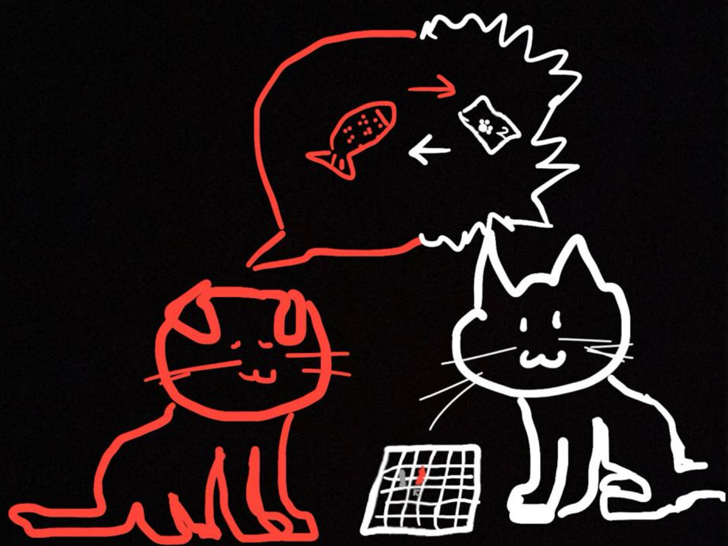
Lecture Notes for a Course in General Equilibrium

Alejandro Melo Ponce



Cover artwork: Sultan Yessirkep
En psspssant (2026)
Digital artwork. Reproduced with permission.

Document Version:
v. 2026-02-26 ᓚ(^. ̫ .^)02:18

Contents

Preface vii

An Abridged Intellectual History of General Equilibrium Theory xi

1 Mathematical Preliminaries 1

1.1 Metric Spaces 3
1.1.1 How and with what to measure distances? 3
1.1.2 Metrics arising from norms in vector spaces 6
1.1.3 Isometries, Metric Subspaces, and more examples 9
1.2 Topological Structure of Metric Spaces 11
1.2.1 Open Balls and Examples 11
1.2.2 Open and Closed Sets in Metric Spaces 16
1.3 Sequences, Complete Spaces, and Separable Spaces 16
1.4 Continuity 16
1.5 Compactness 16
1.6 Connectedness 17
1.7 Convexity 17
1.7.1 Convexity of Sets 17
1.7.2 Separation Theorems 22
1.7.3 Carathéodory and Shapley–Folkman Theorems 31
1.8 Convex, Concave, quasiconcave, and quasiconcave functions 31
1.8.1 Convex functions 31
1.8.2 Properties of Convex Functions 39
1.8.3 Quasiconcave Functions 44
1.9 Homogeneous and Homothetic Functions 47
1.9.1 Homogeneous Functions 47
1.9.2 Homothetic Functions 53
1.10 Correspondences 55
1.10.1 Motivation and Definition of a Correspondence 55
1.10.2 Inverse Images 58
1.11 Fixed point theorems 60

2 Exchange Economies 61

3 Production Economies **63**

4 Core Convergence Results **65**

5 Extensions **67**

A The basics of mathematical logic **69**
A.1 Propositional logic 70
A.2 Logical implication and equivalence 71
A.3 Quantifiers 72
A.4 Statements Involving Quantifiers 74
A.5 Methods of proof 76
A.6 Logical structure of definitions, theorems, and other mathematical results 77

B Sets and Functions **81**
B.1 Naive Set Theory 81
B.2 Functions 85

C The Natural Numbers, Integers, Rationals & Field Axioms **91**
C.1 The Natural Numbers 91
C.2 The Integers, the Rational Numbers, and Field Axioms 97

D Cardinality and Equivalence of Sets **101**
D.1 Cardinality of Sets 101
D.2 Criteria for the equivalence of sets 108
D.3 Cardinal Arithmetic 114

E The Real Numbers **117**
E.1 Why do we need the real numbers? 117
E.2 Another ordered field 119
E.3 Completeness of the real numbers 120
E.4 The Archimedean property of $\mathbb{R}$ 127
E.5 Nested intervals principle 131

F Vector Spaces **137**
F.1 Vector Spaces 137
F.2 Subspaces 140
F.3 Direct Sums 144
F.4 Spanning Sets and Linear Independence 149

G Real Normed Vector Spaces **153**
G.1 Normed Vector Spaces 153
G.2 Spaces with Inner Product 159

H Binary Relations **163**
H.1 Basic Definitions 163
H.2 Preference Relations 164
H.2.1 Notation for Preference Relations 165
H.2.2 Utility Functions 165

Bibliography **167**

Preface

These notes were written for a one-semester advanced course in General Equilibrium taught at Nazarbayev University. They are intended for ambitious students who are interested in microeconomic theory and mathematical economics. Familiarity with consumer and producer theory and constrained optimization is helpful, but not required. What *is* required is a willingness to think formally and abstractly, to work carefully with mathematical notation, and to engage seriously with rigorous arguments. Students uncomfortable with abstraction or unwilling to let mathematics guide intuition may find my approach to the course frustrating.

The central objective of these notes is to present general equilibrium theory as the mathematical backbone of modern microeconomics. General equilibrium is not treated as a computational object or a black box, but as a theoretical structure whose existence, properties, and limitations must be understood. The emphasis throughout is on structure, assumptions, and logical coherence. In particular, the course develops and repeatedly relies on tools from convex analysis, separation theorems, duality, and fixed point theory. These tools recur across many areas of economic theory, including auction theory, mechanism design, information economics, financial economics, and dynamic and repeated games.

