Discrete Mathematics Basics

Bojue Wang

July 11, 2025

Contents

1 Induction

1.1 Mathematical Induction

Theorem 1.1 (Principle of Mathematical Induction)**.** Let $P(n)$ be a statement about an integer n. To prove $P(n)$ is true for all $n \geq n_0$, it suffices to show:

(i) (Base Case) $P(n_0)$ holds,

(ii) (Inductive Step) For any $k \geq n_0$, if $P(k)$ holds then $P(k+1)$ holds.

Then $P(n)$ is true for all $n \geq n_0$.

Proof. Combine the base case and inductive step to conclude by induction. □

Example 1.1 (Sum and Powers of Integers)**.** Prove the following using induction:

(i) $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \geq 1$.

(ii) $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

(iii) $\displaystyle\sum_{k=1}^{n} k^3 = \Big(\sum_{k=1}^{n} k\Big)^2$.

(iv) For the Fibonacci sequence $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$, show

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

(v) If A is finite, prove $|2^A| = 2^{|A|}$.

Exercise 1.1 (Growth Rates)**.** Use induction to compare functions: show for large t,

$$1 \ll \log t \ll t^k \ll e^t \ll t^k e^t \ll e^{t^k} \ll e^{e^t} \ll t!.$$

Remark 1.1. Replace the continuous variable t by the discrete variable n, and modify the parameter k, so that induction works.

1.2 Strong Mathematical Induction

We can modify the inductive hypothesis of mathematical induction - if $P(n_0) \equiv 1$, then $P(n_0 + 1) \equiv 1$ - by the following:

$$\text{if } P(n_0) \wedge P(n_0 + 1) \wedge \cdots \wedge P(n_0 + k) \equiv 1, \text{ then } P(n_0 + k + 1) \equiv 1.$$

This is called *strong* mathematical induction. Logically, it is equivalent to mathematical induction.

1.3 Transfinite Induction

Transfinite induction generalizes ordinary induction to well-ordered sets (e.g., ordinals).

Remark 1.2. Transfinite induction is a generalization of mathematical induction since it generalized the index set $\mathbb{N}$ to any well-ordered set A.

Theorem 1.2 (Transfinite Induction)**.** Let $(A, <)$ be a well-ordered set and $P(x)$ a property for $x \in A$. If

(1) $P(\min A)$ holds, and

(2) For every $a \in A$, if $P(b)$ holds for all $b < a$, then $P(a)$ holds,

then $P(x)$ holds for all $x \in A$.

Sketch. Assume to the contrary there is a least a_0 with $\neg P(a_0)$. By hypothesis, all $b < a_0$ satisfy $P(b)$, so $P(a_0)$ must hold, contradiction. □

Remark 1.3. For ordinals, one often splits into: base (0), successor (from α to $\alpha + 1$), and limit (if $P(\beta)$ for all $\beta < \lambda$ then $P(\lambda)$).

Example 1.2 (Well-Ordering of Ordinals)**.** Use transfinite induction to show every ordinal is well-ordered under membership.

Exercise 1.2. State and prove the principle of transfinite recursion.

2 Sets

2.1 Basic Set Operations

Definition 2.1 (Set and Element)**.** A *set* is a collection of distinct objects. If x is an element of a set A, we write $x \in A$.

Definition 2.2 (Subset)**.** A set A is a *subset* of B, written $A \subseteq B$, if every element of A belongs to B.

Definition 2.3 (Union, Intersection, Difference, Complement)**.** Let A and B be sets.

$$\begin{aligned} A \cup B &= \{\, x : x \in A \text{ or } x \in B \}, \\ A \cap B &= \{\, x : x \in A \text{ and } x \in B \}, \\ A \setminus B &= \{\, x : x \in A \text{ and } x \notin B \}, \\ A^c &= \{\, x : x \notin A \}. \end{aligned}$$

Definition 2.4 (Power Set and Cartesian Product)**.**

- The *power set* of A, denoted $\mathcal{P}(A)$ or 2^A, is the set of all subsets of A.
- The *Cartesian product* of A and B is

$$A \times B = \{\, (a, b) : a \in A,\ b \in B \}.$$

Definition 2.5 (Quotient Set and Disjoint Union)**.**

- If $\sim$ is an equivalence on A, the *quotient set* $A/\!\sim$ is the set of its equivalence classes.
- The *disjoint union* $A \sqcup B$ may be realized as

$$\{(1, a) : a \in A\} \ \cup\ \{(2, b) : b \in B\}.$$

2.2 Countable and Uncountable Sets

Definition 2.6 (Countable)**.** A set is *countable* if it is finite or there exists a bijection to $\mathbb{N}$.

Definition 2.7 (Uncountable)**.** A set is *uncountable* if it is not countable.

Example 2.1. The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are countable, while $\mathbb{R}$ is uncountable (Cantor's diagonal argument).

2.3 Equinumerosity of Sets

Definition 2.8 (Equinumerous Sets)**.** Two sets A and B are *equinumerous*, written $A \sim B$, if there is a bijection $f \colon A \to B$.

Example 2.2. A bijection $(0, 1) \to \mathbb{R}$ is

$$f(x) = \tan\!\big(\pi x - \tfrac{\pi}{2}\big).$$

Since $[0, 1]$ differs from $(0, 1)$ by only countably many points, $[0, 1] \sim (0, 1) \sim \mathbb{R}$.

Example 2.3. Removing one point from the sphere produces a space homeomorphic to $\mathbb{R}^2$ (stereographic projection).

2.4 Relations on Sets

Definition 2.9 (Relation)**.** A *relation* R on A is any subset of $A \times A$.

2.4.1 Properties of Relations

- **Reflexive:** $(a, a) \in R$ for all $a \in A$.
- **Symmetric:** If $(a, b) \in R$ then $(b, a) \in R$.
- **Transitive:** If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

2.4.2 Partial Orders

Definition 2.10 (Partial Order)**.** A relation $\leq$ on A is a *partial order* if it is reflexive, antisymmetric, and transitive.

Example 2.4. The subset relation $\subseteq$ on $\mathcal{P}(A)$ is a partial order. Its Hasse diagram visualizes the inclusion lattice.

2.4.3 Equivalence Relations and Partitions

Definition 2.11 (Equivalence Relation)**.** A relation is an *equivalence* if it is reflexive, symmetric, and transitive.

Remark 2.1. Each equivalence relation on A induces a partition of A into disjoint *equivalence classes*, and vice versa.

Remark 2.2. A *canonical representative* selects exactly one element from each class (often by some minimality or natural choice).

Example 2.5. On $\mathbb{Z}$, define $a \equiv b \pmod{n}$ if $n \mid (a-b)$. The classes $[a]_n$ form the partition.

2.4.4 Congruence Relations and Modular Arithmetic

- $a \equiv b \pmod{n} \iff n \mid (a - b)$.
- The class $[a]_n$ is $\{\, b : b \equiv a \pmod{n}\}$.
- Arithmetic mod n respects addition and multiplication:

$$(a + b) \bmod n = \big((a \bmod n) + (b \bmod n)\big) \bmod n.$$

Example 2.6. $8 \equiv 2 \pmod{3}$ since $8 - 2 = 6$ is divisible by 3.

2.5 Counting with Sets

Definition 2.12 (Cardinality)**.** For a finite set A, its *cardinality* $|A|$ is the number of its elements.

Theorem 2.1 (Inclusion–Exclusion Principle)**.** For finite sets A, B, C,

$$|A \cup B| = |A| + |B| - |A \cap B|,$$
$$|A \cup B \cup C| = \sum |\cdot| - \sum |\cap| + |A \cap B \cap C|.$$

More generally, for $A_1, \dots, A_n$,

$$\Big|\bigcup_{i=1}^{n} A_i\Big| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} \big|A_{i_1} \cap \cdots \cap A_{i_k}\big|.$$

Sketch. Count total, subtract over-counts of intersections, add back higher intersections, and proceed by induction on n. □

Example 2.7. In a class of 50 students, if

$$30 \text{ take Algebra}, \ 25 \text{ take Analysis}, \ 15 \text{ take both},$$

then

$$|A \cup B| = 30 + 25 - 15 = 40$$

took at least one.

