Chapter I — §1 Monoids

Everything you wanted to say about $(\_ \cdot \_)$ but were afraid to parenthesize

Slides generated from your chapter outline (no exercises)

August 20, 2025

Section roadmap

Binary laws of composition

What is a "law of composition"?

- A **law of composition** on a set S is just a map

$$\mu : S \times S \longrightarrow S, \qquad (x, y) \mapsto \mu(x, y) = x \cdot y.$$

- We'll also write xy for $x \cdot y$. When commutativity holds, the additive notation $x + y$ is common.
- **Associative** means $(xy)z = x(yz)$ for all $x, y, z \in S$.
- A **unit (identity)** is an element $e \in S$ with $ex = xe = x$ for all $x \in S$.
- A set with an associative law and a unit is a monoid. (Semigroup = associative, *no* promise of a unit.)

First date with associativity

- Associativity lets us unambiguously write $x_1 x_2 \cdots x_n$ without a forest of parentheses.
- Convention: the **empty product** is e (the unit).
- When the operation is commutative, we may reindex and regroup at will. When not: choose your parentheses wisely.

Cheeky transition
Parentheses are like seatbelts: you only notice them when something non-associative happens.

Definition and basic properties

Definition: monoid

Monoid
A **monoid** is a triple $(M, \cdot, e)$ where M is a set, $\cdot$ is an associative law of composition on M, and e is a unit for $\cdot$.

- If $xy = yx$ for all x, y, the monoid is **commutative** (often written additively as $(M, +, 0)$).
- Elements $u \in M$ with a two-sided inverse are called **units**. The set of units $M^\times$ forms a **group**.

Uniqueness of the unit

Proposition
If e and e' are units in M, then $e = e'$.

Proof (blink-and-you-miss-it)
$e = e \cdot e' = e'$.

Transition
Plot twist: there can be *many* inverses in life, but in a monoid the identity is strictly monogamous.

Left/right units and inverses

- A **left unit** satisfies $ex = x$ for all x; a **right unit** satisfies $xe = x$ for all x.
- If a left unit and a right unit both exist in M, then they are equal and hence the (two-sided) unit.
- **Inverse uniqueness:** if $xu = ux = e$ and $xv = vx = e$, then $u = v$.

Proof sketch
$u = ue = u(xv) = (ux)v = ev = v$.

Transition
Two-sided inverses: because who wants commitment only on weekdays?

Powers and laws of exponents

Let $(M, \cdot, e)$ be a monoid and $x \in M$.

- Define $x^0 := e$, $x^{n+1} := x^n x$ for $n \geq 0$ (and $x^1 = x$).
- **Exponent laws**: for all $m, n \in \mathbb{N}$:

$$x^{m+n} = x^m x^n, \qquad (x^m)^n = x^{mn}.$$

- If $xy = yx$, then $(xy)^n = x^n y^n$.

Transition
Yes, your high-school exponent rules secretly assumed a monoid the whole time. Math teachers are sneaky.

Examples and non-examples

Classic examples

- $(\mathbb{N}, +, 0)$ and $(\mathbb{Z}, +, 0)$.
- $(\mathbb{N}, \times, 1)$ (caution: 0 is not a unit).
- $M_n(R)$ with matrix multiplication and I_n.
- $\mathrm{End}(S)$: all functions $S \to S$ under composition with id_S.
- Strings Σ^* under concatenation, unit the empty word ε.
- $(\mathbb{R}_{\geq 0}, \max, 0)$, $(\mathbb{R} \cup \{-\infty\}, \max, -\infty)$ (idempotent monoids).
- Boolean monoids: $(\{0, 1\}, \vee, 0)$ and $(\{0, 1\}, \wedge, 1)$.

Non-examples & cautionary tales

- $(\mathbb{R}, -, 0)$ with subtraction is *not* associative.
- $(\mathbb{R}, \cdot, 1)$ *is* a monoid, but $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ is a *group*; note how units "peel off" into a nicer object.
- The set of $n \times n$ *singular* matrices is not a monoid under multiplication (no unit).

Transition
If it fails associativity, it's not a phase—it's a different algebraic object.

Submonoids and generation

Submonoids

Definition
A subset $N \subseteq M$ is a **submonoid** if $e \in N$ and $xy \in N$ whenever $x, y \in N$.

- Equivalently: close under the operation and contain the unit.
- Warning: closure under inverses is *not* required (that would make it a subgroup of $M^\times$ if all elements are units).

Generated submonoids

Definition
Given $S \subseteq M$, the **submonoid generated by** S, written $\langle S \rangle$, is the intersection of all submonoids containing S.

- Concretely: $\langle S \rangle$ consists of all finite products $s_1 s_2 \cdots s_k$ with $k \geq 0$ and $s_i \in S$ (empty product allowed $\Rightarrow e \in \langle S \rangle$).
- In a commutative monoid, we may speak of *monomials* in S.
- If S is finite, say $S = \{x_1, \ldots, x_r\}$, write $\langle x_1, \ldots, x_r \rangle$.

Transition
From "some elements I like" to "everything I can build from them" — the LEGO principle of algebra.

