BUILDING GROUPS: FROM MAGMAS TO GROUPS
SUPPLEMENTARY MATERIAL FOR SEPTEMBER 8, 2025

DR. MCNEW

1. Binary Operations and Closure

In mathematics, we constantly combine objects: we add numbers, compose functions, multiply matrices. At its most basic level, this is the idea of a **binary operation**.

A binary operation on a set S is simply a rule that takes any two elements from S and produces another element. We often denote this with symbols like $+$, $\cdot$, $*$, or $\circ$.

For example:

- Addition on integers: $3 + 5 = 8$
- Matrix multiplication on 2×2 matrices: $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$
- Function composition: $(f \circ g)(x) = f(g(x))$

The crucial question is: when we combine two elements from our set, do we always get another element from the same set? This property is called **closure**.

1.1. Operation Tables.

For finite sets, we can completely describe a binary operation using an **operation table** (also called a **Cayley table**). In such a table:

- The **rows** represent the **first** element of the operation
- The **columns** represent the **second** element of the operation
- To find $a * b$, look at the row labeled a and the column labeled b

For example, in this table:

$*$	x	y
x	y	x
y	x	y

We can read: $x * x = y$, $x * y = x$, $y * x = x$, and $y * y = y$.

2. Magmas: The Most Basic Algebraic Structure

Definition 1. A **magma**[1] is a set M together with a binary operation $* : M \times M \to M$. We denote this structure as $(M, *)$.

That's it! A magma requires only that we can combine any two elements to get another element in the set (closure). No other restrictions apply.

Example 1.

- The set $\{1, 2, 3, 4\}$ with operation $a \circ b = \lceil a/b \rceil$ (division, take ceiling). For example, $3 \circ 2 = \lceil 3/2 \rceil = \lceil 1.5 \rceil = 2$.

$\circ$	1	2	3	4
1	1	1	1	1
2	2	1	1	1
3	3	2	1	1
4	4	2	2	1

[1] Magmas are sometimes called **groupoids**, though this term has different meanings in other areas of mathematics.

- $(\mathbb{R}, *)$ where $a * b = a^b$ (exponentiation). Note this isn't even associative!
- **Non-example:** The set $\{1, 2, 3\}$ with ordinary subtraction. This is *not* a magma because $1 - 3 = -2 \notin \{1, 2, 3\}$. The operation is not closed!

Remark 1. Magmas can be quite "wild" - the operation might not be associative, there might be no identity element, and elements might not have inverses.

3. The Hierarchy of Algebraic Structures

Now let's see the big picture of how we can add structure to magmas:

$$\begin{tikzcd}
& \boxed{\text{Magma}} \arrow[dl, "+\text{ associativity}"'] \arrow[dr, "+\text{ division}"] & \\
\boxed{\text{Semigroup}} \arrow[d, "+\text{ identity}"'] & & \boxed{\text{Quasigroup}} \arrow[d, "+\text{ identity}"] \\
\boxed{\text{Monoid}} \arrow[dr, "+\text{ inverses}"'] & & \boxed{\text{Loop}} \arrow[dl, "+\text{ associativity}"] \\
& \boxed{\text{Group}} &
\end{tikzcd}$$

As we can see, there are two main paths from magmas to groups: one emphasizing associativity first, the other emphasizing division properties first.

4. Path 1: Emphasizing Associativity

4.1. Semigroups: Adding Associativity.

Definition 2. A **semigroup** is a magma $(S, *)$ where the operation $*$ is associative. That is, for all $a, b, c \in S$:

$$(a * b) * c = a * (b * c)$$

Associativity is crucial because it allows us to write expressions like $a * b * c * d$ without worrying about parentheses.

Example 2.

- $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ are both semigroups.
- $(\mathbb{N}, -)$ is not a semigroup: $(5 - 3) - 2 = 0$ but $5 - (3 - 2) = 4$.
- The set of all 2×2 matrices with real entries under matrix multiplication forms a semigroup.
- The set of all functions from $\mathbb{R}$ to $\mathbb{R}$ under composition is a semigroup.

4.2. Monoids: Adding an Identity Element.

Definition 3. A **monoid** is a semigroup $(M, *)$ that has an **identity element** $e \in M$. That is, there exists $e \in M$ such that for all $a \in M$:

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

Proposition 1. If a monoid has an identity element, then it is unique.

Proof. Suppose e and e' are both identity elements. Then:

$$e = e * e' = e'$$

where the first equality uses the fact that e' is an identity, and the second uses the fact that e is an identity. ☐

Example 3.

