Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

Categories

Definition. A *category* $\mathcal{C}$ consists of:

(a) A collection $\mathrm{Ob}(\mathcal{C})$ of *objects* X, Y, Z etc

(b) A collection $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of *morphisms* (arrows) $f : X \to Y$ between objects with the following properties:

- there is a distinguished identity element $1_X \in \mathrm{Hom}(X, X)$ for each X and
- a binary *composition* operation on concurrent (tip-to-tail) arrows:

$$\circ : \mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z);\ (g, f) \mapsto g \circ f$$

that satisfy:

- the 1_X morphisms are *two-sided identities*: i.e. $f \circ 1_X = f$ and $1_Y \circ f = f$ and
- composition of arrows is an *associative* operation:

$$(h \circ g) \circ f = h \circ (g \circ f) \text{ for all triples of concurrent arrows}$$

Remark. The notion of a *collection* (rather than a set) is necessary, for example, to avoid Russell's paradox within the category of sets. We will ignore such issues here and implicitly assume that our categories are *small*, i.e. that we can treat our objects and arrows as elements of a set.

Definition. (i) Morphisms $f : X \to Y$ and $g : Y \to X$ are *two-sided inverses* if:

$$f \circ g = 1_Y \text{ and } g \circ f = 1_X$$

(ii) A morphism with a two-sided inverse is an *isomorphism*.

(iii) $\mathrm{End}(X) = \mathrm{Hom}_{\mathcal{C}}(X, X)$ are the *endomorphisms* of X, and

(iv) $\mathrm{Aut}(X)$ (the *automorphisms* of X) are the isomorphisms in $\mathrm{End}(X)$.

Remark. $\mathrm{Aut}(X)$ is a group, usually not abelian.

Before we get to the main examples, we offer two more definitions.

Definition. (i) An object X of $\mathcal{C}$ is an *initial object* if:

$$\mathrm{Hom}(X, Y) \text{ is a singleton, for each object } Y \text{ of } \mathcal{C}$$

(ii) An object Z of $\mathcal{C}$ is a *final object* if:

$$\mathrm{Hom}(Y, Z) \text{ is a singleton, for each object } Y \text{ of } \mathcal{C}$$

Remark. Any two initial (or final) objects are isomorphic via a unique isomorphism.

Examples. (a) In the category of sets (and set mappings), 1_X is the identity, the bijections are the isomorphisms and the permutations are the automorphisms. The empty set is the initial object, and each singleton set is a final object.

(b) The power set $\mathcal{P}(X)$ of a set X is the category in which the objects are the subsets of X (including the empty set), the set inclusions $S \subseteq T$ are the morphisms, so that in particular, each $\mathrm{Hom}_{\mathcal{C}}(S, T)$ is either empty or else a singleton, and every endomorphism is an isomorphism (which is most unusual). The initial object is the empty set and X is the unique final object.

(c) To each category $\mathcal{C}$ there is an opposite category $\mathcal{C}^{\mathrm{op}}$ that shares the same objects and arrows, but reverses the direction of the arrows (and the ordering of arrows in the composition operation). Note that an initial object of $\mathcal{C}$ is a final object in $\mathcal{C}^{\mathrm{op}}$ and vice versa. For example, the opposite category of the power set reverses the notion of "being contained in" a superset to "containing" a subset.

Definition. (i) The *product* (if it exists) of a pair of objects X, Y in a category $\mathcal{C}$ is an object with a pair of *projection* morphisms:

$$(X \times Y,\ p : X \times Y \to X,\ q : X \times Y \to Y)$$

that is universal, in the sense that given any other object with pair of morphisms $(Z,\ f : Z \to X,\ g : Z \to Y)$ there is a unique morphism, which we will denote by $(f, g) : Z \to X \times Y$ such that $p \circ (f, g) = f$ and $q \circ (f, g) = g$.

(ii) A product in $\mathcal{C}^{\mathrm{op}}$ is a *coproduct* in $\mathcal{C}$ (with *injection* morphisms i, j).