The notes are deliberately proof-oriented. Intuition is not abandoned, but it is derived from the mathematics itself rather than from verbal narratives, simplified examples, or numerical simulations. Students should expect abstraction, formal arguments, and careful attention to assumptions. Many technically demanding results are proved in full; others are stated and discussed, with proofs deferred to appropriate outside references. The appendices are meant to serve as a technical resource rather than as material to be read sequentially.

The material is organized into five chapters. The first chapter develops the mathematical preliminaries used throughout the text. The next chapters study exchange economies, production economies, and core convergence results. The final chapter discusses several extensions of the basic general equilibrium framework. While the chapters are ordered logically, some sections may be read independently. The appendix provides useful results and definitions from many areas of mathematics that are needed as background to understand the lecture notes.

Numbering follows a unified chapter–section–item scheme. Within each section, definitions, theorems, propositions, lemmas, remarks, examples, and numbered equations are numbered sequentially in the order in which they appear. Numbered equations are used sparingly and only when they play a structural role in the exposition. Appendices follow the same convention, with chapters labeled by letters. Proofs in this text are concluded using one of the symbols ^. .^)9 or /ᐠ˳‸˳ᐟ\, chosen at random.

Exercises appear throughout the text rather than being systematically collected at the end of each chapter, although in some cases a group of exercises may be gathered at the end of a chapter for convenience. In the appendices, exercises are more often collected toward the end, though some also appear within the discussion itself. This difference reflects the background and reference-oriented role of the appendices, which are meant to support the main development rather than drive it.

Exercises are labeled by section and follow their own letter counter. Some exercises are accompanied by cat-paw (🐾) symbols.[1] These symbols do *not* indicate difficulty. They classify exercises according to the structural role they play in the development of the theory.

- Exercises without a cat-paw are primarily intended for practice and reinforcement of material discussed in the text.
- One-paw (🐾) exercises contain results that will be used later in proofs of subsequent theorems.
- Two-paw (🐾🐾) exercises typically present broader statements, alternative formulations, or useful generalizations. They complement the main line of development but are not logically required for it.
- Three-paw (🐾🐾🐾) exercises explore more abstract extensions or further directions of the theory. They are included for readers interested in deeper structural insights and may require additional mathematical background, though not necessarily greater difficulty once that background is in place.

These notes are a living document and remain in an evolving state. They reflect an ongoing process of refinement shaped by teaching, discussion, and revision over time.

Acknowledgements I am deeply grateful to the teachers from whom I first learned general equilibrium theory, in particular Levent Ülkü and Pradeep Dubey,

[1]Panqueque's Seal of Quality™ applies.

my Ph.D. advisor. I also owe an immense intellectual debt to my mathematics teachers, César Luis García García and Guillermo Grabinsky, from whom I learned real analysis. To César Luis in particular, I owe much of the material that appears in the appendices, which grew out of his remarkable course in real analysis. To Guillermo, I owe not only further training in advanced analysis, but also a refined mathematical taste and an uncompromising commitment to the craft of teaching; from him I learned the standards to which a teacher should aspire.

I owe more than I can adequately express to my wife, Brenda, and to our cat, Panqueque, whose constant and unconditional love has sustained my work and filled my life with light, laughter, and a measure of delightful chaos. Their companionship has been steady, their encouragement unrelenting, their love both bracing and tender.

Above all, my deepest thanks go to my students. From them I learned at least as much as they learned from me; without their curiosity, seriousness, and willingness to wrestle with ideas, these notes would not exist.

An Abridged Intellectual History of General Equilibrium Theory

> "It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest. We address ourselves, not to their humanity but to their self-love, and never talk to them of our own necessities but of their advantages"
>
> ADAM SMITH, *The Wealth of Nations*

General equilibrium theory did not emerge as a purely technical exercise in price theory. It represents the culmination of a long intellectual effort to understand how decentralized economic activity can be mutually consistent, stable, and welfare-relevant. This introduction provides a brief intellectual genealogy of that enterprise, emphasizing the key ideas that culminated in the Arrow–Debreu–McKenzie framework and its cooperative and game-theoretic foundations.

From Coordination to Equilibrium

The intellectual origins of general equilibrium theory lie in a fundamental puzzle about market economies: how can the decentralized decisions of millions of self-interested agents give rise to social order without central coordination?

Adam Smith[1] (1776). The point of departure is Smith (1776)'s celebrated invisible hand metaphor in *The Wealth of Nations*. Smith recognized that markets coordinate economic activity through prices, which serve as signals guiding individual decisions toward socially productive outcomes. Yet Smith's insight remained informal and metaphorical. There was no formal notion of equilibrium, no explicit optimization framework, and no existence question. Smith provided the vision of decentralized coordination, not a theory of competitive equilibrium.

[1] Adam Smith, 1723–1790.

Antoine Augustin Cournot[2] (1838). The first step toward formalization came with Cournot (1838)'s *Recherches sur les principes mathématiques de la théorie des richesses.* Cournot introduced mathematical methods into economics, representing demand and supply as functions and defining equilibrium as the solution to a system of equations. This was, however, a theory of *partial equilibrium.* Cournot analyzed individual markets in isolation, holding the rest of the economy fixed. The economy was not yet conceived as a fully interdependent system.

