(f)$*, and so on.)*

The following notation will be helpful for the next question:

Notation 4.1. Let $(G, *)$ be a group with identity e. For $n > 0$ an integer, let $a^n = a * a * \cdots * a$ (where a is 'multiplied' n times). Let $a^0 = e$. Let $a^{-n} = (a^{-1})^n$. These satisfy all the normal rules of exponentiation - in particular, that $a^{m+n} = a^m * a^n$ for all $m, n \in \mathbb{Z}$).

Question 4.4. Let $(G, *)$ be a finite group with identity e.

1. Let $a \in G$. Explain why there exist integers $m > n \geqslant 1$ such that $a^m = a^n$.
2. Let $a \in G$. Explain why there is an integer $k \geqslant 1$ such that $a^k = e$.
3. Let $k \geqslant 1$ be the minimal integer such that $a^k = e$. Let $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. Show that $(\langle a \rangle, *)$ is a subgroup of $(G, *)$ of size k.
4. Show that $(\langle a \rangle, *)$ is Abelian.

Definition 17. Let $(G, *)$ and $(H, \bigstar)$ be groups. An *isomorphism* from $(G, *)$ to $(H, \bigstar)$ is a homomorphism $f : (G, *) \to (H, \bigstar)$ which is also a bijection. If such an isomorphism exists, we say $(G, *)$ and $(H, \bigstar)$ are *isomorphic*.

Essentially, two groups are isomorphic if they are 'the same' group, up to renaming the elements of G. That is, they have exactly the same structure.

Question 4.5. Let $f : (G, *) \to (H, \bigstar)$ be an isomorphism of groups. Prove that f^{-1} is an isomorphism from $(H, \bigstar)$ to $(G, *)$.

Question 4.6. Let $(G, *)$ be a finite group, and $a \in G$. Show that if $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, then there is some $k \geqslant 1$ an integer such that $(\langle a \rangle, *)$ is isomorphic to $(C_k, +_{\bmod k})$.

Question 4.7. Let $(G, *)$ be a group. The *centre* of $(G, *)$ is $Z(G) = \{x \in G : \text{ for all } y \in G,\ xy = yx\}$. Prove that $(Z(G), *)$ is a subgroup of G, and that $(Z(G), *)$ is Abelian.

Question 4.8. Do the tricky question from the first set of exercises, if you skipped it before!