

11 Applications

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-11-27

The description of finitely generated modules over a principal ideal domain simultaneously generalizes of the fundamental theorem of finitely generated abelian groups and provides a unified framework for understanding various canonical form for square matrices.

11.0 Finitely Generated Abelian Groups

Specializing the structure theorem for finitely generated modules over a principal ideal domain, we obtain a structure theorem for finitely generated abelian groups.

11.0.1 Theorem. *For any finitely generated abelian group G , there exists unique nonnegative integers r and e , and unique positive integers $q_1, q_2, \dots, q_e$ such that $q_1 > 1$, q_j divides q_{j+1} for all $1 \leq j < e$, and*

$$G \cong \frac{\mathbb{Z}}{\langle q_1 \rangle} \oplus \frac{\mathbb{Z}}{\langle q_2 \rangle} \oplus \dots \oplus \frac{\mathbb{Z}}{\langle q_e \rangle} \oplus \mathbb{Z}^r.$$

Proof. Since the ring $\mathbb{Z}$ of integers is a principal ideal domain, this theorem follows immediately from Theorem 10.3.1. $\square$

11.0.2 Corollary. *Let G be a finite abelian group. Assuming that, for any positive integer n , the number of elements g in G such that $ng = 0$ is at most n , the group G is cyclic.*

Proof. By Theorem 11.0.1, there exists a nonnegative integers e and positive integers $q_1, q_2, \dots, q_e$ such that $q_1 > 1$, q_j divides q_{j+1} for all $1 \leq j < e$, and

$$G \cong \frac{\mathbb{Z}}{\langle q_1 \rangle} \oplus \frac{\mathbb{Z}}{\langle q_2 \rangle} \oplus \dots \oplus \frac{\mathbb{Z}}{\langle q_e \rangle}.$$

If $e > 1$, then $|G| > q_e$ and $q_e g = 0$ for all g in G contradicting the assumption. We conclude that $e = 1$ and G is cyclic. $\square$

11.0.3 Corollary. *Let K be a field. Any finite subgroup the multiplicative group $K^\times$ is cyclic.*

Proof. Let n be a positive integer. A polynomial $K[x]$ of degree n has at most n linear factors. Since the polynomial ring $K[x]$ is a unique factorization domain, it follows any polynomial of degree n has at most n roots. In particular, there are at most n elements a in K such that $a^n - 1 = 0$. Applying Corollary 11.0.2, we deduce that any finite subgroup the multiplicative group $K^\times$ is cyclic. $\square$

There is a second form of Theorem 11.0.1 involving prime powers which is often more convenient for applications.

11.0.4 Corollary. *For any finitely generated abelian group G , there exists unique nonnegative integers r and k , prime integers $p_1, p_2, \dots, p_k$, and positive integers $m_1, m_2, \dots, m_k$ such that*

$$G \cong \frac{\mathbb{Z}}{\langle p_1^{m_1} \rangle} \oplus \frac{\mathbb{Z}}{\langle p_2^{m_2} \rangle} \oplus \dots \oplus \frac{\mathbb{Z}}{\langle p_k^{m_k} \rangle} \oplus \mathbb{Z}^r.$$

Sketch of proof. The factorization $q = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ combined with Theorem 5.3.11 imply that

$$\frac{\mathbb{Z}}{\langle q \rangle} \cong \frac{\mathbb{Z}}{\langle p_1^{m_1} \rangle} \oplus \frac{\mathbb{Z}}{\langle p_2^{m_2} \rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle p_k^{m_k} \rangle}. \quad \square$$

11.0.5 Example. We claim that, up to isomorphism, there are three abelian groups of order 8, and we can identify the isomorphism class of each of the following:

$$(\mathbb{Z}/\langle 15 \rangle)^\times, \quad (\mathbb{F}_{17})^\times / \langle -1 \rangle, \quad \mathbb{F}_8^+, \quad (\mathbb{Z}/\langle 16 \rangle)^\times, \quad \mu_8.$$

Corollary 11.0.4 implies that the abelian groups of order $8 = 2^3$ are isomorphic to

$$\frac{\mathbb{Z}}{\langle 2^3 \rangle}, \quad \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}, \quad \text{or} \quad \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}.$$