Remark. As a result of the universal property, any two products (or coproducts) are isomorphic by a uniquely defined isomorphism, which is why we took the liberty of naming the product $X \times Y$, which looks canonical.

Examples. (a) The Cartesian product (with projections) is the product in the category of sets and the disjoint union (with inclusions) is the coproduct.

(b) The intersection (with inclusions) is the product in the power set of a set X. The union (with inclusions) is the coproduct.

The next two examples relate to commutative rings with 1.

(c) The objects of the category $\mathcal{C}Ring$ are commutative rings with 1 and the morphisms are ring homomorphisms. The commutative ring $\mathbb{Z}$ is the unique initial object and the zero ring (with $0 = 1$) is the unique final object. The product of rings (with projections) is the product and we will see in the next section that the tensor product (over the ring $\mathbb{Z}$) is the coproduct.

(d) Fix a commutative ring R with 1. The objects of the category $\mathcal{M}od_R$ of R-modules are the R-modules M and the morphisms are R-module homomorphisms $f : M \to N$. In this case, the **zero module** 0_R is **both** the (unique) initial and (unique) final object. Moreover, the direct sum (of R-modules) is both product (with projections) and coproduct (with $i : M \to M \oplus N$ given by $i(m) = m \oplus 0$ and $j(n) = 0 \oplus n$ defining j).

More Properties of the Category $\mathcal{M}od_R$ of R-Modules.

(i) Each collection of morphisms is an *abelian group.* In fact,

$$\mathrm{Hom}_R(M, N) \text{ is an } R\text{-module, and}$$

the composition is bilinear map on R-modules, i.e.

$$(rf + sg) \circ h = r(f \circ h) + s(g \circ h) \text{ and } e \circ (rf + sg) = r(f \circ g) + s(f \circ h)$$

for morphisms $f, g : M \to N$ and $h : L \to M, e : N \to P$, and $r, s \in R$.

(ii) Each $f : M \to N$ gives rise to the following R-modules:

$$\ker(f) = f^{-1}(0),\ \mathrm{coim}(f) = M/\ker(f),\ \mathrm{im}(f) = f(M),\ \mathrm{coker}(f) = N/f(M)$$

with $\ker(f) \subset M$, $\mathrm{im}(f) \subset N$ and quotient maps $M \to \mathrm{coim}(f)$ and $N \to \mathrm{coker}(f)$.

Moreover, by the first isomorphism theorem:

$$\mathrm{coim}(f) \cong \mathrm{im}(f) \text{ (via the first quotient map)}$$

and the following universal properties of the kernel and cokernel hold:

UK: A morphism $g : L \to M$ satisfies $f \circ g = 0$ if and only if:

$$g : L \xrightarrow{\overline{g}} \ker(f) \subset M \text{ for a unique map to the kernel, and}$$

UC: A morphism $h : N \to P$ satisfies $h \circ f = 0$ if and only if:

$$h : N \to \mathrm{coker}(f) \xrightarrow{\overline{h}} P \text{ for a unique map from the cokernel}$$

Remark. We say above that g (resp h) factors through the kernel (resp the cokernel).

One more definition gives categorical analogues of "injective" and "surjective."

Definition. Let $f : X \to Y$ in a category $\mathcal{C}$. Then

(a) f is an *epimorphism* if $g_1 \circ f = g_2 \circ f$ implies $g_1 = g_2$ (and vice versa) for all objects Z and morphisms $g_1, g_2 : Y \to Z$.

(b) f is a *monomorphism* if $f \circ h_1 = f \circ h_2$ implies $h_1 = h_2$ (and vice versa) for all objects W and morphisms $h_1, h_2 : W \to X$.

Examples. (a) In the category of sets and set mappings:

epimorphism = surjective map, and monomorphism = injective map

(b) In the power set category, every morphism is both mono and epi!

