Category Theory 2022

TalICATS

February 20, 2022

Rappels from lecture 3

We have seen what is (not) a monoid:

Definition

A monoid consists of a set M equipped with

- a binary operation $m : M \times M \to M$, sending (x, y) to $m(x, y) = x \cdot y$, which is associative: $x(yz) = (xy)z$ and
- a neutral element 1, i.e. such that $1 \cdot x = x \cdot 1 = x$ for each $x \in M$.

A monoid can be commutative: for example, sets of numbers ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with respect to either sum or product; or the set $(\{1, e\}, \cdot)$ where $e \cdot e = e$) or noncommutative: for example, the set of rotations in 3D space, or the set of all functions $\mathbb{N} \to \mathbb{N}$ (or any set, for that matter...) both with respect to functional composition.

The monoid of sumsets

Exercise

- Let $(M, +, 0)$ be a monoid; let 2^X be the set of all subsets of X. Define on 2^X the operation

$$U * V = \{u + v \mid u \in U, v \in V\}.$$

  Show that $(2^X, *, \{0\})$ is a monoid. The set $U * V$ is called the sumset of U, V.

- Let X be any set, and 2^X the set of all its subsets; define the operation of symmetric difference:

$$U \triangle V = (U \cup V) \setminus (U \cap V).$$

  Is this a monoid? Who is the identity element for $\triangle$?

Submonoids

Definition

Let $\mathbf{M} = (M, \cdot, 1)$ be a monoid. A submonoid N of M is a subset of M such that

- if $n, n' \in N$, then $n \cdot n' \in N$;
- $1 \in N$.

Every monoid M has at least two submonoids, $\{1\}$ and the whole M. A submonoid $N \subseteq M$ that is neither $\{1\}$ nor M is called *nontrivial*. The submonoid $M \subseteq M$ is called *improper*. All other submonoids are called *proper*.

We write shortly $N \leq (M, \cdot, 1)$ or even shorter, $N \leq M$ when the operation can be left unnamed.

Examples

- Let $n \in \mathbb{N}$, define $\mathbb{N}_{\geq n} = \{a \in \mathbb{N} \mid a \geq n\}$. Then, $\mathbb{N}_{\geq n} \cup \{0\} \leq (\mathbb{N}, +, 0)$ is a submonoid.
- In a similar fashion, $\mathbb{N}_{\geq n} \cup \{1\} \leq (\mathbb{N}, \cdot, 1)$ is a submonoid.
- Let $N, K \subseteq M$ be submonoids of the same M; then $N \cap K$ is a submonoid of M.
- Actually something stronger is true:

Proposition

Let I be any set, and let $\{N_i \mid i \in I\}$ be a family of submonoids of the same M; then $\bigcap_{i \in I} N_i \leq M$.

Generated submonoids

Unions of submonoids, on the other hand, fail dramatically to be submonoids. For example, consider the submonoid $\{1, 2, 4, 8, \ldots, 2^p, \ldots\}$ and the submonoid $\{1, 3, 9, \ldots, 3^q, \ldots\}$ in $(\mathbb{N}, \cdot)$; the set theoretic union does not contain $3 \cdot 2 = 6$.

This leads to the following

Definition

Let $S \subseteq M$ be a subset of a monoid $\mathbf{M}$. The submonoid of M generated by S is the smallest submonoid of M containing S, denoted $\langle S \rangle$.

Using the above proposition, we can show that $\langle S \rangle$ coincides with the intersection $\bigcap \{N \leq M \mid S \subseteq N\}$.

Generated submonoids

Proposition

Let M be a monoid and $S \subseteq M$. Then,

$$\langle S \rangle = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}, \forall i = 1, \dots, n, x_i \in S\} \qquad (\star)$$

where $x_1 x_2 \dots x_n$ is the n-fold product of elements $x_1, \dots, x_n$, and we adopt the convention that when $n = 0$ the product is empty, i.e. equal to 1_M.