Exercise 2.1. State and prove by induction the inclusion–exclusion formula for $\big|A_1 \cup \cdots \cup A_n\big|$.

3 Functions

3.1 Basic Definitions

Definition 3.1 (Function / Map)**.** Let A and B be sets. A *function* (or *map*) $f\colon A \to B$ assigns to each $a \in A$ exactly one element $f(a) \in B$. Here A is the *domain* and B the *codomain*.

Remark 3.1. Two functions $f, g\colon A \to B$ are equal, $f = g$, if and only if $f(x) = g(x)$ for all $x \in A$.

Example 3.1. The rule $f(x) = x^2$ defines a function $f\colon \mathbb{R} \to \mathbb{R}$.

3.2 Notation and Word Representation

- If $f\colon A \to B$ and $a \in A$, then $f(a) \in B$ denotes the *value* of f at a.
- The set of all functions from A to B is denoted

$$B^A = \{\, f\colon A \to B\}.$$

Remark 3.2 (Word Representation)**.** If $X = \{1, 2, \ldots, n\}$ and $Y = \{1, 2, \ldots, m\}$ then each $f\colon X \to Y$ can be written as the word

$$(f(1), f(2), \ldots, f(n))$$

in an m-letter alphabet. Hence

$$Y^X \;\cong\; \{n\text{-letter words over } Y\}.$$

- Repeated letters are allowed unless specified otherwise.
- Injective maps $\longleftrightarrow$ words with no repeated letters.
- Surjective maps $\longleftrightarrow$ words using every letter of Y.
- Bijective maps $\longleftrightarrow$ words using each letter exactly once.

Remark 3.3 (Power-Set as 2^A)**.** Each subset $S \subseteq A$ corresponds to its *indicator function* $\chi_S\colon A \to \{0, 1\}$, so

$$\mathcal{P}(A) \;\cong\; 2^A \quad \text{and} \quad |\mathcal{P}(A)| \;=\; 2^{|A|}.$$

3.3 Range and Codomain

Definition 3.2 (Range / Image)**.** For $f\colon A \to B$, the *image* is

$$\operatorname{im}(f) \;=\; \{\, b \in B : \exists\, a \in A,\ f(a) = b\}.$$

Remark 3.4. The codomain B need not equal the image $\operatorname{im}(f)$.

Example 3.2. For $f(x) = x^2\colon \mathbb{R} \to \mathbb{R}$, we have $\operatorname{im}(f) = [0, \infty) \neq \mathbb{R}$.

3.4 Function Composition

Definition 3.3 (Composition)**.** Given $f\colon A \to B$ and $g\colon B \to C$, their *composition* is

$$g \circ f\colon A \to C, \qquad (g \circ f)(a) = g\big(f(a)\big).$$

Proposition 1. Composition is associative: if $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$, then

$$h \circ (g \circ f) \;=\; (h \circ g) \circ f.$$

3.5 Injective, Surjective, Bijective

3.5.1 Injective (One-to-One)

Definition 3.4 (Injection)**.** $f\colon A \to B$ is *injective* if

$$f(a_1) = f(a_2) \implies a_1 = a_2.$$

Remark 3.5. Injective maps admit *left inverses* (retracts); geometrically they embed A into B.

Example 3.3. $f(x) = 3x - 1$ on $\mathbb{R}$ is injective; x^2 is not.

3.5.2 Surjective (Onto)

Definition 3.5 (Surjection)**.** $f\colon A \to B$ is *surjective* if

$$\forall\, b \in B,\ \exists\, a \in A :\ f(a) = b.$$

Remark 3.6. Surjective maps admit *right inverses* (sections); geometrically they project A onto B.

Example 3.4. $f(x) = x^3$ from $\mathbb{R}$ to $\mathbb{R}$ is surjective; x^2 is not.

3.5.3 Bijective (One-to-One Correspondence)

Definition 3.6 (Bijection)**.** $f\colon A \to B$ is *bijective* if it is both injective and surjective.

Proposition 2. f is bijective $\iff$ there exists $f^{-1}\colon B \to A$ such that

$$f^{-1} \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ f^{-1} = \mathrm{id}_B.$$

3.6 Inverse Functions

Definition 3.7 (Inverse Function)**.** If $f\colon A \to B$ is bijective, its *inverse* $f^{-1}\colon B \to A$ satisfies

$$f^{-1}(f(a)) = a, \quad f(f^{-1}(b)) = b.$$

Example 3.5. If $f(x) = 3x + 2$, then $f^{-1}(y) = \frac{y-2}{3}$.

3.7 Restriction and Extension

Definition 3.8 (Restriction)**.** For $f\colon A \to B$ and $X \subseteq A$, the *restriction* is

$$f|_X\colon X \to B, \quad f|_X(x) = f(x).$$

Definition 3.9 (Extension)**.** An *extension* of $f\colon A \to B$ to $Y \supseteq A$ is a function

$$F\colon Y \to B \quad \text{with} \quad F|_A = f.$$

Example 3.6 (Even/Odd Extension)**.** Let $f\colon (0, L] \to \mathbb{R}$. Its even extension to $[-L, L]$ is

$$f_e(x) = \begin{cases} f(x), & x \in (0, L], \\ a, & x = 0, \\ f(-x), & x \in [-L, 0), \end{cases}$$

and its odd extension is

$$f_o(x) = \begin{cases} f(x), & x \in (0, L], \\ 0, & x = 0, \\ -f(-x), & x \in [-L, 0). \end{cases}$$

3.8 Products of Functions

Definition 3.10 (Pairing)**.** Given $f\colon A \to B$, $g\colon A \to C$, define

$$(f, g)\colon A \to B \times C, \quad a \mapsto (f(a), g(a)).$$

Definition 3.11 (Cross Product)**.** If $f\colon A \to B$, $g\colon C \to D$, then

$$f \times g\colon A \times C \to B \times D, \quad (a, c) \mapsto (f(a), g(c)).$$

3.9 Countability and Equinumerosity

Definition 3.12. A set is *countable* if it is finite or in bijection with $\mathbb{N}$. It is *uncountable* otherwise.

3.10 Countability and Cartesian Product

Theorem 3.1. A finite Cartesian product of countable sets is countable.

Proof. Mathematical induction, if A, B are countable, then $A \times B$ is countable by array representation of elements of form (a, b). Then any finite product can be formed by finitely many times product. □

Example 3.7. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable; $\mathbb{R}$ is uncountable (Cantor's diagonal argument).

Example 3.8. $(0, 1) \cong \mathbb{R}$ via $x \mapsto \tan\big(\pi x - \frac{\pi}{2}\big)$, and $[0, 1] \cong (0, 1)$.

Example 3.9. The punctured sphere $S^2 \setminus \{p\}$ is equinumerous to the plane $\mathbb{R}^2$.

3.11 Exercises

1. Count the number of functions $f\colon \{1,2,3\} \to \{a,b,c,d\}$.
2. Prove or disprove: $f(n) = 2n+1$ is injective/surjective on $\mathbb{Z}$.
3. Give a function $\mathbb{Z} \to \mathbb{Z}$ that is injective but not surjective.
4. Give a function $\mathbb{Z} \to \mathbb{Z}$ that is surjective but not injective.
5. Show that composition of injective functions is injective.
6. Show that composition of surjective functions is surjective.
7. Let $f\colon A \to B$ and $g\colon B \to A$ satisfy $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. Prove f, g are inverses.
8. Is $f(x) = x^3 + 1$ bijective on $\mathbb{R}$? Find f^{-1}.
9. (Advanced) If $f\colon \mathbb{R} \to \mathbb{R}$ is continuous and injective, must it be surjective?

4 Cardinality

The concept of *cardinality* enables us to compare the "size" of sets, whether finite or infinite. For finite sets, this is simply counting elements. For infinite sets, we use bijections and other tools to analyze their size.

4.1 Equinumerosity and Cardinality

Definition 4.1 (Equinumerous Sets)**.** Two sets A and B are **equinumerous** if there exists a bijection $f : A \to B$. We then write $|A| = |B|$.

Remark 4.1. Equinumerosity is an equivalence relation (reflexive, symmetric, transitive).