(c) In $\mathcal{C}Ring$, $\mathbb{Z} \subset \mathbb{Q}$ is both a monomorphism and epimorphism!

Proposition 1. Like the category of sets, within the category $\mathcal{M}od_R$,

- $f : M \to N$ is an epimorphism if and only if f is a surjection (of sets),
- $f : M \to N$ is a monomorphism if and only if f is injective.
- $f : M \to N$ is an isomorphism if and only if f is a bijection.

Definition. A category $\mathcal{C}$ is *abelian* if:

(i) All collections $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ are abelian groups, and composition is bilinear.

(ii) There is a unique *zero object* 0 of $\mathcal{C}$ that is both initial and final.

(iii) Products and coproducts of objects of $\mathcal{C}$ exist and are isomorphic, with:

$$0 = q \circ i : X \to X \times Y \to Y \text{ and } 0 = p \circ j : Y \to X \times Y \to X$$

for the universal projections p, q and injections i, j.

(iv) To each morphism $f : X \to Y$, there is a uniquely associated:

(a) kernel monomorphism $k : K \to X$ and

(b) cokernel epimorphism $c : Y \to C$ such that:

UK: Each $g : W \to X$ with $f \circ g = 0$ factors (uniquely) through the kernel via:

$$g = k \circ \overline{g}$$

UC: Each $h : Y \to Z$ with $h \circ f = 0$ factors (uniquely) through the cokernel:

$$h = \overline{h} \circ c$$

(v) Every monomorphism is a kernel and every epimorphism is a cokernel .

How to Use these Axioms. The prototype for an abelian category is the category of abelian groups, or, more generally, the category of R-modules. These axioms are fundamental to the art of "diagram chasing," which is central to *Homological Algebra*. The following Propositions are a starter kit for the use of these axioms.

Let $\mathcal{C}$ be a category satisfying (i)-(v), i.e. an abelian category.

H0. The zero morphism $0 \in \text{Hom}(X,Y)$ (in (i)) is the unique morphism:

$$X \to 0 \to Y$$

that factors (uniquely) through the zero object (from (ii)).

Proof. $\text{Hom}(X,0)$ and $\text{Hom}(0,Y)$ are singletons, hence zero abelian groups, and the Proposition therefore follows from bilinearity of composition.

H1. $f \in \text{Hom}(X,Y)$ is a monomorphism if and only if $k : 0 \to X$ is the kernel.

Proof. All the canonical morphisms $i : 0 \to X$ (from (ii)) are monomorphisms. If $f : X \to Y$ is a monomorphism and $h : W \to X$ satisfies $f \circ h = 0 = f \circ 0$, then $h = 0$ (by the monomorphism assumption) and so h factors through $k : 0 \to X$ (by H0). Conversely, if $k : 0 \to X$ is the kernel of f and $h_1, h_2 : W \to X$ satisfy $f \circ h_1 = f \circ h_2$, then $f \circ (h_1 - h_2) = 0$ (bilinearity), and so $h_1 - h_2$ factors through the kernel, i.e. (by H0), $h_1 - h_2 = 0$, and $h_1 = h_2$. $\square$

CoH1. f is an epimorphism if and only if $c : Y \to 0$ is the cokernel.

H2. f is an isomorphism if and only both the kernel and cokernel are zero.

Proof. One direction is clear. Let $f : X \to Y$ and $f^{-1} : Y \to X$ be inverses. Given $h_1, h_2 : W \to X$, if $f \circ h_1 = f \circ h_2$, then $h_1 = f^{-1} \circ f \circ h_1 = f^{-1} \circ f \circ h_2 = h_2$. Given $g_1, g_2 : Y \to Z$, if $g_1 \circ f = g_2 \circ f$, then $g_1 = g_1 \circ f \circ f^{-1} = g_1 \circ f \circ f^{-1} = g_2$. Thus f is both a monomorphism and an epimorphism. Now use H1.