Proof.
It suffices to show that N as defined in $(\star)$ coincides with the intersection $\bigcap\{N \leq M \mid S \subseteq N\}$. In order to do this, we prove

- that N is a submonoid of M;
- that N is contained in every submonoid containing S. $\square$

Examples

Let $\mathbf{N} = (\mathbb{N}, \cdot, 1)$ and $S = \{2, 3, 4\}$. Then, $\langle S \rangle$ coincides with the set

$$\{2^p 3^q 4^r \mid p, q, r \in \mathbb{N}\},$$

which in turn is the set $\{2^p 3^q \mid p, q \in \mathbb{N}\}$.

The submonoid of $(\mathbb{N}, \cdot)$ generated by $\{2\}$ is the set of all consecutive powers of 2. More generally, $\langle n \rangle = \{n^p \mid p \geq 0\}$.

Let $\mathbf{N} = (\mathbb{N}, +, 1)$ and $S = \{2, 3, 4\}$. Then, $\langle S \rangle$ coincides with the set

$$\{2p + 3q + 4r \mid p, q, r \in \mathbb{N}\}.$$

Let A be any set, and $(A^A, \circ)$ the monoid of endofunctions on A. For each $a \in A$ consider the function $f_a : A \to A$ that is constant at a. What is the submonoid K of A^A generated by the set $S = \{f_a \mid a \in A\}$?

Cyclic submonoids

A submonoid $N \leq M$ is cyclic is there exists an element $x \in N$ such that $N = \langle x \rangle$. The submonoid $\langle n \rangle \leq (\mathbb{N}, \cdot)$ is cyclic.

A monoid M is cyclic if $M = \langle a \rangle$. The additive monoid $(\mathbb{N}, +)$ is cyclic: $\mathbb{N} = \langle 1 \rangle$.

Exercise

Are these (sub)monoids cyclic?

- $(\mathbb{N}, \cdot, 1)$;
- $(A^A, \circ)$;
- $K = \langle \{ f_a \mid a \in A \} \rangle$ as above;
- $\{1, e\}$ where $ee = e$.

Monoid homomorphism

Definition

Let $\mathbf{M}, \mathbf{N}$ be two monoids; a monoid homomorphism $f : \mathbf{M} \to \mathbf{N}$ is a function $f : M \to N$ with the property that

- $f(x \cdot_M y) = f(x) \cdot_N f(y)$;
- $f(1_M) = 1_N$.

A simple remark: the inclusion of a submonoid in the ambient monoid is a homomorphism.

Monoid homomorphism

Standard nomenclature in abstract algebra:

- an endomorphism (Gr. /ένδον/) a homomorphism of M into itself;
- an isomorphism (Gr. /ίσος/) a bijective homomorphism;
- an automorphism (Gr. /αυτός/) an endomorphism which is also an automorphism.

Examples of monoid homomorphisms

The map

$$p : \mathbb{Z} \to \{1, -1\}$$

defined sending $z \mapsto (-1)^z$ is a homomorphism of monoids from $(\mathbb{Z}, +, 0)$:

- Certainly, $p(0) = (-1)^0 = 1$;
- $p(a + b) = (-1)^{a+b} = (-1)^a(-1)^b = p(a)p(b)$.

The map $s : (\mathbb{Z} \setminus \{0\}, \cdot, 1) \to \{-1, 1\}$ defined sending $z \mapsto \frac{z}{|z|}$ is a monoid homomorphism.

Examples of monoid homomorphisms

Let B be a set, and $A \subseteq B$ a subset. Define the function

$$\psi : 2^A \to 2^B : (U \subseteq A) \mapsto (U \subseteq B)$$

using the transitivity of the partial order $\subseteq$ on 2^B. Then,

- ψ is a monoid homomorphism $(2^A, \cup) \to (2^B, \cup)$, because $\psi(X \cup Y) = X \cup Y = \psi(X) \cup \psi(Y)$ and $\psi(\varnothing) = \varnothing$;
- ψ is a homomorphism of semigroups $(2^A, \cap) \to (2^B, \cap)$, because $\psi(X \cap Y) = X \cap Y = \psi(X) \cap \psi(Y)$;
- but ψ is not always a monoid homomorphism; why?