Léon Walras[3] (1874–1877). The decisive conceptual breakthrough came with Walras (1874)'s *Éléments d'économie politique pure.* Walras transformed the problem by treating all prices as endogenous unknowns and defining equilibrium as the simultaneous clearing of all markets. The economy became a system of equations rather than a collection of isolated problems. Walras introduced the *tâtonnement* process—a hypothetical price adjustment mechanism—to provide an intuitive story of how markets might reach equilibrium. Yet Walras could not prove that his system of equations had a solution. The existence of general equilibrium remained conjectural.

Vilfredo Pareto[4] (1896–1906). Pareto (1896–1897) and Pareto (1906) extended and refined Walras's framework in important ways. He replaced cardinal utility with ordinal preferences, laying the groundwork for modern consumer theory. More fundamentally, Pareto introduced the concept of allocative efficiency that now bears his name. A Pareto-efficient allocation is one in which no agent can be made better off without making another worse off. This notion provided a precise welfare criterion for evaluating market outcomes and became central to welfare economics. Pareto's work established the normative significance of competitive equilibrium, even as the existence question remained open.

Coalitions, Stability, and the Core

While Walras and Pareto focused on competitive equilibrium, an alternative perspective emerged from cooperative game theory.

Francis Ysidro Edgeworth[5] (1881). Edgeworth (1881) introduced a fundamentally different approach in *Mathematical Psychics.* Rather than focusing on

[2] Antoine Augustin Cournot, 1801–1877.
[3] Marie-Esprit-Léon Walras, 1834–1910.
[4] Vilfredo Federico Damaso Pareto, 1848–1923.
[5] Francis Ysidro Edgeworth, 1845–1926.

price-taking behavior, Edgeworth studied allocations that cannot be *blocked* by coalitions of agents. An allocation is in the *core* if no group of agents can reallocate their endowments among themselves and make all group members strictly better off. Edgeworth conjectured that as the economy grows large—through replication of agent types—the core shrinks and converges to the set of competitive equilibria. This conjecture anticipated a deep connection between cooperative stability and competitive markets, but its formal proof would wait over eighty years.

Game Theory and Fixed Points

The mid-twentieth century brought two critical developments: the formalization of strategic interaction and the mathematical tools to prove existence of equilibrium.

John von Neumann[6] and Oskar Morgenstern[7] (1944). Neumann and Morgenstern (1944)'s *Theory of Games and Economic Behavior* provided a rigorous framework for analyzing strategic interaction and a formal foundation for utility maximization under uncertainty. The theory of games introduced the concept of equilibrium as mutual consistency of optimal behavior. This perspective proved essential for subsequent existence proofs in both game theory and competitive markets. Von Neumann's earlier work on fixed-point theorems also provided key mathematical machinery.

John Nash[8] (1950–1951). J. F. Nash (1950) and J. Nash (1951) formalized the concept of equilibrium in non-cooperative games as a fixed point of best-response correspondences. His existence proof relied on Kakutani's fixed-point theorem, exploiting properties of convexity and compactness. A crucial conceptual shift occurred here: equilibrium does not require a dynamic adjustment process or convergence story. It requires only logical consistency—that each agent's choice is optimal given the choices of others. This static, fixed-point perspective would prove central to the existence proofs in general equilibrium theory.

[6] John von Neumann (born János Neumann), 1903–1957.
[7] Oskar Morgenstern, 1902–1977.
[8] John Forbes Nash Jr., 1928–2015.

Existence of Competitive Equilibrium

Kenneth Arrow[9] and Gérard Debreu[10] (1954); Lionel McKenzie[11] (1959). The existence of competitive equilibrium was finally established in the 1950s. Arrow and Debreu (1954) and McKenzie (1959) independently proved existence under standard assumptions of convexity, continuity, and local non-satiation. Debreu (1959)'s *Theory of Value* provided a definitive axiomatic treatment, establishing general equilibrium theory as a rigorously formalized branch of economic theory.

Conceptually, the competitive economy can be viewed as a *generalized game*: consumers choose demand plans, firms choose production plans, and prices coordinate these choices such that markets clear. The mathematical structure of the existence proof closely parallels Nash's equilibrium arguments, relying on fixed-point theorems applied to best-response correspondences in abstract spaces. The Walrasian price mechanism emerges not from a dynamic adjustment process, but from a consistency condition: prices must be such that aggregate demand equals aggregate supply.

The Core Revisited: Large Economies

The connection between competitive equilibrium and cooperative stability was eventually made precise.

Debreu and Scarf[12] (1963). Edgeworth's conjecture was formally proved using replication arguments. Debreu and Scarf (1963) showed that as the economy is replicated—adding more agents of each type—the core shrinks and converges to the set of competitive equilibria. In large economies, competitive prices emerge endogenously from the requirement of coalitional stability.

Robert Aumann[13] (1964–1966). Aumann (1964) and Aumann (1966) extended this result to economies with a continuum of agents. In the continuum limit, the core coincides exactly with the set of competitive equilibria. This established a deep equivalence: competitive markets implement precisely those allocations

[9] Kenneth Joseph Arrow, 1921–2017.
[10] Gérard Debreu, 1921–2004.
[11] Lionel Wilfred McKenzie, 1919–2010.
[12] Herbert Eli Scarf, 1930–2015.
[13] Robert John Aumann, 1930–.

that are immune to blocking by coalitions. The Walrasian price mechanism is not imposed externally; it emerges as the unique stable outcome in large economies.