Conversely, given $f : X \to Y$ that is both a mono and epi, then by (v), $f : X \to Y$ is a kernel of some $g : Y \to Z$ since f is a monomorphism, so $g \circ f = 0 \circ f$ and $g = 0$ since f is an epimorphism. But then the morphism $1_Y : Y \to Y$ factors through the kernel of g, giving the inverse $f^{-1} = \overline{1}_Y : X \to Y$ by the universal property, factoring 1_Y through the kernel. It is then immediate, by construction, that $f \circ f^{-1} = 1_Y$. But now $f^{-1} \circ 1_Y \circ f$ and 1_X satisfy $f \circ (f^{-1} \circ 1_Y \circ f) = f \circ 1_X$, so again since f is a monomorphism, we have $f^{-1} \circ f = f^{-1} \circ 1_Y \circ f = 1_X$, and f^{-1} is a *two-sided* inverse. $\square$

The curious reader may be wondering about the *(co)image* of a morphism in an abelian category $\mathcal{C}$. Never fear, they are still accessible from the axioms.

Definition. The image of $f : X \to Y$ is the kernel of the cokernel:

$$f \rightsquigarrow c : Y \to C \rightsquigarrow i : I \to Y$$

(which is a monomorphism, since it is a kernel). Likewise, the coimage:

$$f \rightsquigarrow k : K \to X \rightsquigarrow ci : X \to CI$$

is the cokernel of the kernel, and then our final (for now) tool in the kit is:

H3. The coimage and image are isomorphic, via the double lift:

$$f : X \to Y \rightsquigarrow 0 = c \circ k : K \to C \rightsquigarrow \overline{\overline{c \circ k}} : CI \to I$$

that is both a monomorphism and epimorphism (Exercise). Now use H2.

Example. The categories $\mathcal{FGMod}_R$ of *finitely generated* R-modules are not abelian categories, in general, since kernels of morphisms of finitely generated modules need not be finitely generated. All the other axioms, however, still hold, so when R is a **Noetherian** ring, the submodules of finitely generated modules (i.e. the kernels) are in the category of finitely generated modules, and this category of abelian.

This includes the categories of finite dimensional vector spaces over k and finitely generated abelian groups, but also the categories of finitely generated modules over polynomial rings $k[x_1, ..., x_n]$ or $\mathbb{Z}[x_1, ..., x_n]$, which are much more interesting.

We'll finish this section with another abelian category of modules.

Definition. (i) A $\mathbb{Z}$-grading on a commutative ring $S_\bullet$ with $1 \in S_0$ is a direct sum

$$S_\bullet = \bigoplus_{d=0}^{\infty} S_d$$

into *homogeneous* (abelian group) summands that are compatible with the product in the sense that $S_d \cdot S_e \subset S_{d+e}$, i.e. $ab \in S_{d+e}$ whenever $a \in S_d$ and $b \in S_e$.

(ii) An ideal $I \subset S_\bullet$ of a graded ring $S_\bullet$ is *homogeneous* if:

$$a = a_0 + \cdots + a_d \in I \subset S_\bullet \;\Rightarrow\; a_i \in I \text{ for all } i$$

i.e. if I is the direct sum: $I = \bigoplus_{d=0}^{\infty} I_d$ with $I_d = I \cap S_d$.

(iii) A ring homomorphism $f : S_\bullet \to T_\bullet$ is graded if $f(S_d) \subset T_d$ for all d.

This gives rise to the category $\mathcal{G}r\mathcal{R}ing$ of graded (commutative) rings with 1.

Proposition 2. The kernel $\ker(f)$ of a graded homomorphism $f : S_\bullet \to T_\bullet$ of graded rings is a homogeneous ideal. Conversely, given a homogeneous ideal $I \subset S_\bullet$ in a graded ring, the quotient ring is graded:

$$S_\bullet/I = \bigoplus_{d=0}^{\infty} S_d/I_d$$

and the ring homomorphism $\overline{f} : S_\bullet \to S_\bullet/I$ is a graded ring homomorphism.