- $(\mathbb{N} \cup \{0\}, +)$ is a monoid with identity 0.
- $(\mathbb{N}, \cdot)$ is a monoid with identity 1.
- $(\mathbb{N}, +)$ is not a monoid because $\mathbb{N}$ doesn't contain 0.
- The set of all $n \times n$ matrices under multiplication is a monoid with identity I_n.
- The set of strings over an alphabet under concatenation is a monoid with the empty string as identity.

5. Path 2: Emphasizing Division

5.1. Quasigroups: Adding Division.

Definition 4. A **quasigroup** is a magma $(Q, *)$ where for all $a, b \in Q$, the equations $a * x = b$ and $y * a = b$ have unique solutions in Q.

In other words, we can always "divide" - given any a and b, there's a unique "left quotient" x such that $a * x = b$, and a unique "right quotient" y such that $y * a = b$.

Example 4. Consider the set $\{a, b, c\}$ with operation:

$*$	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

This is a quasigroup (each element appears exactly once in each row and column), but it's not associative: $(a * b) * a = a * a = b$ while $a * (b * a) = a * c = c$.

Remark 2. A key property: A finite magma is a quasigroup if and only if each element appears exactly once in each row and each column of its operation table (called a **Latin square**).

5.2. Loops: Quasigroups with Identity.

Definition 5. A **loop** is a quasigroup with an identity element.

Example 5 (Exercise)**.** Try to construct an example of a loop that is not a group (i.e., a loop that is not associative).

Hint: The smallest such example has 5 elements. You'll need to carefully construct an operation table where:

- One element acts as the identity
- Each element appears exactly once in each row and column (Latin square property)
- You can find specific elements a, b, c such that $(a * b) * c \neq a * (b * c)$

This exercise demonstrates that finding non-associative loops requires careful construction!

Remark 3. Loops are "almost groups" - they have unique division and an identity, but they might not be associative. Finding simple examples of non-associative loops requires some care!

6. Groups: Where Both Paths Meet

Definition 6. A **group** is a monoid where every element has an inverse. That is, for each $a \in G$, there exists $a^{-1} \in G$ such that:

$$a * a^{-1} = a^{-1} * a = e$$

where e is the identity element.

Definition 7. A **group** is an associative loop.

Both definitions give us the familiar four group axioms:

(1) **Closure**: For all $a, b \in G$, we have $a * b \in G$.
(2) **Associativity**: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
(3) **Identity**: There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
(4) **Inverses**: For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Theorem 1. Every group is automatically a quasigroup.

Proof. Let $(G, *)$ be a group and let $a, b \in G$. We need to show that the equations $a * x = b$ and $y * a = b$ have unique solutions.

For $a * x = b$: Multiply both sides on the left by a^{-1} to get $a^{-1} * (a * x) = a^{-1} * b$. By associativity, $(a^{-1} * a) * x = a^{-1} * b$, so $e * x = a^{-1} * b$, giving $x = a^{-1} * b$. This solution is unique because if $a * x_1 = a * x_2 = b$, then multiplying by a^{-1} on the left gives $x_1 = x_2$.

Similarly, for $y * a = b$: We get $y = b * a^{-1}$. □

Example 6.

- $(\mathbb{Z}, +)$ is a group with identity 0 and inverses $a^{-1} = -a$.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group with identity 1 and inverses $a^{-1} = 1/a$.
- $(\mathbb{N}, +)$ is not a group because natural numbers don't have additive inverses.
- $(\mathbb{Z}, \cdot)$ is not a group because most integers don't have multiplicative inverses in $\mathbb{Z}$.

7. Why Each Property Matters

Let's see what happens when we remove each key property:

7.1. Without Closure.
If we don't have closure, we can't guarantee that combining elements stays within our set. This breaks the entire algebraic structure.

7.2. Without Associativity.
We lose the ability to unambiguously parse expressions like $a * b * c$. Many important theorems (like the uniqueness of identity and inverses) rely on associativity. We get structures like loops, which can be interesting but lack the predictable behavior of groups.

7.3. Without Identity.
We can't define what it means for an element to have an inverse. Many elements might have "partial inverses" but no true inverse. We get structures like semigroups.

7.4. Without Inverses.
We lose the ability to "undo" operations. For instance, $(\mathbb{N}, +)$ is a nice monoid, but we can't solve equations like $x + 3 = 1$ within the natural numbers. More generally, without inverses we cannot solve linear equations $a * x = b$ and $y * a = b$ for arbitrary elements a and b.

8. Extended Hierarchy

The story doesn't end with groups. One important extension is:

$$\begin{tikzcd} \boxed{\text{Groups}} \arrow[d, "+\text{ commutativity}"] \\ \boxed{\text{Abelian Groups}} \end{tikzcd}$$

- **Abelian groups**: Groups with commutative operations ($a * b = b * a$)

This adds another layer of structure, leading to even richer mathematical theory that we'll explore later in the course.