Units, cancellation, and idempotents

Group of units

Definition
An element $u \in M$ is a **unit** if there exists $v \in M$ with $uv = vu = e$.

- The set $M^\times$ of all units is closed under multiplication and inversion, so $(M^\times, \cdot, e)$ is a group.
- Example: in $M_n(R)$, $M^\times$ is the general linear group $\mathrm{GL}_n(R)$.

Cancellation vs. invertibility

- **Left-cancellative**: $ax = ay \Rightarrow x = y$; **right-cancellative**: $xa = ya \Rightarrow x = y$.
- If a is a unit, then both left and right cancellation by a hold.
- The converse can fail in general monoids (cancellation does not imply invertibility), but holds in groups.

Transition
Being cancellative is like being persuasive; having an inverse is like having receipts.

Idempotents and absorbing elements

- $e \in M$ is **idempotent** if $e^2 = e$ (every identity is idempotent, but not every idempotent is an identity).
- **Absorbing element** $0 \in M$: $0x = x0 = 0$ for all x (e.g. 0 under multiplication in $\mathbb{N}$).
- In idempotent commutative monoids (a.k.a. join-semilattices), $x + y$ behaves like set-theoretic union or logical OR.

Finite products and indexing

Products over finite index sets

- If only finitely many terms are $\neq e$, define $\prod_{i \in I} x_i$ by choosing any order (associativity ensures unambiguity; commutativity allows reordering freely).
- For functions $f : I \times J \to M$ with finite support, we have the "Fubini for finite products"

$$\prod_{i \in I} \prod_{j \in J} f(i,j) = \prod_{(i,j) \in I \times J} f(i,j) = \prod_{j \in J} \prod_{i \in I} f(i,j).$$

Transition
Reindex responsibly. Associativity is your seatbelt; commutativity is cruise control.

Morphisms and quotients

Monoid homomorphisms

Definition
A **homomorphism** $f : (M, \cdot, e) \to (N, \star, 1)$ is a map with $f(x \cdot y) = f(x) \star f(y)$ and $f(e) = 1$.

- Images of units are units: if $u \in M^\times$ then $f(u) \in N^\times$.
- Composition of homomorphisms is a homomorphism; the identity map is a homomorphism.

Congruences and quotients

- A **monoid congruence** $\sim$ is an equivalence relation on M compatible with multiplication: $x \sim x'$, $y \sim y' \Rightarrow xy \sim x'y'$.
- The quotient $M/\sim$ inherits a monoid structure.
- Any homomorphism $f : M \to N$ yields a congruence $x \sim y \iff f(x) = f(y)$ (the *kernel congruence*).

First isomorphism theorem (monoids)
$M/\sim \;\cong\; \mathrm{Im}(f)$ where $\sim$ is the kernel congruence of f.

Transition
Same plot as in group theory, but with a slightly different side character named "congruence."

Free monoids and presentations

Free monoids

- For an alphabet Σ, the **free monoid** Σ^* consists of all finite words in Σ under concatenation; unit is the empty word ε.
- **Universal property:** any function $g : \Sigma \to (M, \cdot, e)$ extends uniquely to a homomorphism $\widehat{g} : \Sigma^* \to M$ with $\widehat{g}(\sigma_1 \cdots \sigma_k) = g(\sigma_1) \cdots g(\sigma_k)$.

Presentations

- A monoid can be given by **generators and relations**: $M \cong \Sigma^*/\equiv$ where $\equiv$ is the smallest congruence forcing chosen relations.
- Example: the commutative monoid on generators x, y is $\langle x, y \mid xy = yx \rangle$.

Transition
Presentations: because writing down every element individually is a terrible hobby.

Constructions and actions

Direct products and substructures

- The product of monoids $(M, \cdot, e)$ and $(N, \star, 1)$ is $M \times N$ with $(x, a)(y, b) = (xy, ab)$ and identity $(e, 1)$.
- Submonoids and homomorphic images behave as expected under products.

Monoid actions

Definition
An **action** of a monoid $(M, \cdot, e)$ on a set S is a map $M \times S \to S$ satisfying $e \cdot s = s$ and $x \cdot (y \cdot s) = (xy) \cdot s$.

- Example: $\mathbb{N}$ acts on S by iterating a function $f : S \to S$, via $n \cdot s = f^{\circ n}(s)$.
- Every action corresponds to a homomorphism $M \to \mathrm{End}(S)$.

Transition
Actions: when monoids stop being polite and start getting real (on sets).

Checklists and pitfalls

How to verify a monoid in the wild

1. Specify the underlying set M.
2. Specify the binary operation clearly.
3. Prove associativity.
4. Exhibit a unit and verify two-sidedness.
5. (Optional) Identify units $M^\times$, submonoids, and natural homomorphisms.

Common pitfalls

- Assuming a left identity is automatically a right identity (true in presence of associativity, but needs a proof).
- Using cancellation without confirming invertibility or appropriate hypotheses.
- Forgetting the empty product convention when proving product identities.

Final transition to next section
If every element has an inverse, congratulations—you've unlocked the DLC: **Groups**.
Coming up next!