The Raison d'Être of Studying General Equilibrium

General equilibrium theory is not simply another field within microeconomics. It is the mathematical backbone upon which much of modern microeconomic theory rests.

Studying general equilibrium develops mastery of fundamental tools that reappear throughout economic theory:

- convex analysis and separation theorems,
- duality and supporting prices,
- fixed-point theorems and their applications,
- existence arguments and welfare analysis.

These mathematical techniques are not confined to competitive markets. They form the foundation for auction theory, mechanism design, information economics, financial economics, and game theory (Mas-Colell, Whinston, and Green 1995). The modern theory of repeated games, for instance, relies crucially on compactness, convexity, and fixed-point arguments (Abreu, Pearce, and Stacchetti 1990; Fudenberg and Tirole 1991). Even fields that appear distant from general equilibrium share its mathematical infrastructure.

For this reason, general equilibrium traditionally sits at the beginning of any advanced microeconomic theory sequence. It is both a culmination of the intellectual development of competitive markets and a training program for rigorous economic reasoning. Learning general equilibrium once makes the rest of microeconomic theory more readable, more transparent, and far less intimidating. Fixed-point theorems stop appearing magical, welfare theorems reveal themselves as geometric arguments, and equilibrium concepts across fields expose a shared mathematical structure.

To study modern microeconomic theory without mastering general equilibrium is to read poetry without understanding grammar, to study classical singing without music theory, to ski without edge control, to live without curiosity.[14]

[14] The reader will forgive the proliferation of analogies. The point stands.

Is General Equilibrium a Closed Theory?

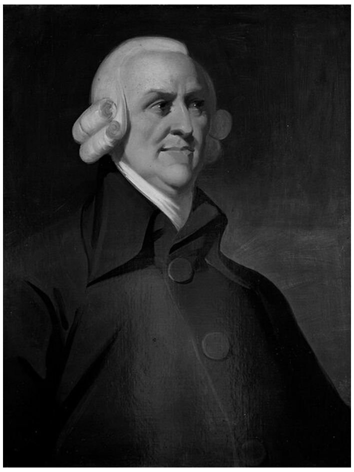
Under the standard Arrow–Debreu assumptions—convexity, local non-satiation, complete markets, perfect competition, and full information—general equilibrium theory can be regarded as a conceptually complete theory of competitive allocation. This framework extends naturally to incorporate uncertainty when asset markets are complete, allowing agents to trade state-contingent claims. Its central results, including equilibrium existence, the fundamental welfare theorems, and core equivalence, are settled. Most subsequent extensions refine this framework rather than overturn it.

Modern economic theory did not move beyond general equilibrium because the theory failed. Rather, it moved beyond because the assumptions became endogenous objects of study. The game-theoretic and informational revolutions introduced strategic interaction, private information, and institutional detail. These developments fragmented the competitive benchmark rather than replacing it.

In this sense, general equilibrium is no longer the central object of active research. But it remains the *limit object* of economic theory. As strategic power becomes diluted, markets grow large, and informational frictions diminish, economic models converge toward general equilibrium logic. This is why the mathematical tools originating in general equilibrium theory—convexity, duality, fixed-point arguments, and supporting prices—continue to appear across economic theory and applied work.

Today, general equilibrium serves as the organizing benchmark of economics. It provides the reference point against which departures from perfect competition are defined and evaluated. Its mathematical structure underlies modern work in auctions, market design, information economics, macroeconomics, and finance, even when the models themselves are explicitly strategic or informational.

General equilibrium is not where modern research happens, but it is where modern economic reasoning comes from.