Example 4.1. $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$ are equinumerous via $f(1) = a, f(2) = b, f(3) = c$.

4.2 Finite and Infinite Sets

Definition 4.2. A set A is:

- **Finite** if $|A| = n$ for some $n \in \mathbb{N}$;
- **Infinite** if it is not finite;
- **Countably infinite** if there is a bijection $A \to \mathbb{N}$;
- **Uncountable** if no such bijection exists.

Example 4.2.

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable.
- $\mathbb{R}$ is uncountable.

Definition 4.3 (Aleph Numbers)**.** The cardinality of $\mathbb{N}$ is denoted $\aleph_0$ (aleph-null), the smallest infinite cardinal.

4.3 Cardinal Arithmetic

Definition 4.4 (Cardinality of a Finite Set)**.** Let A be a finite set. Its **cardinality** $|A|$ is the number of elements in A.

Theorem 4.1 (Finite Cardinality Rules)**.** Let A, B be finite sets.

1. $|A \cup B| = |A| + |B| - |A \cap B|$
2. If $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$
3. $|A \times B| = |A| \cdot |B|$

4. $|\mathcal{P}(A)| = 2^{|A|}$

Definition 4.5 (Sum)**.** For disjoint sets A and B, the sum is

$$|A| + |B| = |A \cup B| \quad \text{when } A \cap B = \varnothing.$$

Definition 4.6 (Product)**.** For any sets A and B, the product is

$$|A| \cdot |B| = |A \times B| = |\{(a, b) : a \in A, b \in B\}|.$$

Remark 4.2. For disjoint families $(A_i)_{i \in I}$:

$$\sum_{i \in I} |A_i| = \left| \bigcup_{i \in I} A_i \right|, \qquad \prod_{i \in I} |A_i| = \left| \prod_{i \in I} A_i \right|,$$

where $\prod_{i \in I} A_i$ is the set of functions f with $f(i) \in A_i$.

Example 4.3. If $|A| = 3$, $|B| = 4$, then $|A \cup B| = 7$, $|A \times B| = 12$.

Definition 4.7 (Cardinal Exponentiation)**.** Given sets A and B, define:

$$|A|^{|B|} = |\{f : B \to A\}|.$$

Example 4.4. If $|A| = 2$, $|B| = 3$, then $|A|^{|B|} = 2^3 = 8$ (e.g., 3-bit binary strings).

Theorem 4.2 (Arithmetic of Infinite Cardinals)**.** Let κ, λ be infinite cardinals, both nonzero:

1. $\kappa + \lambda = \max\{\kappa, \lambda\}$
2. $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$
3. If $2 \leq \kappa \leq 2^\lambda$, then $\kappa^\lambda = 2^\lambda$

Example 4.5.

$$\aleph_0 + \aleph_0 = \aleph_0, \quad \aleph_0 \cdot \aleph_0 = \aleph_0, \quad 2^{\aleph_0} = \mathfrak{c}$$

4.4 Cantor's Theorem and Consequences

Theorem 4.3 (Cantor's Theorem)**.** For any set A, $|A| < |\mathcal{P}(A)| = 2^{|A|}$.

Corollary 1. There is no largest cardinal:

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \cdots$$

4.5 Countability Theorems and Diagonalization

Theorem 4.4. The set $\mathbb{Q}$ is countable.

Sketch. Enumerate all pairs (m, n) with $m \in \mathbb{Z}, n \in \mathbb{N}^+$, and map $m/n \in \mathbb{Q}$. □

Theorem 4.5 (Cantor's Diagonal Argument)**.** The set $\mathbb{R}$ is uncountable.

Sketch. Suppose $r_1, r_2, \ldots$ list all reals in $[0, 1]$. Construct r differing from r_n at the n-th decimal. Then r is not in the list. □

Corollary 2. Any interval in $\mathbb{R}$ is uncountable.

4.6 Important Facts

$$|2^{\mathbb{N}}| = |\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{R}^n| = |\mathbb{R}^{\mathbb{N}}|$$

for any $n \in \mathbb{N}$.

Remark 4.3. To prove the equality on the above, there are some bridges:

(i) $(0,1) \sim \mathbb{R}$

(ii) $(0,1)^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{N}}$

(iii) $(0,1) \sim (0,1)^{\mathbb{N}}$

The key is $(0,1)^{\mathbb{N}} \hookrightarrow (0,1)$.
Consider $x = (x_1, ..., x_n, ...) \in (0,1)^{\mathbb{N}}$, and write each x_i by the decimal expansion $x_i = .a_{i1}a_{i2}, ...$ Then there is an array

$$\begin{array}{c|ccc} x_1 & a_{11} & a_{12} & \cdots \\ x_2 & a_{21} & a_{22} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Consider a specific way to exhausted the digits in the array, and we obtained a string consisting of a's. This map is a injection. It will be completed after this interleaving technique.

4.7 Advanced Observations and Pitfalls

- $\mathbb{Q}$ is dense in $\mathbb{R}$ but countable.
- $\mathbb{R}$ and $\mathbb{R}^2$ are equinumerous.
- The set of all polynomials with rational coefficients is countable.
- The set of real-valued functions on $\mathbb{R}$ is uncountable.

4.8 Exercises and Reflections

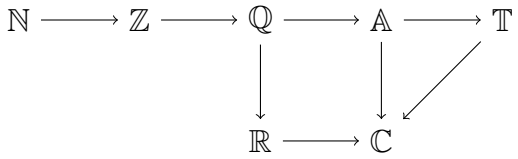
1. Prove that $\mathbb{Z}$ is countable.
2. Show that the set of finite subsets of $\mathbb{N}$ is countable.
3. Use diagonalization to prove the uncountability of $\{0,1\}^{\mathbb{N}}$.
4. Prove that the set of algebraic numbers is countable.
5. Prove $|\mathbb{R}| = 2^{\aleph_0}$.
6. Count $|A \cup B|$ if $|A| = 12$, $|B| = 8$, $|A \cap B| = 5$.
7. Prove: $|\mathcal{P}(A)| = 2^{|A|}$ for any finite set A.
8. Reflection: Is the set of real numbers in $[0,1]$ with finitely many nonzero decimal digits countable?

5 Numbers

5.1 The Hierarchy of Number Systems

The real number system is constructed through a hierarchy of extensions:

- **Natural Numbers:** $\mathbb{N} = \{1, 2, 3, \ldots\}$
- **Integers:** $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- **Rational Numbers:** $\mathbb{Q} = \left\{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}\right\}$
- **Real Numbers:** $\mathbb{R}$ (completion of $\mathbb{Q}$ via Cauchy sequences; includes irrationals)
- **Complex Numbers:** $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$



Remark 5.1. The arrows on the above not entirely denote subset relation, please make sure the meaning of each arrow.

Remark 5.2. For each number a, if there is a polynomial p s.t. a is a root of p, i.e. $p(a) = 0$, we call p is a vanishing/annihilating polynomial of a. Once such special polynomial exists for a given a, we can define a unique object, called minimal polynomial of a, which is the

monic (leading coefficient is 1) annihilating polynomial of a with the lowerest degree,

and such that any other annihilating polynomial of a is a multiple of the minimal polynomial.

Remark 5.3. Each algebraic number has a minimal polynomial in a weaker sense. (What is the weaker sense?)

5.2 Algebraic and Transcendental Numbers

Definition 5.1. A complex number α is **algebraic** if there exists a nonzero polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Otherwise, α is **transcendental**.

- **Algebraic Numbers:** Roots of nonzero integer polynomials. Countable and form a field $\overline{\mathbb{Q}}$.
- **Transcendental Numbers:** Not algebraic. Examples include e, π, and Liouville numbers.

Example 5.1. $\sqrt{2}$ is algebraic: it is a root of $x^2 - 2 = 0$.

5.3 Other Notions of Numbers

- **Constructible Numbers:** A constructible number is a real (or complex) number that can be constructed from the rational number $\mathbb{Q}$ using a **finite** sequence of the operations:
  - addition
  - subtraction
  - multiplication
  - division (by nonzero numbers)
  - square roots

  Remark 5.4. Equivalently, a number is constructible if and only if it can be obtained by straightedge and compass constructions starting from the point 0 and 1 in the complex plane.