Since $(\mathbb{Z}/\langle 15 \rangle)^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$, every element has order 1, 2, or 4, so $(\mathbb{Z}/\langle 15 \rangle)^\times \cong \mathbb{Z}/\langle 2^2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Similarly, we have

$$(\mathbb{F}_{17})^\times = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8\}$$

and $(\mathbb{F}_{17})^\times / \langle -1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8\}$ which is generated by 3, so $(\mathbb{F}_{17})^\times / \langle -1 \rangle \cong \mathbb{Z}/\langle 2^3 \rangle$. The field $\mathbb{F}_8$ has characteristic 2, so every element added to itself is 0, whence $\mathbb{F}_8^+ \cong \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Because we have $(\mathbb{Z}/\langle 16 \rangle)^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$, every element has order 1, 2, or 4, so $(\mathbb{Z}/\langle 16 \rangle)^\times \cong \mathbb{Z}/\langle 2^2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Finally, the group μ_8 is cyclic so $\mu_8 \cong \mathbb{Z}/\langle 2^3 \rangle$. $\diamond$

11.0.6 Example. We can determine the number of abelian groups of order 720 up to isomorphism.

Since $720 = 2^4 \cdot 3^2 \cdot 5$, the Corollary 11.0.4 implies that the abelian groups of order 720 are isomorphic to

$$\begin{array}{ll} \frac{\mathbb{Z}}{\langle 2^4 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^4 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\ \frac{\mathbb{Z}}{\langle 2^3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\ \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\ \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\ \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle}. \end{array}$$

There are 10 isomorphic classes of abelian groups of order 720. $\diamond$

11.0.7 Remark. For any prime integer p , Corollary 11.0.4 implies that the number of abelian groups of order p^k , up to isomorphism, is the number of integer partitions of k .

11.1 Jordan Canonical Form

The structure theorem for finitely generated modules over a principal ideal domain has a striking application to linear algebra.

11.1.1 Proposition. *Let K be a field and let V be a finite-dimensional K -vector space. Choosing a linear operator $T: V \rightarrow V$ is equivalent to endowing V with structure of a module over the polynomial ring $K[t]$.*

Sketch of proof. To endow V with the structure of a $K[t]$ -module, we must define the product of a polynomial $f := a_0 + a_1 t + \cdots + a_n t^n$ in $K[t]$ and a vector v in V . Set

$$f v := a_0 v + a_1 T(v) + a_2 T^2(v) + \cdots + a_n T^n(v) = [f(T)](v),$$

where $f(T) = a_0 I + a_1 T + a_2 T^2 + \cdots + a_n T^n \in \text{End}_K(V)$. One verifies that this makes V into a $K[t]$ -module.

Conversely, multiplication by t defines a map $T: V \rightarrow V$. For any a in K , and any v and w in V , the $K[t]$ -module structure gives $T(av + w) = t(av + w) = atv + tw = aT(v) + T(w)$, so T is a linear operator on V . Identifying the elements in K with constant polynomials, we see that V is a K -vector space. $\square$

In particular, multiplying by t is the same as acting by T . Multiplying by a polynomial of degree 0 is just scalar multiplication by an element in K .

11.1.2 Theorem. *Let V be a nonzero finite-dimensional K -vector space. For any linear operator $T: V \rightarrow V$, there exists a positive integer e and unique monic polynomials $q_1, q_2, \dots, q_e$ in $K[t]$ of positive degree such that q_j divides q_{j+1} for all $1 \leq j < e$ and*

$$V \cong \frac{K[t]}{\langle q_1 \rangle} \oplus \frac{K[t]}{\langle q_2 \rangle} \oplus \cdots \oplus \frac{K[t]}{\langle q_e \rangle}.$$

Proof. Proposition 11.1.1 shows that V is a $K[t]$ -module. Since $K[t]$ is a principal ideal domain, Theorem 10.3.1 expresses V as a direct sum of cyclic $K[t]$ -modules. There are no free summands, because V is finite dimensional. $\square$

11.1.3 Definition. The polynomial $q_e(t)$ in Theorem 11.1.2 is called the *minimal polynomial* of the linear operator T . It is the unique monic polynomial m_T in $K[t]$ of lowest degree such that $m_T(T) = 0$. The *characteristic polynomial* of T is the product $\chi_T(t) := \prod_{i=1}^e q_i(t)$.

11.1.4 Remark. Suppose that $q = b_0 + b_1 t + \cdots + b_{m-1} t^{m-1} + t^m$ in $K[t]$. Relative to the basis $1, t, t^2, \dots, t^{m-1}$ for $K[t]/\langle q \rangle$, we have

$$M(T) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{m-1} \end{bmatrix}.$$

This is called the *companion* matrix of q .