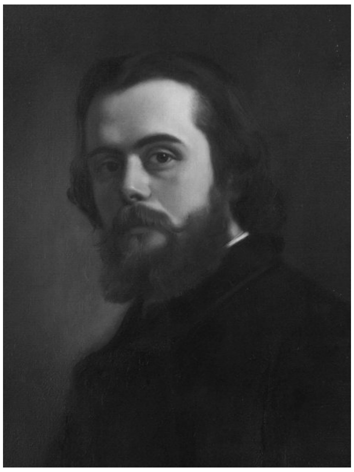


Adam Smith

1723–1790

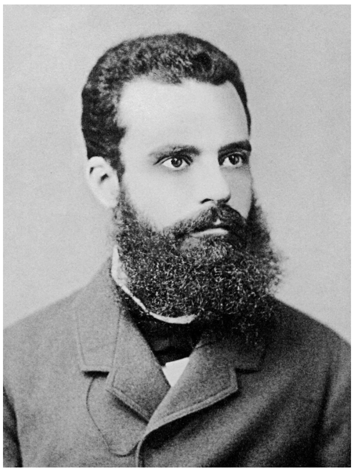
Antoine Augustin Cournot

1801–1877



Léon Walras

1834–1910



Vilfredo Pareto

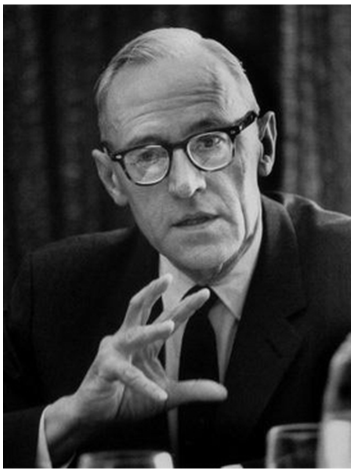
1848–1923

Francis Ysidro Edgeworth

1845–1926

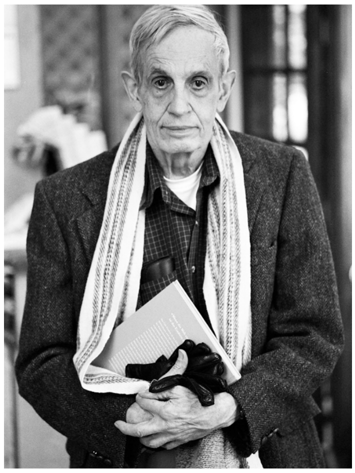
John von Neumann

1903–1957



Oskar Morgenstern

1902–1977



John Nash

1928–2015

Kenneth Arrow

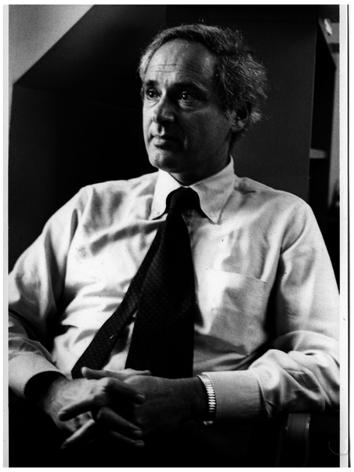
1921–2017

Gérard Debreu

1921–2004

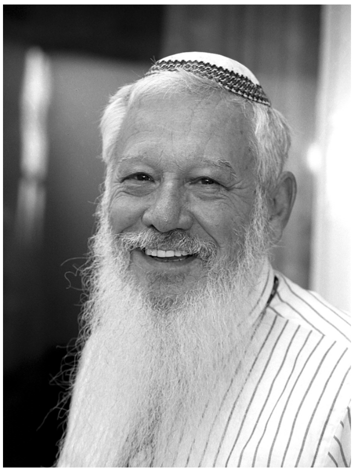
Lionel McKenzie

1919–2010



Herbert Scarf

1930–2015



Robert Aumann

1930–

Labubu (Zimomo)

∞

1 Mathematical Preliminaries

> He often used to say there was only one Road; that it was like a great river: its springs were at every doorstep and every path was its tributary. "It's a dangerous business, Frodo, going out of your door," he used to say. "You step into the Road, and if you don't keep your feet, there is no telling where you might be swept off to."
>
> Frodo Baggins in J.R.R. Tolkien's
> *The Fellowship of the Ring*, "Three is Company"

At the ending of Donald Duck's wondrous journey through Mathmagic Land, the following exchange occurs between our feathered hero and the "True Spirit of Adventure":[1]

> **Spirit**: In fact, it is only in the minds that we can conceive infinity. Mathematical thinking has opened the doors to the exciting adventures of science.
>
> **Donald**: [*walks down to the doors*] I'll be doggone! I've never seen so many doors before. [*walks in through the doors*]
>
> **Spirit**: Each discovery leads to many others, an endless chain.
>
> **Donald**: [*tries to open the doors*] Hey, hey! What's the matter with these doors? Hey! These doors won't open! They're locked!
>
> **Spirit**: Of course they are locked. These are the doors of the future, and the key is...
>
> **Donald**: Mathematics!
>
> **Spirit**: Right. Mathematics. The boundless treasures of science are locked behind those doors. ... In time, they will be opened by the

[1] *Donald in Mathmagic Land* is a 1959 Disney educational short film directed by Hamilton Luske, with the Spirit of Adventure narrated by Paul Frees. It was originally released as a theatrical featurette alongside *Darby O'Gill and the Little People.* Walt Disney reportedly considered it one of the most important films the studio ever produced.

> curious and inquiring minds of future generations. In the words of Galileo, "Mathematics is the alphabet with which God has written the universe."
>
> *Donald in Mathmagic Land* (Walt Disney Productions, 1959)

Much like Donald, you are about to discover a small but rather important slice of the wonderland of mathematics, one that unlocks many of the doors of current and future microeconomic theory. The topics covered in this chapter may at first seem like abstract machinery with no obvious destination. They are not. Each one enters the theory of general equilibrium, and economic theory in general, at a specific and indispensable moment, and by the end of this course their roles will, hopefully, feel entirely natural.

The treatment here is based primarily on the survey of Green and Heller (1981), but significantly expanded in several places, with different proofs of some results and different emphases throughout. The reader looking for a more concise treatment of a selection of these topics, written from the perspective of a working microeconomist, will find a useful and self-contained appendix in Mas-Colell, Whinston, and Green (1995). This book has trained countless generations of Ph.D. economists across the world.

For the foundations of metric spaces and their topology, the classical reference is Rudin (1976).[2] The reader wishing to go deeper into general topology can consult Munkres (2000), which is exceptionally clear and well-organized. Most of the topics covered here are also treated at a similar level—and in some instances, at a more general level—in the two monographs of Kim Border and collaborators: Border (1985), on fixed point theorems with direct applications to economics and game theory, and Aliprantis and Border (2006), a hitchhiker's guide to infinite-dimensional analysis that is simply an indispensable resource for the serious economic theorist.

The reader is also warmly encouraged to consult the appendices of this text, where the kind author[3] has assembled a substantial collection of prerequisite material: the sort of mathematics one encounters in courses in discrete mathematics, undergraduate real analysis, and linear algebra. That material is not assumed to have been seen recently, or in full, and the appendices are meant to be a genuine resource rather than a mere formality.