  Remark 5.5. Here, let me introduce the frequently used algebraic structure - field. A field structure is closed under addition, subtraction, multiplication, division. The structure of constructible numbers is a field. Try to verify it.

- **Computable Numbers:** Real numbers that can be approximated to any desired precision via algorithm.
- **Definable Numbers:** Uniquely described by a finite statement in a formal language.

5.4 Properties and Examples

(i) **All rational numbers are algebraic.** Every rational number $\frac{p}{q}$ (with $p \in \mathbb{Z}$, $q \in \mathbb{N}$) is a root of the linear polynomial $qx - p \in \mathbb{Z}[x]$.

(ii) **Algebraic numbers include both rational and irrational numbers.** For example, $\sqrt{2}$ is irrational but algebraic, as it is a root of $x^2 - 2 = 0$.

(iii) **The set of algebraic numbers is countable.** This follows because there are countably many polynomials with integer coefficients, and each has finitely many roots.

(iv) **The set of transcendental numbers is uncountable.** Since the real (or complex) numbers are uncountable and the algebraic numbers form a countable subset, it follows that most real (or complex) numbers are transcendental.

5.5 Key Examples of Transcendental Numbers

- **Liouville's constant:**

$$L = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0.11000100000000000000000001\ldots$$

- **Euler's number e:** Transcendental, proven by Hermite (1873).
- **The number π:** Transcendental, proven by Lindemann (1882).
- **Gelfond–Schneider numbers:** $2^{\sqrt{2}}$ is transcendental.
- **Chaitin's constant Ω:** Transcendental and non-computable.

5.6 Historical Milestones

- **1799:** Lambert proves e and π are irrational.
- **1844:** Liouville constructs the first known transcendental numbers.
- **1873:** Hermite proves e is transcendental.
- **1882:** Lindemann proves π is transcendental.
- **1934:** Gelfond–Schneider theorem expands known transcendental numbers.

5.7 Transcendence Proof Sketches

A. Liouville's Theorem

Theorem 5.1 (Liouville, 1844)**.** If α is algebraic of degree $n \geq 2$, then there exists $C > 0$ such that for any rational $\frac{p}{q}$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}.$$

Sketch for L. For each n, L can be approximated by rationals to within $1/10^{(n+1)!}$, better than any algebraic number allows, hence L is transcendental. □

B. Hermite's Proof of Transcendence of e

Uses contradiction and sequences of integer-valued expressions involving e converging to 0.

C. Lindemann–Weierstrass Theorem

Theorem 5.2. If α is a nonzero algebraic number, then e^{α} is transcendental. Since $e^{i\pi} = -1$, this implies π is transcendental.

Corollary 3. It is impossible to square the circle with compass and straightedge.

D. Gelfond–Schneider Theorem

Theorem 5.3 (Gelfond–Schneider, 1934)**.** If a and b are algebraic with $a \neq 0, 1$ and b irrational, then a^b is transcendental.

Example 5.2. $2^{\sqrt{2}}$ is transcendental.

5.8 Measure-Theoretic Perspective

Remark 5.6. Since the real numbers are uncountable and algebraic numbers are countable, almost every real number (in the sense of Lebesgue measure) is transcendental.

5.9 Transcendentals in Advanced Mathematics

- **Transcendental functions:** $\exp(x), \sin(x), \log(x)$, Bessel functions, etc.
- **Number theory:** Algebraic independence, transcendence measures.
- **Logic and computability:** Non-computable transcendental numbers like Chaitin's Ω.
- **Open problems:** Is $e + \pi$ transcendental? Is π^e transcendental?

5.10 Exercises

Exercise 5.1. Prove that $\sqrt[3]{2}$ is algebraic but not rational.

Exercise 5.2. Give an example of a non-constructible algebraic number.

Exercise 5.3. Show that the set of algebraic numbers is countable.

Exercise 5.4. Why is almost every real number transcendental?

5.11 Non-Examples

- **Algebraic:** $\sqrt{2}$, i, $\frac{1}{2}$ (roots of integer polynomials).
- **Rational numbers:** A strict subset of algebraic numbers.

5.12 Summary

$$\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{F}_{\text{const}} \to \mathbb{A} \to \text{Computable} \to \text{Definable} \to \mathbb{C}$$

6 Structures

Discrete mathematics underpins computer science, logic, and combinatorics. Its two most fundamental notions are **operations** and **relations**, which give rise to a variety of algebraic and order-theoretic systems. We develop them here in four stages: operations on sets, relations on sets (and their algebra), special classes of relations, and abstract algebraic structures.

6.1 Operations on Sets

6.1.1 Definition

Definition 6.1 (Operation)**.** Let A be a set. An *n–ary operation* on A is a function

$$f : A^n \longrightarrow A.$$

Special cases:

- *Unary*: $f \colon A \to A$.
- *Binary*: $* \colon A \times A \to A$.

6.1.2 Examples

- $(\mathbb{Z}, +)$: addition is binary.
- $(\mathcal{P}(A), \cup)$: union is binary.
- $(\{0,1\}, \neg)$: logical NOT is unary.
- $(\mathbb{N}, \max)$: $\max(a, b)$ is binary.

6.1.3 Properties of Binary Operations

Commutativity $a * b = b * a$.

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

Identity $\exists e \in A \; \forall a : \; a * e = e * a = a$.

Inverse $\forall a \in A, \; \exists b \in A : \; a * b = b * a = e$.

Nilpotency (with index n) there is least positive integer n such that $\forall a_1, ..., a_n \in A$: $a_1 * \cdots * a_n = e$

Idempotency $\forall a \in A : a * a = a$

Absorption (between $\wedge, \vee$) $\forall a, b \in A : a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$

Remark 6.1. Please specify the meaning of the following terminologies in mathematical texts: “dimension”, “order”, “rank”, “degree”, “multiplicity”, “index”.

6.2 Relations on Sets

6.2.1 Definitions

Definition 6.2 (Relation)**.** A *relation* R from A to B is a subset $R \subseteq A \times B$. If $A = B$, it is a *binary relation* on A.

Definition 6.3 (Domain & Image)**.**

$$\mathrm{dom}(R) = \{a \in A : \exists b\,(a,b) \in R\}, \quad \mathrm{im}(R) = \{b \in B : \exists a\,(a,b) \in R\}.$$

6.2.2 Examples

$$=,\ <,\ |\ ,\ \subseteq,\ \equiv \pmod n,\ \ldots$$

6.2.3 Properties of Binary Relations

Reflexive $(a,a) \in R$ for all $a \in A$.

Irreflexive $(a,a) \notin R$ for all $a \in A$.

Symmetric $(a,b) \in R \implies (b,a) \in R$.

Antisymmetric $(a,b),(b,a) \in R \implies a = b$.

Transitive $(a,b),(b,c) \in R \implies (a,c) \in R$.

6.2.4 Representations

- *Linear representation*: $M \in \{0,1\}^{|A|\times|A|}$.

  Remark 6.2. What if A is finite, countable and uncountable?

- *Digraph*: vertices A, arrow $a \to b$ iff $(a,b) \in R$.

6.2.5 Algebra of Relations

Let $\mathrm{Rel}(A) = \mathcal{P}(A \times A)$. For $R, S \subseteq A \times A$ define

$$\Delta_A = \{(a,a) : a \in A\}, \qquad R^{-1} = \{(b,a) : (a,b) \in R\},$$
$$R \circ S = \{(x,z) : \exists y,\ (x,y) \in S,\ (y,z) \in R\}, \quad R^0 = \Delta_A, \quad R^{n+1} = R \circ R^n.$$

$$R^{\mathrm{refl}} = R \cup \Delta_A, \quad R^{\mathrm{sym}} = R \cup R^{-1}, \quad R^+ = \bigcup_{n \geq 1} R^n.$$

Remark 6.3. $(\mathrm{Rel}(A), \circ, \Delta_A)$ is a monoid.

6.2.6 Special Classes of Relations

Equivalence Relations A relation that is reflexive, symmetric, and transitive. Each $a \in A$ defines an *equivalence class*

$$[a] = \{b \in A : a \sim b\},$$

and these classes partition A.