11.1.5 Theorem (Rational canonical form). *Let K be a field and let V be a finite-dimensional K -vector space. For any linear operator $T: V \rightarrow V$, there exists a basis of V such that the matrix $M(T)$ is block diagonal and each block is a companion matrix.* $\square$

11.1.6 Corollary. *Let K be an algebraically closed field and let V be a nonzero finite-dimensional K -vector space. For any linear operator $T: V \rightarrow V$, there exists a positive integer k , elements $\lambda_1, \lambda_2, \dots, \lambda_k$ in K , and positive integers $e_1, e_2, \dots, e_k$ such that*

$$V \cong \frac{K[t]}{\langle (t - \lambda_1)^{e_1} \rangle} \oplus \frac{K[t]}{\langle (t - \lambda_2)^{e_2} \rangle} \oplus \cdots \oplus \frac{K[t]}{\langle (t - \lambda_k)^{e_k} \rangle}.$$

Sketch of proof. Over an algebraically closed field, every polynomial factors into a product of linear ones. Combining the factorization of the polynomials q_j and Theorem 5.3.11 yield the decomposition. $\square$

11.1.7 Remark. Relative to the basis $1, t - \lambda, (t - \lambda)^2, \dots, (t - \lambda)^{e-1}$ for the K -vector space $K[t]/\langle (t - \lambda)^e \rangle$, we have

$$M(T) := \begin{bmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{bmatrix}.$$

This is called the *Jordan* matrix of $(t - \lambda)^e$.

11.1.8 Theorem (Jordan canonical form). *Let K be algebraically closed and let V be a finite-dimensional nonzero K -vector space. For any linear operator $T: V \rightarrow V$, there exists a basis of V such that the matrix $M(T)$ is block diagonal and each block is a Jordan matrix.* $\square$

11.1.9 Example. We construct all linear operators $T: K^6 \rightarrow K^6$ with minimal polynomial $(t - 5)^2(t - 6)^2$ up to similarity. The minimal polynomial divides the characteristic polynomial and these polynomials have the same irreducible factors. Therefore, Corollary 11.1.6 implies that K^6 is isomorphic to one of the following:

$$\begin{aligned} & \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle}, \\ & \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle} \oplus \frac{K[t]}{\langle t - 6 \rangle} \oplus \frac{K[t]}{\langle t - 6 \rangle}, \\ & \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle t - 5 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle} \oplus \frac{K[t]}{\langle t - 6 \rangle}, \\ & \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle t - 5 \rangle} \oplus \frac{K[t]}{\langle t - 5 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle}, \\ & \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle (t - 5)^2 \rangle} \oplus \frac{K[t]}{\langle (t - 6)^2 \rangle}. \end{aligned}$$

$\diamond$

Every square matrix over a field is similar to a matrix in rational canonical form.

The Jordan canonical form is named after [Camille Jordan](#), who first stated it in 1870.

For all nonnegative j , observe that $t(t - \lambda)^j = 1(t - \lambda)^{j+1} + \lambda(t - \lambda)^j$.

Over an algebraically closed field, every square matrix is similar to a matrix in Jordan canonical form.

The Jordan canonical form for the matrix of the desired linear operators is one of the following:

$$\begin{aligned} & \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 & 6 \end{bmatrix}, & \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 1 & 6 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \end{bmatrix}, \\ & \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 1 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{bmatrix}, & \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 & 6 \end{bmatrix}, \\ & \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 & 6 \end{bmatrix}. \end{aligned}$$

11.2 Exercises

11.2.1 Problem. Consider the integer matrix

$$B := \begin{bmatrix} -1 & 5 & -8 & 7 \\ 2 & 8 & -2 & 4 \\ 1 & -11 & 32 & -13 \end{bmatrix}.$$

- i. Find a (3×3) -matrix Q over $\mathbb{Z}$ and a (4×4) -matrix P over $\mathbb{Z}$ such that QBP is in Smith normal form.
- ii. Let G be an abelian group with four generators g_1, g_2, g_3 and g_4 subject to the relations

$$\begin{aligned} -g_1 + 5g_2 - 8g_3 + 7g_4 &= 0 \\ 2g_1 + 8g_2 - 2g_3 + 4g_4 &= 0 \\ g_1 - 11g_2 + 32g_3 - 13g_4 &= 0. \end{aligned}$$

Show that $G \cong \mathbb{Z}/\langle 6 \rangle \oplus \mathbb{Z}/\langle 54 \rangle \oplus \mathbb{Z}$. In addition, find new generators h_1, h_2 and h_3 such that $6h_1 = 0$, $54h_2 = 0$ and h_3 has infinite order.