Example. The polynomial ring $S_\bullet = k[x_0, ..., x_n]$ is graded by degree (yeah, when we speak of graded polynomial rings, we usually start the variables with x_0) , i.e. each polynomial of degree d is uniquely a sum: $p = p_0 + \cdots + p_d$ of homogeneous polynomials (sums of monomials $\prod x_i^{d_i}$ of the same degree $d = \sum d_i$). Thus:

$$S_\bullet = \bigoplus_{d=0}^{\infty} k[x_0, ..., x_n]_d$$

and the summands S_d are finite dimensional vector spaces over $S_0 = k$. Recall that $S_\bullet$ is Noetherian (by the Hilbert Basis Theorem) and so every homogeneous ideal $I \subset S_\bullet$ is generated by finitely many *homogeneous* polynomials. Note also that there is *one homogeneous ideal to rule them all*, namely:

$$\mathfrak{m} = \bigoplus_{d>0} S_d$$

the unique maximal homogeneous ideal in $S_\bullet$.

Fix now a graded commutative ring $S_\bullet$ with $1 \in S_0$.

Definition. An $S_\bullet$-module $M_\bullet$ with a direct sum (abelian group) decomposition:

$$M_\bullet = \bigoplus_{d\in\mathbb{Z}} M_d$$

is a graded $S_\bullet$-module if $S_d \cdot M_e \subset M_{d+e}$ for all d, e.

Note. Unlike $S_\bullet$, a module $M_\bullet$ may have homogeneous elements of any degree.

Examples. (a) Homogeneous ideals are graded modules.

(b) For each $e \in \mathbb{Z}$, the *e-twisted free* module is:

$$S(e) = \bigoplus_{d=-e} S_{e+d} \text{ (i.e. } S(e) \text{ in degree } d \text{ is the same as } S \text{ in degree } e+d)$$

Definition. An $S_\bullet$-homomorphism $f : M_\bullet \to N_\bullet$ of graded S-modules is graded if:

$$f(M_d) \subset N_d \text{ for all } d$$

Example. Multiplication by $b \in S_e$ defines a graded homomorphism:

$$b : S \to S(e);\ a \mapsto ab \in S_{d+e} = S(e)_d \text{ for } a \in S_d$$

of graded modules and more generally, $b : S(n) \to S(n+e)$ defined the same way. In particular, each *principal* homogeneous ideal $I = \langle b\rangle$ for $b \in S_e$ is the image of the twisted S-module $S(-e)$ via the graded homomorphism:

$$b : S(-e) \to I \subset S$$

and if b is not a zero divisor in S, then this is an isomorphism of graded modules.

More generally still, if $M_\bullet$ is a graded S-module and $m \in M_e$ is homogeneous, then $m : S(-e) \to M_\bullet;\ a \mapsto am$ is a graded S-module homomorphism, and if $M_\bullet$ is generated by homogeneous elements $m_1, ..., m_N$ of degrees $e_1, ..., e_N$, then we obtain a surjective graded homomorphism:

$$\bigoplus_{i=1}^{N} S(-e_i) \to M_\bullet;\ (a_1, ..., a_N) \mapsto a_1m_1 + \cdots + a_Nm_N$$

Thus in particular, the degrees of the summands of a finitely generated graded module $M_\bullet$ are bounded from below, and if $S_0 = k$ and S_d are finite-dimensional vector spaces over k, then each M_d is a finite-dimensional vector space over k, and we obtain the following *numerical invariant* of $M_\bullet$:

Definition. The Hilbert function $h_M : \mathbb{Z} \to \mathbb{Z}$ of $M_\bullet$ is defined by:

$$h_M(d) = \dim_k M_d$$

Extended Exercise. Show that the categories $\mathcal{G}rMod_S$ of graded $S_\bullet$-modules over a graded commutative ring $S_\bullet$ are abelian categories and that when $S_\bullet$ is Noetherian, the category of finitely generated graded $S_\bullet$-modules is also abelian.