Partial Orders A relation that is reflexive, antisymmetric, and transitive. A *poset* is $(A, \leq)$, often visualized by a Hasse diagram.

6.3 Algebraic Structures

6.3.1 Signatures

Definition 6.4 (Signature)**.** A *signature* is a set

$$\Sigma = \{\, (f_i, n_i) \mid i \in I\},$$

where each f_i is an operation symbol of arity $n_i \in \mathbb{N}$.

Definition 6.5 (Σ–Algebra)**.** Given Σ, a Σ*–algebra* is a nonempty set A together with for each $f_i \in \Sigma$ a function

$$f_i : A^{n_i} \to A.$$

We denote it $(A, \{(f_i, n_i)\}_{i \in I})$.

6.3.2 Fundamental Examples

Example 6.1 (Group)**.** $\Sigma_{\text{grp}} = \{e : 0,\ (\ )^{-1} : 1,\ \cdot : 2\}$. A *group* is $(G, e, (\ )^{-1}, \cdot)$ satisfying associativity, identity, and inverses.

Example 6.2 (Ring)**.** $\Sigma_{\text{ring}} = \{0 : 0,\ 1 : 0,\ -(\ ) : 1,\ + : 2,\ \cdot : 2\}$. A *ring* is $(R, 0, 1, -(\ ), +, \cdot)$ where $(R, +)$ is an abelian group, $(R, \cdot)$ is a monoid, and $\cdot$ distributes over $+$.

Example 6.3 (Lattice)**.** $\Sigma_{\text{lat}} = \{\wedge : 2,\ \vee : 2\}$. A *lattice* is $(L, \wedge, \vee)$ satisfying commutativity, associativity, idempotency, and absorption.

July 11, 2025

6.3.3 Boolean Algebras

Definition 6.6 (Boolean Algebra)**.** A *Boolean algebra* is a distributive lattice with least element 0, greatest element 1, and where every element has a complement.

Theorem 6.1. In a Boolean algebra, each element has a unique complement.

6.4 Algebraic Structures on the Set of All Relations

Let A be any set, and define

$$\mathrm{Rel}(A) \;:=\; \mathcal{P}\big(A \times A\big),$$

the collection of all binary relations on A.

1. Boolean–Algebra Structure

Definition 6.7. For $R, S \in \mathrm{Rel}(A)$, define

$$R \vee S \;:=\; R \cup S, \quad R \wedge S \;:=\; R \cap S, \quad R^{c} \;:=\; (A \times A) \setminus R.$$

The constants are $\bot = \varnothing$ and $\top = A \times A$.

Proposition 3. $\big(\mathrm{Rel}(A),\, \vee, \wedge, {}^{c},\, \bot, \top\big)$ is a Boolean algebra. In particular:

(i) Closed under $\cup, \cap$, and complement.

(ii) $\vee, \wedge$ are associative, commutative, distributive.

(iii) For every R, $R \vee R^{c} = \top$ and $R \wedge R^{c} = \bot$.

Sketch of proof. All of these follow from the usual set-theoretic laws for $\cup, \cap$ and complementation in $\mathcal{P}(A \times A)$. □

2. Relational Composition Monoid

Definition 6.8. The *composition* of R and S is

$$R \circ S \;:=\; \{(x, z) \in A \times A : \exists\, y \in A,\, (x, y) \in S \wedge (y, z) \in R\}.$$

The *identity relation* is $\Delta_A = \{(a, a) : a \in A\}$.

Proposition 4. $\big(\mathrm{Rel}(A),\, \circ, \Delta_A\big)$ is a (generally non-commutative) monoid:

(i) $\circ$ is associative: $(R \circ S) \circ T = R \circ (S \circ T)$.

(ii) Δ_A is a two-sided unit: $\Delta_A \circ R = R = R \circ \Delta_A$.

Sketch of proof. Follows directly from the definition of relational composition and the fact that Δ_A picks out exactly those pairs needed for an identity. □

3. Example

Let $A = \{1, 2\}$, and

$$R = \{(1, 2)\}, \quad S = \{(2, 1), (2, 2)\}.$$

Then

$$R \vee S = \{(1, 2), (2, 1), (2, 2)\}, \quad R \circ S = \{(1, 1), (1, 2)\},$$

and $\Delta_A = \{(1, 1), (2, 2)\}$, which indeed acts as identity under $\circ$.

6.5 Interplay of Operations and Relations

- Operations often satisfy relational laws (e.g. associativity viewed via a ternary relation).
- Relations form an algebra under union, intersection, complement, and composition.
- Equivalence relations partition sets; orders organize them.
- Digraphs provide visual models for relations; algebraic operations can transform and analyze these graphs.

7 Canonical Forms and Invariants

This section explores how symmetries and equivalence relations can be studied through the concepts of *invariants* and *canonical forms*, which provide tools for classification, simplification, and computation in discrete mathematics.

7.1 Invariants

Definition 7.1 (Invariant)**.** Let G be a group acting on a set X. A function $f : X \to Y$ is called a G**-invariant** if

$$f(g \cdot x) = f(x), \quad \text{for all } g \in G,\, x \in X.$$

That is, f is constant on each G-orbit.

Example 7.1. Let $G = S_n$ (the symmetric group) act on $X = \mathbb{R}^n$ by permuting coordinates:

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

Then $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n$ is S_n-invariant since permutations do not change the sum.

Remark 7.1. Invariants arise naturally when studying symmetries, group actions, and equivalence classes. They serve to classify or distinguish objects up to symmetry.

7.2 Complete Systems of Invariants

Definition 7.2 (Complete System of Invariants)**.** Let G act on a set X. A collection of invariants $f_1, \ldots, f_k : X \to Y$ is called a **complete system of invariants** if

$$f_1(x) = f_1(x'),\ \ldots,\ f_k(x) = f_k(x') \quad \Longrightarrow \quad x' \in G \cdot x.$$

That is, two elements are in the same orbit if and only if all the invariants agree.

Example 7.2. For the S_n-action on $\mathbb{R}^n$, the elementary symmetric polynomials

$$e_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}, \quad k = 1, \ldots, n,$$

form a complete system of invariants. Two vectors are permutations of each other if and only if their elementary symmetric polynomials agree.

Theorem 7.1 (Fundamental Theorem of Symmetric Polynomials)**.** Every symmetric polynomial in n variables can be written as a polynomial in the elementary symmetric polynomials.

Exercise 7.1. Let $G = \mathbb{Z}_2$ act on $\mathbb{R}^2$ by swapping coordinates: $(x, y) \mapsto (y, x)$. Find a complete system of invariants.

Remark 7.2. Finding a complete system of invariants provides a full solution to the orbit classification problem under a group action.

7.3 Applications of Invariants

- **Invariant theory** studies polynomial invariants and their generators.
- **Combinatorics:** Invariants help solve game, puzzle, and coloring problems.
- **Geometry:** Quantities like length, area, and volume are invariant under certain transformations.
- **Classification:** Complete invariants distinguish objects up to symmetry.

7.4 Canonical Forms

Definition 7.3 (Canonical Form)**.** A **canonical form** is a unique or standard representative from each equivalence class of objects. It allows for simplification, classification, and computation by reducing equivalent objects to a common form.

Remark 7.3. Canonical forms appear in linear algebra, graph theory, logic, automata, and many other areas of discrete mathematics.

Motivation and Role

- Many mathematical objects are considered up to an equivalence (e.g., isomorphism, permutation).
- Canonical forms reduce comparison to checking equality of representatives.
- They help automate equivalence tests in algorithms and symbolic computation.

7.5 Examples of Canonical Forms

(1) **Sets:** Remove duplicates and ignore order: $\{3, 1, 2, 1\} \to \{1, 2, 3\}$.

(2) **Boolean Functions:** DNF and CNF are canonical (up to reordering).

(3) **Matrices:** Reduced row echelon form (RREF), Jordan canonical form.

(4) **Equivalence Relations:** Canonical labeling of equivalence classes using representatives.

(5) **Graphs:** Canonical adjacency matrices or outputs from graph isomorphism algorithms.

(6) **Permutations:** Standard cycle notation with sorted cycles and minimal elements.