- iii. Find all integer (3×1) -matrices X such that $BX = C$ where

$$C := \begin{bmatrix} -5 \\ 100 \\ -7 \end{bmatrix}.$$

11.2.2 Problem. Consider the matrix

$$A := \begin{bmatrix} -2 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & -2 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

- i. Find the minimal polynomial of A .
- ii. Find the rational canonical form of A .
- iii. Find the Jordan canonical form of A .

Category theory provides a language for mathematics, designed to capture general phenomena and enable the transfer of ideas. This approach supplies simplifying abstraction, isolating those results that hold for formal reasons from those that require methods from a particular branch of mathematics. Category theory also formulates new proof techniques.

11.3 Mathematical Analogies

Category theory emphasizes the maps between objects. From this perspective, mathematical structures are defined or described by diagrams of arrows. Each arrow $f: X \rightarrow Y$ represents a map or function. A typical diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow g & \downarrow h \\ & & Z \end{array}$$

is commutative when $g = h \circ f$. The same diagram applies in many contexts: sets and functions, topological spaces and continuous maps, groups and homomorphisms, etc.

Many structural properties may be viewed as universal features of diagrams. Consider the cartesian product $X \times Y$ of two sets X and Y , which consists of all ordered pairs (x, y) of elements $x \in X$ and $y \in Y$. The projections $(x, y) \mapsto x$ and $(x, y) \mapsto y$ of the product on its factors are the maps $p: X \times Y \rightarrow X$ and $q: X \times Y \rightarrow Y$. Any map $h: W \rightarrow X \times Y$ is uniquely determined by $p \circ h$ and $q \circ h$.

$$\begin{array}{ccccc} & & W & & \\ & \swarrow f & \downarrow h & \searrow g & \\ X & \xleftarrow{p} & X \times Y & \xrightarrow{q} & Y. \end{array}$$

Conversely, given two functions $f: W \rightarrow X$ and $g: W \rightarrow Y$, there is a unique function $h: W \rightarrow X \times Y$ which makes the diagram commute: $h(w) = (f(w), g(w))$. Thus, given the sets X and Y , the pair (p, q) is “universal” among the functions from some set to X and Y , because any other such pair (f, g) factors uniquely (via h) through the pair (p, q) . This property uniquely characterizes the cartesian product $X \times Y$ (up to a unique bijection). The same diagram, within the category of groups or topological spaces, describes the direct product of groups or the cartesian product of spaces.

The “cartesian product” construction is called a functor because it applies to sets and the maps between them. Two maps $k: X \rightarrow X'$ and $\ell: Y \rightarrow Y'$ have a map $k \times \ell: X \times Y \rightarrow X' \times Y'$, defined by $(x, y) \mapsto (k(x), \ell(y))$ as their cartesian product. Observe that the

one-point set $\text{pt} := \{0\}$ serves as an identity under the operation “cartesian product”, in view of the bijections

$$\text{pt} \times X \xrightarrow{i} X \xleftarrow{j} X \times \text{pt}.$$

given by $i(0, x) = x$ and $j(x, 0) = x$.

A monoid M (semigroup with identity) may be described as a set M together with two maps $\mu: M \times M \rightarrow M$ and $\eta: \text{pt} \rightarrow M$ such that the following two diagrams commute:

$$\begin{array}{ccc} M \times M \times M & \xrightarrow{\text{id}_M \times \mu} & M \times M \\ \mu \times \text{id}_M \downarrow & & \downarrow \mu \\ M \times M & \xrightarrow{\mu} & M \end{array}$$

$$\begin{array}{ccccc} \text{pt} \times M & \xrightarrow{\eta \times \text{id}_M} & M \times M & \xleftarrow{\text{id}_M \times \eta} & M \times \text{pt} \\ i \downarrow & & \downarrow \mu & & \downarrow j \\ M & \xlongequal{\quad} & M & \xlongequal{\quad} & M \end{array}$$

which means $\mu \circ (\text{id}_M \times \mu) = \mu \circ (\mu \times \text{id}_M)$, $\mu \circ (\eta \times \text{pt}) = i$, and $\mu \circ (1 \times \eta) = j$. Rewriting these diagrams with elements gives