Classify monoid homomorphisms

Theorem

Let M be a monoid; the set of homomorphisms

$$\hom((\mathbb{N},+,0),M) = \{f : (\mathbb{N},+,0) \to M \mid f \text{ is a homomorphism}\}$$

contains as many elements as there are elements in M.

Proof.
Let $f : \mathbb{N} \to M$ be a homomorphism of monoids; since every element of $\mathbb{N}$ can be obtained as the sum $1 + \cdots + 1 = n$ iterated n times, one has that

$$f(n) = f(1 + \cdots + 1) = f(1) \dots f(1) = f(1)^n$$

in M. Conversely, let $x \in M$ be a fixed element; then $n \mapsto x^n$ defines a monoid homomorphism (mapping to the cyclic submonoid $\langle x \rangle$ generated by x).

This sets up a bijection $\hom((\mathbb{N},+,0),M) \cong M$. $\square$

Classify monoid homomorphisms

In the particular case where $M = (\mathbb{N}, \cdot, 1)$ we obtain as a corollary that every monoid homomorphism $(\mathbb{N}, +) \to (\mathbb{N}, \cdot)$ is an exponential map:

- on one side, every map $e_n : k \mapsto k^n$ is a monoid homomorphism;
- on the other side, all monoid homomorphisms are of this form: retracing the above argument in this special case we get that if $f : (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$ is a homomorphism, then $f = e_{f(1)}$.

Classify monoid homomorphisms

Let's classify the homomorphisms $(\mathbb{N}, \cdot) \to M$:

Theorem

Every homomorphism of monoids $h : (\mathbb{N}, \cdot) \to M$ is uniquely determined by the image of all prime numbers,

$$h(2), h(3), h(5), \ldots, h(4283), \ldots.$$

Proof.
Let $h : (\mathbb{N}, \cdot) \to M$ be a homomorphism; then, since every positive integer can be factored in a unique way as a product of powers of primes, we have

$$h(n) = h(p_1^{k_1} \ldots p_r^{k_r}) = h(p_1^{k_1}) \ldots h(p_r^{k_r}) = h(p_1)^{k_1} \ldots h(p_r)^{k_r}.$$

□

Classify monoid homomorphisms

Let M be a monoid, and $(A^A, \circ)$ be the monoid of endomorphisms of a set A.

Question

What is a monoid homomorphism $M \to A^A$?

Let's unpack the definition: we are given a function a such that

- $a(x \cdot y) = a(x) \circ a(y)$;
- $a(1) = id_A$.

denote $a(x) = a_x : A \to A$ for short; then the homomorphism conditions translate into

$$a_{x \cdot y}(u) = a_x(a_y(u)), \qquad a_1(u) = u \quad \forall u \in A, x, y \in M$$

Monoid actions

A monoid action is a function $\alpha : M \times A \to A$ such that the following conditions are satisfied:

- $\alpha(x \cdot y, u) = \alpha(x, \alpha(y, u))$ for every $x, y \in M$ and $u \in A$;
- $\alpha(1, u) = u$ for every $u \in A$.

Proposition

Let M be a monoid, A a set; there is a bijection between the set of monoid actions $\alpha : M \times A \to A$ as above, and the set of monoid homomorphisms $M \to (A^A, \circ)$.

Montone maps

Let $\mathbf{P}, \mathbf{Q}$ be posets; a monotone map is a function $f : P \to Q$ such that if $p \leq p'$ in P, then $fp \leq fp'$ in Q.

A simple as that! But this definition allows to develop an interesting theory.

Example of monotone maps: if $f : X \to Y$ is a function between sets,

- there is a monotone map $f_* : PX \to PY$ sending a subset $U \subseteq X$ to $f_*U \subseteq Y$, where
$$f_*U = \{f(x) \mid \in U\}$$
- there is a monotone map $f^{\leftarrow} : PY \to PX$ sending a subset $V \subseteq Y$ to $f^{\leftarrow}V \subseteq X$, where
$$f^{\leftarrow}V = \{x \in X \mid fx \in V\}$$

Galois connections

There is a relation between $f_*, f^{\leftarrow}$:

Definition

Given posets P, Q, a pair of monotone maps

$$f : P \leftrightarrows Q : g$$

is called a Galois connection (see page 29) if for any two $x \in P, y \in Q$ the inequality $fx \leq y$ is true if and only if the inequality $x \leq gy$ is true.