Example 7.3. Let $A = \{3, 1, 2, 1, 2\}$. Its canonical form as a set is $\{1, 2, 3\}$.

Example 7.4. The matrix $M = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ has RREF $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$.

7.6 Canonical Forms and Computation

- Canonical forms enable efficient equivalence testing and classification.
- They are fundamental in symbolic computation, algebra systems, and coding theory.
- Computing canonical forms can be difficult (e.g., graph isomorphism problem).

Exercise 7.2. Find the canonical form (as a set) of the multiset $\{a, b, a, c, b, c\}$.

Exercise 7.3. Write the Boolean function $f(x, y) = (x \vee y) \wedge (\neg x \vee y)$ in CNF.

Remark 7.4. Canonical forms may not always be strictly unique (e.g., up to term order), but they remove unnecessary variation and make classification feasible.

Theorem 7.2 (Uniqueness of Canonical Forms)**.** If a canonical form is well-defined for an equivalence relation on a set S, then $x \sim y$ if and only if their canonical forms are equal.

Proof. By definition, a canonical form is a unique representative for each equivalence class. Hence, $x \sim y \iff \text{Canon}(x) = \text{Canon}(y)$. □

Exercise 7.4. Under congruence modulo n, what is the canonical form of an integer a?

Remark 7.5. Canonical forms and invariants provide complementary tools: invariants detect equivalence; canonical forms represent equivalence classes.

8 Products

This section surveys a variety of algebraic products used across linear algebra, multilinear algebra, and complex analysis. Each of these products generalizes or extends the notion of multiplication in different mathematical contexts.

8.1 Complex Multiplication

Definition 8.1 (Complex Multiplication)**.** Let $z_1 = a+bi$ and $z_2 = c+di$ be two complex numbers. Their product is defined by

$$z_1 z_2 = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Remark 8.1. Complex multiplication encodes both length (modulus) and angle (argument) multiplication in the complex plane.

8.2 Dot Product (Inner Product)

Definition 8.2 (Dot Product)**.** Given vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, their **dot product** (or **inner product**) is defined by

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i.$$

Remark 8.2. The dot product is bilinear, symmetric, and induces the Euclidean norm: $\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}}$.

8.3 Cross Product

Definition 8.3 (Cross Product)**.** For vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$, their **cross product** is

$$\mathbf{u} \times \mathbf{v} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} = (u_2v_3 - u_3v_2)\mathbf{i} + (u_3v_1 - u_1v_3)\mathbf{j} + (u_1v_2 - u_2v_1)\mathbf{k}.$$

Remark 8.3. The cross product is anti-symmetric and yields a vector orthogonal to both $\mathbf{u}$ and $\mathbf{v}$. It is only defined in $\mathbb{R}^3$ (and in $\mathbb{R}^7$ in a more abstract sense).

8.4 Tensor Product

Definition 8.4 (Tensor Product)**.** Let V and W be vector spaces over a field $\mathbb{F}$. The **tensor product** $V \otimes W$ is a vector space generated by formal expressions $v \otimes w$ with $v \in V, w \in W$, satisfying bilinearity:

$$(av_1 + bv_2) \otimes w = a(v_1 \otimes w) + b(v_2 \otimes w), \quad v \otimes (aw_1 + bw_2) = a(v \otimes w_1) + b(v \otimes w_2).$$

Example 8.1. If $V = W = \mathbb{R}^n$, then $V \otimes W \cong \mathbb{R}^{n \times n}$, the space of $n \times n$ matrices.

8.5 Wedge (Exterior) Product

Definition 8.5 (Wedge Product)**.** Let V be a vector space over $\mathbb{F}$. The **exterior algebra** $\bigwedge V$ is generated by symbols $v_1 \wedge \cdots \wedge v_k$ that are anti-symmetric:

$$v_i \wedge v_j = -v_j \wedge v_i, \quad \text{and} \quad v \wedge v = 0.$$

In particular, for $u, v \in V$, the **wedge product** is defined by

$$u \wedge v = u \otimes v - v \otimes u.$$

Remark 8.4. The wedge product encodes oriented areas in $\mathbb{R}^2$, volumes in $\mathbb{R}^3$, and more generally forms the basis of differential forms.

8.6 Hadamard Product

Definition 8.6 (Hadamard Product)**.** Given matrices $A = (a_{ij})$ and $B = (b_{ij})$ of the same dimensions, the **Hadamard product** is the entrywise product:

$$(A \circ B)_{ij} = a_{ij} b_{ij}.$$

Remark 8.5. The Hadamard product is used in statistics, signal processing, and neural networks.

8.7 Kronecker Product

Definition 8.7 (Kronecker Product)**.** Let A be an $m \times n$ matrix and B a $p \times q$ matrix. The **Kronecker product** $A \otimes B$ is the $mp \times nq$ block matrix:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}.$$

Example 8.2. Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 5 \\ 6 & 7 \end{pmatrix}$. Then

$$A \otimes B = \begin{pmatrix} 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \\ 0 & 15 & 0 & 20 \\ 18 & 21 & 24 & 28 \end{pmatrix}.$$

8.8 Cauchy Product

Definition 8.8 (Cauchy Product)**.** Given two sequences $\{a_n\}, \{b_n\}$, their **Cauchy product** $\{c_n\}$ is defined by

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

If $A(x) = \sum_{n=0}^{\infty} a_n x^n$ and $B(x) = \sum_{n=0}^{\infty} b_n x^n$ are power series, then their product is

$$A(x)B(x) = \sum_{n=0}^{\infty} c_n x^n.$$

Remark 8.6. The Cauchy product is fundamental in the study of generating functions and power series convergence.

9 Polynomial-like Structures

Polynomial rings, and the various ways we extend them (Laurent, rational, formal power series), form a hierarchy of ring-theoretic constructions. We proceed from ordinary polynomials to their most general formal expansions.

9.1 Classical Polynomial Rings

9.1.1 Graded Structure

Definition 9.1 (Graded Ring)**.** A ring R is *graded* if

$$R = \bigoplus_{n \geq 0} R_n, \quad R_n \cdot R_m \subseteq R_{n+m}.$$

Elements of R_n are *homogeneous of degree* n.

Example 9.1. For a field K,

$$K[x] = \bigoplus_{n \geq 0} K x^n, \quad K[x_1, \ldots, x_r]_d = \operatorname{span}_K \{ x_1^{a_1} \cdots x_r^{a_r} : a_1 + \cdots + a_r = d \}.$$

Exercise 9.1. Show $\dim_K K[x,y]_d = \binom{d+1}{1}$ and, more generally, $\dim_K K[x_1, \ldots, x_r]_d = \binom{d+r-1}{r-1}$.

9.1.2 Tensor Products

Definition 9.2 (Tensor Product of K-Algebras)**.** If A, B are K-algebras, then $A \otimes_K B$ is a K-algebra with

$$(a_1 \otimes b_1)\,(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2).$$

Theorem 9.1.

$$K[x_1, \ldots, x_m] \otimes_K K[y_1, \ldots, y_n] \;\cong\; K[x_1, \ldots, x_m, y_1, \ldots, y_n].$$

Proposition 5 (Induced Grading)**.** If $A = \bigoplus A_i$ and $B = \bigoplus B_j$, then

$$(A \otimes_K B)_n = \bigoplus_{i+j=n} A_i \otimes_K B_j.$$

Exercise 9.2. Describe $(K[x] \otimes_K K[y])_3$ and compute its dimension over K.

9.2 Laurent Polynomial Rings

Definition 9.3 (Laurent Polynomial Ring)**.** For a ring R,

$$R[x, x^{-1}] = \Big\{ \sum_{i=m}^{n} a_i x^i : m, n \in \mathbb{Z},\ a_i \in R \Big\},$$

graded by $\deg(x^k) = k$.

Proposition 6. Units in $R[x, x^{-1}]$ are precisely $u\, x^k$ with $u \in R^\times$.

Exercise 9.3. Over $R = \mathbb{Z}$, is $x^{-2} + 3 + x^4$ invertible in $R[x, x^{-1}]$?