$$\begin{array}{ccc} (x, y, z) & \longmapsto & (x, yz) \\ \downarrow & & \downarrow \\ (xy, z) & \longmapsto & (xy)z = x(yz) \end{array}$$

$$\begin{array}{ccc} (0, x) & \longmapsto & (e, x) \\ \downarrow & & \downarrow \\ x & \xlongequal{\quad} & ex \end{array} \qquad \begin{array}{ccc} (x, e) & \longleftarrow & (x, 0) \\ \downarrow & & \downarrow \\ xe & \xlongequal{\quad} & x \end{array}$$

where $\eta(0) = e \in M$. These are the familiar axioms: multiplication is associative and the element e is a left and right identity. The same process applies to other axioms.

Because the diagrams make no mention of elements, they apply in other circumstances. When applied to topological spaces and continuous maps, they define topological groups. For differentiable manifolds and smooth maps, they define a Lie group.

11.4 Categories

A category is a context for studying a class of mathematical objects. Importantly, a category has both ‘nouns’ and ‘verbs’ with specified collections of objects and maps between them.

11.4.1 Definition. A *category* $\mathbf{C}$ consists of a collection $X, Y, Z, \dots$ of *objects*, and a collection $f, g, h, \dots$ of *morphisms* such that

(*tails/heads*) Every morphism has specified source and target objects. The morphism f with source X and target Y is denoted by $f : X \rightarrow Y$.

(*identity*) Each object X has a designated *identity morphism* $\text{id}_X : X \rightarrow X$.

(*composition*) For any pair of morphisms f and g such that the target of f is equal to the source of g , there exists a specified *composite morphism* $g f$ whose source is equal to the source of f and whose target is equal to the target of g .

This data satisfies the following two conditions:

(*identity*) For any $f : X \rightarrow Y$, we have $f \text{id}_X = f = \text{id}_Y f$.

(*associativity*) For any triple $f : X \rightarrow Y$, $g : Y \rightarrow Z$, and $h : Z \rightarrow W$, we have $h(g f) = (h g) f$, so the notation $h g f$ is unambiguous.

11.4.2 Example. The category **Set** has sets as its objects and maps, with specified source and target, as its morphisms. $\diamond$

11.4.3 Example. The category **Grp** has groups as its objects and group homomorphisms as its morphisms. $\diamond$

11.4.4 Example. The category **Ab** has abelian groups as its objects and group homomorphisms as its morphisms. $\diamond$

11.4.5 Example. The category **CRng** has commutative rings as its objects and ring homomorphisms as its morphisms. $\diamond$

11.4.6 Example. For an commutative ring R , the category $\mathbf{Mod}_R$ has R -modules as its objects and R -linear maps as its morphisms. Thus, the category **Ab** is the same as the category $\mathbf{Mod}_{\mathbb{Z}}$. $\diamond$

11.4.7 Example. The category **Top** has topological spaces as objects and continuous functions as morphisms. $\diamond$

11.4.8 Example. The category $\mathbf{Top}_*$ has pointed topological spaces (having a distinguished point called the basepoint) as objects and basepoint-preserving continuous functions as morphisms. $\diamond$

11.4.9 Example. The category **Htpy** has topological spaces as objects and homotopy classes of continuous maps as morphisms. $\diamond$

Russell’s paradox implies that there is no set whose elements are “all sets”. For this reason, we use the vague word “collection” in Definition 11.4.1. The set-theoretical foundations for category theory are a separate topic.

As in Definition 1.3.3, a morphism $f : X \rightarrow Y$ is an *isomorphism* if there exists a morphism $g : Y \rightarrow X$ such that $g f = \text{id}_X$ and $f g = \text{id}_Y$.

Despite downplaying the significance of the morphisms, it is traditional to name a category after its objects.

The first examples are “concrete” categories—objects have underlying sets and the morphisms are maps between the underlying sets. However, “abstract” categories are also common.