[2] Rudin's little blue book has the rare quality of being simultaneously terse and illuminating. Its terseness can be forbidding on a first reading, but the rewards of a patient second reading are considerable.

[3] That would be me, yes.

The remainder of this chapter is organized as follows. We begin in Section 1.1 with metric spaces and in Section 1.2 their topological structure. We then discuss sequences, convergence, completeness, and separability in Section 1.3. Section 1.4 takes up continuity. Section 1.5 covers compactness, which is, in a precise sense, the property that makes optimization possible: it is what turns a supremum into a maximum. Section 1.6 covers connectedness, which plays a quieter but equally real role in several important theorems in mathematics, and in the existence of a utility representation for a preference relation. We then turn in Section 1.7 to convexity and its many uses, with particular emphasis on the classical separation theorems and the Carathéodory and Shapley–Folkman theorems. Building on this foundation, we discuss convexity, concavity, quasiconvexity, and quasiconcavity of functions in Section 1.8. In Section 1.9 we discuss homogeneity and homotheticity. Section 1.10 develops the theory of correspondences, the multi-valued maps that arise throughout economic theory; we pay particular attention to hemicontinuity and the Theorem of the Maximum. The chapter closes in Section 1.11 with fixed point theorems, chiefly those of Brouwer and Kakutani, which are the tools that ultimately establish the existence of competitive equilibrium and Nash equilibrium.

A fair warning before we begin: this material is not easy, and there is no point pretending otherwise. But the difficulty is not one of obscurity. Every definition has a clear motivation, and every hypothesis in every theorem is there for a reason. Asking why a hypothesis cannot be weakened, or what breaks if a particular assumption is dropped, is almost always the most productive question one can ask.

1.1 Metric Spaces

1.1.1 How and with what to measure distances?

Measuring is an activity inherent to human nature. Indeed, many human activities may be understood as acts of comparison, and comparison is, at its core, a form of measurement. In this section, our interest lies in measuring the distance between arbitrary points of a given set. The first step is therefore to determine what constitutes a satisfactory notion of distance.

The reader may recall the Cartesian formula for distance in $\mathbb{R}^n$. Given two points $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{R}^n$, the distance between x and y is defined by

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}. \tag{1.1.1}$$

This formula is inspired by a simple geometric observation: the shortest path between x and y is the straight line segment joining them. The distance between the two points is therefore the length of this segment, computed via the Pythagorean theorem.

Geometrically, the principle of optimality underlies formula (1.1.1). If one travels from x to y along any path that passes through an intermediate point z not lying on the straight segment between them, the total length of the path will necessarily exceed the direct distance between x and y. This fundamental property is known as the *triangle inequality*, and it will form one of the axioms in the abstract definition of distance.

It is also natural to require that distance be nonnegative and symmetric: the distance from x to y should coincide with the distance from y to x. We now formalize these ideas.

Definition **1.1.2** (Metric). Let X be a nonempty set. A *metric* (or *distance*) on X is a function

$$d\colon X \times X \to \mathbb{R}$$

such that for all $x, y, z \in X$:

a) $d(x, y) \geq 0$; (positive definiteness)

b) $d(x, y) = 0$ if and only if $x = y$;

c) $d(x, y) = d(y, x)$; (symmetry)

d) $d(x, y) \leq d(x, z) + d(z, y)$. (triangle inequality)

Definition **1.1.3** (Metric space). A pair (X, d) consisting of a set X and a metric d on X is called a *metric space*.

Example **1.1.4** (The discrete metric). The simplest metric, and one that is often useful for constructing counterexamples, is the *discrete metric*. Let X be a nonempty set and define $d\colon X \times X \to \mathbb{R}$ by

$$d(x, y) = \begin{cases} 0 & \text{if } x = y, \\ 1 & \text{if } x \neq y. \end{cases}$$

We verify that d is a metric. Conditions (a)–(c) of Definition 1.1.2 are immediate. For the triangle inequality, let $x, y, z \in X$. If $x = y$, then $d(x, y) = 0$ and the inequality

$$d(x, y) \leq d(x, z) + d(z, y)$$

is trivially satisfied. If $x \neq y$, then $d(x, y) = 1$. If either $x \neq z$ or $z \neq y$, then at least one of $d(x, z)$ or $d(z, y)$ equals 1, and therefore

$$d(x, z) + d(z, y) \geq 1 = d(x, y).$$

Thus the triangle inequality holds in all cases. Therefore, d is a metric on X. In particular, this example shows that every nonempty set can be endowed with a metric.

EXERCISE 1.1.A. For $x, y \in \mathbb{R}$, consider the following functions $d_i : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$:

$$\begin{aligned}
d_1(x, y) &= (x - y)^2, \\
d_2(x, y) &= \sqrt{|x - y|}, \\
d_3(x, y) &= |x^2 - y^2|, \\
d_4(x, y) &= |x - 2y|, \\
d_5(x, y) &= \frac{|x - y|}{1 + |x - y|}.
\end{aligned}$$

For each $i = 1, \ldots, 5$, determine whether d_i defines a metric on $\mathbb{R}$. Justify your answer in each case.