9.3 Field of Rational Functions

Definition 9.4 (Rational Function Field)**.** Let F be a field. Then

$$F(x) = \left\{ \tfrac{P(x)}{Q(x)} : P, Q \in F[x],\, Q \not\equiv 0 \right\} / \sim$$

with $P_1/Q_1 \sim P_2/Q_2$ iff $P_1Q_2 = P_2Q_1$.

Definition 9.5 (Degree)**.** If $R = P/Q$ in lowest terms, $\deg R = \max\{\deg P, \deg Q\}$.

Theorem 9.2 (Partial Fraction Decomposition)**.** For $\deg P < \deg Q$ and $Q = \prod_{i=1}^{k} (x - \alpha_i)^{m_i}$,

$$\frac{P}{Q} = \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{A_{i,j}}{(x - \alpha_i)^j}.$$

Exercise 9.4. Decompose $\dfrac{2x+3}{(x-1)(x+2)}$ into partial fractions.

9.4 Quotient Rings and Localizations

9.4.1 Quotient Rings

Definition 9.6 (Ideal & Quotient)**.** $I \lhd R$ is an ideal. Then

$$R/I = \{r + I : r \in R\}, \quad (r+I)(s+I) = rs + I.$$

Example 9.2. $\mathbb{Z}/n\mathbb{Z}$ and $k[x]/(f(x))$.

9.4.2 Localization

Definition 9.7 (Localization at S)**.** If $S \subseteq R$ multiplicative,

$$S^{-1}R = \left\{ \tfrac{r}{s} : r \in R, s \in S \right\} / \sim,$$

with $\frac{r}{s} \sim \frac{r'}{s'} \iff \exists\, u \in S,\ u(rs' - r's) = 0$.

Exercise 9.5. Show $\mathbb{Z}_{(p)} \cong (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$ and that $R \to S^{-1}R$ is injective when R is a domain.

9.5 Formal Power Series

Definition 9.8 (Formal Power Series)**.**

$$R[\![x]\!] = \left\{ \sum_{n=0}^{\infty} a_n x^n : a_n \in R \right\},$$

with Cauchy-convolution multiplication.

Proposition 7. $f(x)$ is a unit iff its constant term $a_0 \in R^\times$.

Example 9.3. $\dfrac{1}{1-x} = \sum_{n \geq 0} x^n, \quad e^x = \sum_{n \geq 0} \frac{x^n}{n!} \in \mathbb{Q}[\![x]\!]$.

Exercise 9.6. Given $f(x) = \sum a_n x^n$, construct its inverse recursively when a_0 is invertible.

9.6 Formal Laurent Series

Let K be a field. Recall that the ring of formal power series is

$$K[\![x]\!] = \{\sum_{n=0}^{\infty} a_n x^n : a_n \in K\}.$$

Definition 9.9 (Formal Laurent Series)**.** The *ring of formal Laurent series* over K, denoted $K((x))$, consists of all expressions of the form

$$f(x) \;=\; \sum_{n=N}^{\infty} a_n\, x^n,$$

where $N \in \mathbb{Z}$ may be negative, and each $a_n \in K$. Addition and multiplication are defined exactly as for power series (with only finitely many negative-indexed terms).

Example 9.4.

- The series
$$x^{-3} + 2x^{-1} + 5 + 7x + 4x^2 + \cdots$$
is in $K((x))$ but *not* in $K[\![x]\!]$.
- Every element of $K[\![x]\!]$ is a Laurent series with $N \geq 0$.

Proposition 8. $K((x))$ is a field. Its inverse is obtained by factoring off the lowest nonzero power: if

$$f(x) = x^N\, u(x), \quad u(0) \neq 0,$$

then

$$f(x)^{-1} = x^{-N}\, u(x)^{-1},$$

where $u(x)^{-1} \in K[\![x]\!]$ exists by the usual power-series inversion.

Remark 9.1. There is a natural inclusion

$$K[x] \;\subset\; K[\![x]\!] \;\subset\; K((x)),$$

and $K((x))$ serves as the field of fractions of the discrete valuation ring $K[\![x]\!]$.

9.7 Quotient Field of the Ring of Formal Power Series

Let K be a field and consider the ring of formal power series

$$K[\![x]\!] \;=\; \Big\{\, a_0 + a_1 x + a_2 x^2 + \cdots : a_i \in K \Big\},$$

which is an integral domain but not a field. Its field of fractions (quotient field) can be described concretely as the ring of formal Laurent series.

Definition 9.10 (Field of Fractions)**.** If R is an integral domain, its *field of fractions* $\mathrm{Frac}(R)$ is the set of equivalence classes of pairs (f, g) with $f, g \in R$, $g \neq 0$, under the relation

$$(f, g) \sim (f', g') \quad \Longleftrightarrow \quad fg' = f'g.$$

Addition and multiplication are defined in the usual way:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'}, \quad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}.$$

Definition 9.11 (Formal Laurent Series)**.** A *formal Laurent series* over K is an expression

$$\sum_{n=N}^{\infty} a_n x^n, \quad a_n \in K,\ N \in \mathbb{Z},$$

with only finitely many negative-indexed coefficients nonzero. We denote the set of all such series by

$$K((x)) \;=\; \Big\{ \sum_{n=N}^{\infty} a_n x^n : a_n \in K,\ N \in \mathbb{Z} \Big\}.$$

Proposition 9. $K((x))$ is a field, and in fact is canonically isomorphic to the field of fractions of $K[\![x]\!]$:

$$\mathrm{Frac}\big(K[\![x]\!]\big) \;\cong\; K((x)).$$

Sketch of Proof. Every nonzero $f \in K[\![x]\!]$ can be written as $x^N u(x)$ where $u(0) \neq 0$, hence invertible in $K[\![x]\!]$. Thus any fraction $\frac{f}{g}$ with $g \neq 0$ becomes a Laurent series in $K((x))$. Conversely, every Laurent series $\sum_{n=N}^{\infty} a_n x^n$ can be written as

$$x^N \, \frac{\sum_{m=0}^{\infty} a_{m+N} x^m}{1},$$

exhibiting it as a fraction of power series. One checks these constructions are inverses. □

Example 9.5. Over $\mathbb{R}$, an element of $\mathbb{R}((x))$ might be

$$x^{-2} - 3x^{-1} + 5 - 7x + 2x^3 + \cdots,$$

which is not in $\mathbb{R}[\![x]\!]$ but becomes legitimate once inverses of powers of x are admitted.

Remark 9.2. The valuation $\nu \colon K((x))^{\times} \to \mathbb{Z}$ defined by

$$\nu\Big(\sum_{n=N}^{\infty} a_n x^n \Big) \;=\; N$$

makes $K((x))$ into a discrete valuation field, with valuation ring exactly $K[\![x]\!]$.

9.8 Formal Frobenius Series and Its Quotient Field

Let K be a field of characteristic $p > 0$, and let x be an indeterminate. Recall that the Frobenius endomorphism on K is the map $F \colon K \to K$ given by $a \mapsto a^p$.

Definition 9.12 (Ring of Formal Frobenius Series)**.** We define the *ring of formal Frobenius series* over K as

$$\mathrm{Frob}_K \;=\; \left\{ f(x) \;=\; \sum_{n=0}^{\infty} a_n \, x^{p^n} \;\middle|\; a_n \in K \right\} \;\subset\; K[\![x]\!].$$

Addition and multiplication are those inherited from the formal power series ring $K[\![x]\!]$.

Proposition 10. Frob_K is a subring of $K[\![x]\!]$, stable under the Frobenius map

$$F\big(f(x)\big) \;=\; \sum_{n=0}^{\infty} a_n^p \, x^{p^{n+1}}.$$

Proof. Closure under addition is immediate. For multiplication, note that

$$\Big(\sum_{i\ge 0} a_i x^{p^i}\Big)\Big(\sum_{j\ge 0} b_j x^{p^j}\Big) = \sum_{k\ge 0}\Big(\sum_{i+j=k} a_i b_j\Big)\, x^{p^k},$$

since $p^i + p^j = p^{\min\{i,j\}}(1+p^{|i-j|})$ and cross-terms with distinct exponents combine into the allowed form after reindexing by $k = \min\{i,j\} + |i-j|$. Moreover, applying F to each coefficient preserves the same exponent pattern. □

Definition 9.13 (Quotient Field of Frobenius Series)**.** The *field of fractions* (or *quotient field*) of Frob_K is

$$Q\big(\mathrm{Frob}_K\big) \;=\; \big\{\, g(x)/h(x) \;\big|\; g(x), h(x) \in \mathrm{Frob}_K,\; h(0)\neq 0\big\} \;\subset\; K((x)),$$

where $K((x))$ denotes the field of formal Laurent series.