If (f, g) form a GC as above, f is called the left adjoint, and g is called the right adjoint.

Remark

Let (f, g) be a GC as above. Then

- since $fx \leq fx$ (reflexivity), we have $x \leq g(fx)$;
- since $gy \leq gy$ (reflexivity), we have $f(gy) \leq y$.

This implies at once that in a GC, the left and the right adjoint are uniquely determined hen they exist: let $g, g' : Q \to P$ be right adjoints to the same $f : P \to Q$. Then,

$$gy \leq g'fgy \leq g'y,$$

and similarly,

$$g'y \leq gfg'y \leq gy.$$

Order lattices

Definition

A (order) lattice is a poset $\mathbf{P} = (P, \leq)$ such that

- every finite subset $\varnothing \subsetneq S \subseteq P$ has a meet;
- every finite subset $\varnothing \subsetneq S \subseteq P$ has a join;

A lattice is bounded if the above two conditions are extended also to empty subsets.

Examples of lattices: PX for every set X (bounded), $([0,1], \leq)$ (bounded), $(\mathbb{Z}, \leq)$ (not bounded), $[0, \infty)$ (not bounded).

Algebraic lattices

We can define a lattice in an alternative fashion using binary operations:

Definition

A (bounded) algebraic lattice $\mathbf{X}$ is a set X equipped with the following structure

- binary operations $- \wedge - : X \times X \to X$ and $- \vee - : X \times X \to X$ with elements $0, 1 \in X$; subject to the following axioms:
  - $(X, \wedge 1)$ and $(X, \vee, 0)$ form monoids, and every element is idempotent: $x \wedge x = x = x \vee x$;
  - they satisfy the absorption laws: for every $x, y \in X$,

$$x \wedge (x \vee y) = y \qquad x \vee (x \wedge y) = x.$$

Algebraic from order lattices

Given an order lattice $\mathbf{P}$ having finite infs and sups, define an algebraic lattice $\mathbf{P}^{\mathrm{Alg}}$ posing $x \wedge y := \bigwedge\{x, y\}$ and $x \vee y := \bigvee\{x, y\}$.

These define binary, idempotent operations that satisfy the absorption laws

(we have proved 80% of these statements on lecture 2).

Moreover, a monotone function preserving finite infs and sups induces a homomorphism of lattices.

Order from algebraic lattices

Given an algebraic lattice $\mathbf{X}$, define a partial order on X, so an order lattice $\mathbf{X}^{\mathrm{Ord}}$ by

$$x \leq y := x \wedge y = x$$

(equivalently, $x \leq y := x \vee y = y$).

- $x \leq x$ because $x \wedge x = x$;
- $x \leq y, y \leq x$ implies that $x = x \wedge y = y \wedge x = y$.
- if $x \leq y, y \leq z$, then $x \wedge y = x, y \wedge z = y$; so $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$.

The equivalence between two definitions of a lattice:

- given an algebraic lattice $\mathbf{X} = (X, \wedge, \vee)$ we have

$$(\mathbf{X}^{\mathsf{Ord}})^{\mathsf{Alg}} = \mathbf{X}.$$

- Given an order lattice $\mathbf{P} = (P, \leq, \bigvee, \bigwedge)$, we have

$$(\mathbf{P}^{\mathsf{Alg}})^{\mathsf{Ord}} = \mathbf{P}.$$

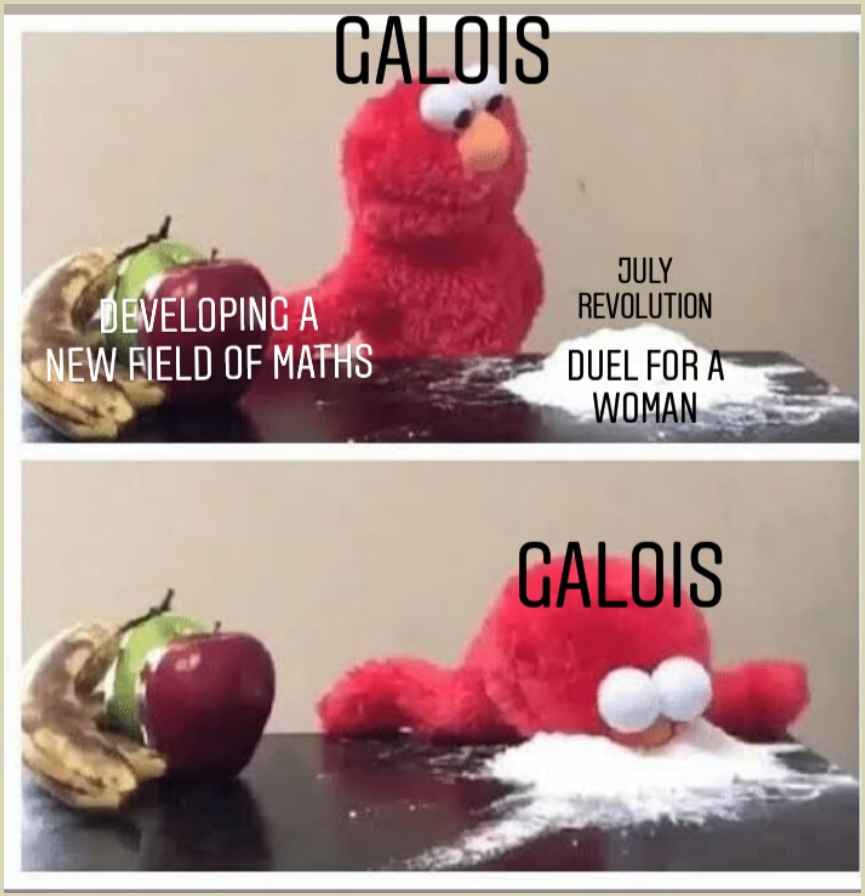
The entirety of category theory, in a single slide

The above phenomenon epitomises a fundamental aspect of mathematical inquiry: we have two classes of structures, and two correspondences in two opposite directions that 'transform' object of type A into objects of type B, reversibly. The two classes of structure contain in a suitable sense the same amount of information; they can be *presented* and understood differently, but they encode the same abstract theories.

The two classes of structures are categories; the two correspondences are called functors; when there is a reversible way to link two categories A, B we say that they are equivalent.

Galois theory

(in a tiny nutshell)



Galois theory

Since the Babylonians (or was it the Egyptians?) we know that there is a formula to solve the generic quadratic equation

$$X^2 + bX + c = 0$$

as $X_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ (this might be a pair of complex numers, depending on the sign of $b^2 - 4c$).

Similar formulas exist for equations of degree three and four.

What about degree five? Is there a way to express the roots $X_1, \ldots, X_5$ of a generic polynomial

$$x^5 + aX^4 + bX^3 + cX^2 + dX + e$$

that involves only ring operations (sums and products) and nth root extractions ('solution by radicals')?

Galois: «Nope».

Galois theory

Let $p \in \mathbb{Q}[X]$ a polynomial; attach to p its splitting field $S(p) \supseteq \mathbb{Q}$, the field where p factors completely as a product of degree 1 monomials.

Let $E \supseteq F$ be a field extension; its Galois group $Gal(E|F)$ is the group of automorphisms of E that 'fix F', i.e. restrict to the identity on F.

1^{st} fundamental theorem of Galois theory: there exists a Galois connection between the poset of subgroups of $Gal(E|F)$ and the poset of intermediate field $E \supseteq K \supseteq F$.

2^{nd} fundamental theorem of Galois theory: to every $p \in \mathbb{Q}[X]$ is attached the Galois group of its splitting field. This group is solvable if and only if the polynomial p is solvable by radicals.