EXERCISE 1.1.B. (Distance from a Point to a Set.) Let (X, d) be a metric space and let $A \subset X$. For $x \in X$, define

$$d(x, A) = \inf\{d(x, a) : a \in A\},$$

which we interpret as the *distance from x to the set A*. Show that for every $x, y \in X$,

$$d(x, A) \leq d(x, y) + d(y, A).$$

EXERCISE 1.1.C. Let (X, d) be a metric space and let $A, B \subseteq X$ be nonempty. Define the *distance between A and B* by

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

a) Show that $d(A, B) \geq 0$ and that $d(A, B) = d(B, A)$.

b) Show that if $A \cap B \neq \emptyset$, then $d(A, B) = 0$.

c) Give an example of two disjoint subsets $A, B \subseteq \mathbb{R}$ such that $d(A, B) = 0$.

d) Determine whether the triangle inequality

$$d(A,C) \leq d(A,B) + d(B,C)$$

holds for arbitrary nonempty sets $A, B, C \subseteq X$. Give either a proof or a counterexample.

EXERCISE 1.1.D.🐾 Let (X, d) be a metric space and let $A \subseteq X$ be nonempty. The *diameter* of A is defined by

$$\operatorname{diam}(A) := \sup\{d(x,y) : x, y \in A\},$$

where the supremum is taken in the extended[4]

a) Show that $\operatorname{diam}(A) \geq 0$.

b) Show that $\operatorname{diam}(A) = 0$ if and only if A consists of a single point.

c) Show that if $A \subseteq B$, then

$$\operatorname{diam}(A) \leq \operatorname{diam}(B).$$

1.1.2 Metrics arising from norms in vector spaces

Many of the metric spaces that will be relevant in analysis and in economic theory arise from a linear structure. In Appendix F we introduced vector spaces, and in Appendix G we discuss normed real vector spaces.

Let $(X, \|\cdot\|)$ be a normed vector space in the sense of Appendix G. As established in Proposition G.1.2, every norm induces a metric on X via

$$d(x,y) = \|x - y\|.$$

Thus every normed vector space canonically carries a metric structure. In particular, the classical metrics on $\mathbb{R}^n$ arise in this way from the usual norms. We now examine these examples more explicitly and introduce further metrics derived from them.

[4] See Definitions E.3.11 real line $\overline{\mathbb{R}}$. and E.3.12.

Example 1.1.5 (The Euclidean metric on $\mathbb{R}^n$). Recall from Appendix G.2 that the Euclidean norm on $\mathbb{R}^n$ arises from the standard inner product in $\mathbb{R}^n$, the dot product:

$$\langle x, y\rangle = x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

Specifically,

$$\|x\|_2 = \sqrt{\langle x, x\rangle} = \left(\sum_{i=1}^{n} x_i^2\right)^{1/2}.$$

The induced metric is therefore

$$d(x, y) = \|x - y\|_2 = \left(\sum_{i=1}^{n} (x_i - y_i)^2\right)^{1/2}.$$

We verify the metric axioms. (a) and (b) follow from the properties of the inner product: $\langle x - y, x - y\rangle \geq 0$, with equality if and only if $x = y$. Symmetry is immediate since $\|x - y\|_2 = \|y - x\|_2$. For the triangle inequality, observe that $d(x,z) = \|x - z\|_2 = \|(x - y) + (y - z)\|_2$. Using the triangle inequality for the Euclidean norm, $\|u + v\|_2 \leq \|u\|_2 + \|v\|_2$, which follows from the Cauchy–Buniakovsky–Schwarz inequality (see lemma G.2.10), we obtain

$$\|x - z\|_2 \leq \|x - y\|_2 + \|y - z\|_2.$$

Thus $d(x,z) \leq d(x, y) + d(y,z)$. Hence d defines a metric on $\mathbb{R}^n$.

Example 1.1.6 (Other classical metrics on $\mathbb{R}^n$). The following norms on $\mathbb{R}^n$ also induce metrics:

$$\|x\|_\infty = \max_{1\leq i\leq n} |x_i|, \qquad \|x\|_1 = \sum_{i=1}^{n} |x_i|.$$

The associated metrics are given by

$$d_\infty(x, y) = \|x - y\|_\infty, \qquad d_1(x, y) = \|x - y\|_1.$$

Example 1.1.7 (p metrics on $\mathbb{R}^n$). More generally, for $1 \leq p < \infty$, define

$$\|x\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}.$$

The metric induced by this norm is $d_p(x, y) = \|x - y\|_p$.

The triangle inequality for $\|p\|\cdot$ follows from Minkowski's inequality G.1.13 (see Appendix G). Hence d_p defines a metric on $\mathbb{R}^n$ for every $1 \leq p \leq \infty$.

***Example* 1.1.8** (Railroad metric). Fix $P \in \mathbb{R}^n$, fix a norm $\|\cdot\|$ and define

$$d(x,y) = \begin{cases} \|x-y\| & \text{if } x, y, P \text{ are collinear,} \\ \|x-P\| + \|y-P\| & \text{otherwise.} \end{cases}$$

Intuitively, the point P plays the role of a central hub or station. If x and y lie on the same line passing through P, one may travel directly between them, and the distance coincides with the Euclidean distance. Otherwise, travel must proceed from x to P and then from P to y, so that distance is measured along a broken path with vertex at P.

Exercise 1.1.E. Show that the function defined in Example 1.1.8 satisfies the four properties of a metric. Conclude that it defines a metric on $\mathbb{R}^n$.