Theorem 9.3. Every element of $Q(\mathrm{Frob}_K)$ can be uniquely written in the form

$$\frac{\displaystyle\sum_{i=0}^{m} a_i\, x^{p^i}}{\displaystyle\sum_{j=0}^{n} b_j\, x^{p^j}} \quad \text{with } a_i, b_j \in K,\; b_0 \neq 0.$$

Sketch of Proof. Since Frob_K is a GCD domain (it is a subring of the UFD $K[\![x]\!]$ closed under taking p-power exponents), any two series have a greatest common divisor of the same form. One then follows the usual construction of the field of fractions and checks uniqueness by clearing common factors in $K[x^{p^0}, x^{p^1}, \dots]$. □

Example 9.6. Over $K = \mathbb{F}_p$, the field $\mathrm{Frob}_{\mathbb{F}_p}$ is

$$\big\{a_0 + a_1 x^p + a_2 x^{p^2} + \cdots\big\},$$

and its quotient field $Q(\mathrm{Frob}_{\mathbb{F}_p})$ consists of expressions like

$$\frac{1+x^p}{1-x^{p^2}} \;=\; \sum_{k=0}^{\infty} x^{p^2 k} + \sum_{k=0}^{\infty} x^{p^2 k + p},$$

which indeed lies in $\mathbb{F}_p((x))$.

9.9 Differential Calculus

Let

$$f(x) = \sum_{k\ge 0} a_k x^k \;\in\; K[\![x]\!].$$

Substitution of $x+t$ for x yields a power series in two variables:

$$f(x+t) = a_0 + a_1(x+t) + a_2(x+t)^2 + \cdots = \sum_{m\ge 0} f_m(x)\, t^m, \tag{3.5}$$

where each $f_m(x) \in K[\![x]\!]$ is uniquely determined by f :contentReference[oaicite:0]index=0.

Exercise 9.7 (3.4)**.** Check that $f_0(x) = f(x)$.

The coefficient $f_1(x)$ is called the *derivative* of f, denoted f' or $\frac{d}{dx}f$, and is uniquely characterized by

$$f(x+t) = f(x) + f'(x)\,t + (\text{terms divisible by } t^2) \quad \text{in } K[\![x,t]\!]. \tag{3.6}$$

By dividing $f(x+t) - f(x)$ by t and evaluating at $t = 0$, one obtains the classical formula

$$f'(x) = \sum_{k\geq 1} k\,a_k\,x^{k-1} = a_1 + 2a_2x + 3a_3x^2 + \cdots . \tag{3.7}$$

Example 9.7 (Series with Zero Derivative)**.** Assume K is an integral domain. If $\operatorname{char} K = 0$, then $f' = 0$ if and only if f is constant. If $\operatorname{char} K = p > 0$, the derivation kills exactly those monomials whose degree is divisible by p, so $f' = 0$ if and only if $f(x) = g(x^p)$ for some $g \in K[\![x]\!]$ (and likewise in $K[x]$). :contentReference[oaicite:1]index=1

Lemma 1. Over a prime $p \in \mathbb{N}$, the polynomials with zero derivative in $\mathbb{F}_p[x]$ are precisely the pth powers $g(x)^p$, $g \in \mathbb{F}_p[x]$.

Proof. Since the Frobenius endomorphism $\varphi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$, $h \mapsto h^p$, acts identically on coefficients, its image consists exactly of those f satisfying $f' = 0$. :contentReference[oaicite:2]index=2 □

Proposition 11 (Differentiation Rules)**.** For a commutative ring K with unit and all $f, g \in K[x]$, $\alpha \in K$, one has

$$(\alpha f)' = \alpha\, f', \tag{3.8}$$

$$(f+g)' = f' + g', \tag{3.9}$$

$$(fg)' = f'\,g + f\,g', \tag{3.10}$$

$$\big(f \circ g\big)'(x) = g'(x)\, f'\big(g(x)\big), \tag{3.11}$$

$$(f^{-1})' = -\frac{f'}{f^2} \quad (\text{for } f \text{ invertible in } K[x]). \tag{3.12}$$

Proof. The first two follow directly from (3.7). The Leibniz rule (3.10) comes from expanding $f(x+t)\,g(x+t)$ and collecting terms in t. The chain rule (3.11) and inverse rule (3.12) are obtained by similar expansions. :contentReference[oaicite:3]index=3 □

10 Further Reading and References

General Discrete Mathematics

- Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, McGraw-Hill.
  A widely used introductory text with comprehensive coverage of logic, proofs, counting, graphs, and algorithms.
- Richard Johnsonbaugh, *Discrete Mathematics*, Pearson.
  Emphasizes proof techniques and algorithmic thinking.
- Ralph P. Grimaldi, *Discrete and Combinatorial Mathematics*, Addison-Wesley.
  Rich in combinatorics and graph theory, with a theoretical focus.
- Susanna S. Epp, *Discrete Mathematics with Applications*.
  Especially strong on logical reasoning and foundational concepts.
- J. L. Hein, *Discrete Structures, Logic, and Computability*.
  Includes extensive treatment of logic, automata, and computability.
- J. L. Gerstein, *Introduction to Mathematical Structures and Proofs*.
  A transition text emphasizing proof construction and set-theoretic foundations.
- B. A. Davey and H. A. Priestley, *Introduction to Lattices and Order*.
  An accessible yet rigorous treatment of ordered sets and lattices.

Set Theory and Logic

- T. Jech, *Set Theory*, 3rd ed., Springer.
  A comprehensive graduate-level reference on axiomatic set theory.
- H. B. Enderton, *Elements of Set Theory*.
  A rigorous yet readable undergraduate-level introduction.
- P. Halmos, *Naive Set Theory*.
  A classic informal treatment of fundamental concepts.
- K. Kunen, *Set Theory: An Introduction to Independence Proofs*.
  Focuses on advanced set theory, including forcing and large cardinals.

Algebra and Algebraic Structures

- J. B. Fraleigh, *A First Course in Abstract Algebra*.
  A popular undergraduate text for group, ring, and field theory.
- J. Gallian, *Contemporary Abstract Algebra*.
  Emphasizes intuition and examples, with accessible exposition.
- M. Artin, *Algebra*.
  A geometric and conceptual approach to algebra, suitable for advanced undergraduates.
- S. Lang, *Algebra*.
  An encyclopedic reference for graduate-level abstract algebra.

- D. S. Dummit and R. M. Foote, *Abstract Algebra.*
  A standard, detailed reference with coverage of graded rings and tensor products.
- M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra.*
  Concise and elegant introduction to algebraic geometry foundations.
- D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry.*
  More advanced; ideal for bridging commutative algebra and geometry.

Number Theory and Arithmetic

- I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers.*
  A classical comprehensive introduction.
- G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.*
  Rich in classical results and elegant proofs.
- I. Niven, *Irrational Numbers*, Carus Mathematical Monographs.
  A focused study on irrational and transcendental numbers.
- J. Stillwell, *Elements of Number Theory.*
  Blends historical context with modern theory.
- A. Baker, *Transcendental Number Theory.*
  A standard reference for transcendence results.
- P. Ribenboim, *The Book of Numbers.*
  A tour of numerical curiosities and theory.

Computability and Foundations

- A. M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem," (1936).
  The foundational paper for modern computability theory and Turing machines.

Online and Open-Access Resources

- MIT OpenCourseWare: `https://ocw.mit.edu/courses/mathematics/`
  Includes full lecture notes and video lectures for courses such as 6.042J and 18.100.
- Stacks Project (Algebraic Geometry): `https://stacks.math.columbia.edu/`
  A free, open-source textbook and reference on algebraic geometry, commutative algebra, and category theory.
- Wikipedia Article on Transcendental Numbers: `https://en.wikipedia.org/wiki/Transcendental_number`