9. Connection to Our Course

The approach taken here—building groups from magmas through intermediate structures—differs significantly from your textbook's presentation in Section 3.1. Understanding both perspectives will deepen your appreciation of group theory.

9.1. **Textbook Approach vs. This Hierarchical Approach. Textbook (Section 3.1):** The textbook introduces groups directly by stating the four axioms (closure, associativity, identity, inverses) and immediately exploring examples like symmetric groups, matrix groups, and modular arithmetic. This approach emphasizes:

- Immediate focus on the complete group structure
- Rich examples that motivate the axioms through symmetry and transformations
- Quick transition to computational aspects and specific group families

This Supplementary Approach: We've built groups gradually by starting with magmas and adding one property at a time. This hierarchical perspective emphasizes:

- Understanding why each axiom is necessary by seeing what happens without it
- Recognizing that groups are the convergence of two different mathematical philosophies (associativity-first vs. division-first)
- Appreciating intermediate structures that arise naturally in other areas of mathematics

9.2. **Connecting the Approaches.** Both approaches illuminate different aspects of group theory:

- When you encounter the symmetric groups S_n in the textbook, remember they're not just examples of groups—they're examples where the quasigroup property (unique division) is automatically satisfied because every group is a quasigroup.
- The matrix groups like $GL_n(\mathbb{R})$ showcase how closure isn't always obvious—you need to verify that the product of invertible matrices is invertible, highlighting why closure is a fundamental requirement.
- The modular arithmetic groups $\mathbb{Z}_n$ under addition demonstrate the "associativity-first path" perfectly: addition is naturally associative, zero provides identity, and negatives give inverses.
- When the textbook discusses binary operations and their properties, you'll recognize these as the foundational concepts we used to define magmas.

9.3. **Looking Ahead.** As we progress through the course, this hierarchical understanding will prove valuable:

- **Subgroups:** When we study subgroups, we're looking at subsets that are themselves groups—they inherit the magma structure but must satisfy all four group axioms within the subset.

- **Homomorphisms:** These preserve the binary operation structure, connecting different groups while maintaining their algebraic properties.
- **Quotient Groups:** These create new groups from existing ones, and understanding the underlying magma structure helps clarify why the construction works.
- **Isomorphisms:** When two groups are isomorphic, they share the same algebraic structure—the same "shape" in our hierarchy.

Remember this hierarchy when proving theorems about groups: we're using *all* the axioms. When seeking counterexamples, we often find them in structures that satisfy some but not all group properties—the intermediate structures we've studied today.

10. Exercises

(1) **Magma Construction:** Consider the set $\{a, b, c\}$. Create an operation table that makes this set a magma but *not* a semigroup (i.e., the operation is not associative). Verify your answer by finding specific elements where $(x * y) * z \neq x * (y * z)$.

(2) **Quasigroup Analysis:** Show that the following operation table defines a quasigroup by verifying that each element appears exactly once in each row and column:

$*$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

Is this quasigroup also a group? Explain your reasoning.

(3) **Hierarchy Navigation:** For each of the following algebraic structures, determine which level of our hierarchy it belongs to and explain why it cannot be classified higher:
  (a) $(\mathbb{Z}, -)$ (integers under subtraction)
  (b) $(\mathbb{N}, +)$ (natural numbers under addition)
  (c) $(\mathbb{Q}^*, \cdot)$ (nonzero rationals under multiplication)
  (d) The set $\{0, 1\}$ under the operation $a * b = \max(a, b)$

(4) **Two Paths to Groups:** Explain why both the "associativity-first" path (Magma $\rightarrow$ Semigroup $\rightarrow$ Monoid $\rightarrow$ Group) and the "division-first" path (Magma $\rightarrow$ Quasigroup $\rightarrow$ Loop $\rightarrow$ Group) are necessary. That is, why can't we reach all groups by following only one of these paths?

(5) **Operation Table Challenge:** Construct the smallest possible loop that is *not* a group. (Hint: You'll need at least 5 elements.) Your operation table should satisfy:
  - One element acts as the identity
  - Each element appears exactly once in each row and column
  - The operation is not associative

  Verify that your construction works by showing specific elements where associativity fails.

(6) **Textbook Connection:** Review Section 3.1 of your textbook. Choose one of the group examples presented there (such as S_3, $GL_2(\mathbb{R})$, or $\mathbb{Z}_n$) and explain how it illustrates both paths in our hierarchy. Specifically, show how this group satisfies the properties from both the associativity-first and division-first paths.