11.4.10 Example. The category **Graph** has graphs (undirected and simple) as objects and graph morphisms (a pair of maps on vertices and edges preserving incidence relations) as morphisms. $\diamond$

11.4.11 Example. The category **Poset** has partially-ordered sets as its objects and order-preserving maps as its morphisms. $\diamond$

11.4.12 Example. For any commutative ring R , the category $\mathbf{Mat}_R$ has nonnegative integers as its objects. For any nonnegative integers n and m , the morphisms from n to m are $(m \times n)$ -matrices with entries in R . Composition is given by matrix multiplication with identity matrices serving as the identity morphisms. $\diamond$

11.4.13 Example. For any group G , the category **BG** has one object. Each group element gives a distinct endomorphism of the single object with composition given by multiplication in G . The identity e in G acts as the identity morphism for the unique object. $\diamond$

11.4.14 Definition. Let $\mathbf{C}$ be a category. The *opposite category* has the same objects as $\mathbf{C}$. There is a morphism $f^{\text{op}} : X \rightarrow Y$ in $\mathbf{C}^{\text{op}}$ if there is a morphism $f : Y \rightarrow X$ in $\mathbf{C}$. A pair of morphisms f^{op} and g^{op} in $\mathbf{C}^{\text{op}}$ is composable when the pair g, f is composable in $\mathbf{C}$. We define $g^{\text{op}} f^{\text{op}}$ to be $(f g)^{\text{op}}$.

11.4.15 Definition. A morphism $f : X \rightarrow Y$ is a *monomorphism* if, for any morphisms $h : W \rightarrow X$ and $k : W \rightarrow X$, the relation $f h = f k$ implies that $h = k$. In other words, f is left-cancellable.

Dually, a morphism $f : X \rightarrow Y$ is an *epimorphism* if, for any morphisms $h : Y \rightarrow Z$ and $k : Y \rightarrow Z$, the relation $h f = k f$ implies that $h = k$. Equivalently, f is right-cancellable.

11.4.16 Lemma. Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be morphisms.

(products) When f and g are monomorphisms, $g f : X \rightarrow Z$ also is.

When f and g are epimorphisms, $g f : X \rightarrow Z$ also is.

(factors) When $g f : X \rightarrow Z$ is a monomorphism, the first factor f is a monomorphism. When $g f : X \rightarrow Z$ is an epimorphism, the second factor g is an epimorphism.

Proof. Consider morphisms $h : W \rightarrow X$ and $k : W \rightarrow X$. Assuming that g is monomorphism, the relation $g f h = g f k$ implies that the composite $f h = f k$. Assuming that f is also a monomorphism, we deduce that $h = k$, so the composite $g f$ is a monomorphism. The relation $f h = f k$ implies that $g f h = g f k$. Assuming that $g h$ is a monomorphism, we see that $h = k$, so f is a monomorphism.

The notions of monomorphism and epimorphism are dual, so the remaining two cases follow from the first two. $\square$

This duality has a very important in the development of category theory. Any theorem containing a universal quantification of the form “for all categories $\mathbf{C}$ ” applies to the opposites of these categories. Interpreting the result in the dual context leads to a dual theorem, in which the direction of each arrow is reversed.

11.5 Exercises

11.5.1 Problem. In any category $\mathbf{C}$, provide a direct prove for each of the following:

- i. The composition of two epimorphisms is an epimorphism.
- ii. If the composition of two morphisms is an epimorphism, then the second morphism is an epimorphism.
- iii. Every isomorphism is an epimorphism and a monomorphism.

A morphism that is both a monomorphism and an epimorphism need not be an isomorphism.

11.5.2 Problem. A *poset* is a set P with a binary relation $\leq_P$ which is reflexive, transitive and antisymmetric. More precisely, for any elements x, y , and z in P , we have the following:

(*reflexivity*) The relation $x \leq_P x$ holds.

(*antisymmetry*) The relations $x \leq_P y$ and $y \leq_P x$ imply that $x = y$.

(*transitivity*) The relations $x \leq_P y$ and $y \leq_P z$ imply that $x \leq_P z$.

A function $f : P \rightarrow Q$ between two posets is *order-preserving* if, for any x and y in P satisfying $x \leq_P y$, we have $f(x) \leq_Q f(y)$.

- i. Demonstrate that the collection of posets together with order-preserving functions form a category.
- ii. In the category of posets, exhibit a bijective morphism between nonisomorphic posets.

11.5.3 Problem. Let G be a group. The *center* of G , denoted $Z(G)$, is the set of elements in G that commute with every element in G . The *commutator* of the elements g and h in G is the element $[g, h] := g^{-1}h^{-1}gh$. The *commutator subgroup* G' of G is the subgroup generated by all the commutators of elements in G .

- i. Show that the assignment $G \mapsto Z(G)$ does *not* give a functor from $\mathbf{Grp}$ to $\mathbf{Ab}$.
- ii. Show that $G \mapsto G/G'$ does give a functor from the category of groups to the category of abelian groups.

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.