Exercise 1.1.F. Let (X, d) be a metric space. Show that for all $a, b, c, d \in X$,

$$|d(a,b) - d(c,d)| \leq d(a,c) + d(b,d).$$

This inequality is sometimes called the *tetrahedron inequality.*

If $\|\cdot\|$ is a norm, deduce that

$$|\|x\| - \|y\|| \leq \|x - y\|.$$

Exercise 1.1.G. Let (X, d) be a metric space. Determine which of the following functions define metrics on X:

a) $d_1(x,y) = d(x,y)^2$,

b) $d_2(x,y) = \sqrt{d(x,y)}$,

c) $d_3(x,y) = \dfrac{d(x,y)}{1 + d(x,y)}$,

d) $d_4(x,y) = \min\{d(x,y), 1\}$,

e) $d_5(x,y) = \log\big(1 + d(x,y)\big)$.

Exercise 1.1.H. Let $0 < \alpha < 1$.

a) Show that if $x, y \geq 0$, then

$$(x+y)^\alpha \leq x^\alpha + y^\alpha.$$

Let $p = 1/\alpha$ and use the inequality

$$\|(x^\alpha, y^\alpha)\|_p \leq \|(x^\alpha, 0)\|_p + \|(0, y^\alpha)\|_p.$$

b) Show that the function

$$d(x, y) = \sum_{k=1}^{n} |x_k - y_k|^{\alpha}$$

defines a metric on $\mathbb{R}^n$ which does not arise from a norm.

Exercise 1.1.I. Let (X, d) be a metric space and let $Y = X \times X$. For $z = (x_1, x_2)$ and $w = (y_1, y_2)$ in Y, define

$$\rho(z, w) = d(x_1, y_1) + d(x_2, y_2).$$

Show that (Y, ρ) is a metric space.

1.1.3 Isometries, Metric Subspaces, and more examples

Definition **1.1.9** (Isometry). Let (X_1, d_1) and (X_2, d_2) be metric spaces. A function $f : X_1 \to X_2$ is an *isometry* if

$$d_2\big(f(x), f(y)\big) = d_1(x, y) \quad \text{for all } x, y \in X_1.$$

If there exists a bijective isometry $f : X_1 \to X_2$, we say that (X_1, d_1) and (X_2, d_2) are *isometric.*

Remark **1.1.10**. The elements of a metric space are not required to be geometric points in the usual sense. They may be functions, sequences, or other mathematical objects. For simplicity of language, however, we still refer to them as *points.*

Example **1.1.11**. Let $C[0, 1] = \{f : [0, 1] \to \mathbb{R} : f \text{ is continuous}\}$.

Consider the following metric spaces:

a) $(C[0, 1], d_\infty)$, where

$$d_\infty(f, g) = \sup_{x \in [0,1]} |f(x) - g(x)|.$$

b) $(C[0, 1], d_1)$, where

$$d_1(f, g) = \int_0^1 |f(x) - g(x)|\, dx.$$

Exercise 1.1.J. Verify that the functions d_∞ and d_1 defined in Example 1.1.11 are metrics on $C[0, 1]$.

***Definition* 1.1.12** (Subspace). Let (X, d) be a metric space. A metric space (S, d_S) is called a *subspace* of (X, d) if $S \subseteq X$ and $d_S(x, y) = d(x, y)$ for all $x, y \in S$.

***Example* 1.1.13** (The space ℓ_∞ and some of its subspaces). Let

$$\ell_\infty = \left\{ x = (x_i)_{i\in\mathbb{N}} \subseteq \mathbb{R} : \sup_{i\in\mathbb{N}} |x_i| < \infty \right\}.$$

denote the set of all bounded sequences in $\mathbb{R}$. Define

$$d_\infty(x, y) = \sup_{i\in\mathbb{N}} |x_i - y_i|.$$

Then (ℓ_∞, d_∞) is a metric space.

a) The subspace c. Let $c = \{x \in \ell_\infty : x_i \to \ell \text{ for some } \ell \in \mathbb{R}\}$. Then (c, d_∞) is a subspace of (ℓ_∞, d_∞).

b) The space c_0. Let $c_0 = \{x \in \ell_\infty : x_i \to 0\}$. Then (c_0, d_∞) is a subspace of (c, d_∞).

***Example* 1.1.14** (The sphere and a great circle). Consider the S^2, the surface of a sphere of dimension 2, that is:

$$S^2 = \{x \in \mathbb{R}^3 : \|x\|_2 = 1\}.$$

For $x, y \in S^2$, define $d(x, y)$ as the length of the shorter arc on the surface of the sphere connecting x and y. Then (S^2, d) is a metric space.

If $u \in \mathbb{R}^3$ satisfies $\|u\|_2 = 1$, define

$$S^1 = \{x \in S^2 : u \cdot x = 0\}.$$

Then S^1 is a great circle in S^2, and

$$(S^1, d_{S^1})$$

is a subspace of (S^2, d).

1.2 Topological Structure of Metric Spaces

The concept of a metric is used to define a notion of distance on a space and carries with it a certain structure. The idea that points are close, as measured by the metric, allows us to make precise concepts such as *boundary*, *interior*, and *connectedness*, which admit a geometric interpretation in ordinary language. More generally, certain properties of sets (for example, those that contain their own boundary) inherit their structure indirectly from the metric.

1.2.1 Open Balls and Examples

The metric on a space determines what is known as the *topology* of the space. The fundamental notion in topology is that of a *neighborhood* of a point. In metric spaces, neighborhoods are described by the open balls that we now define.

Definition 1.2.1 (Open balls). Let (X, d) be a metric space, let $x \in X$, and let $\varepsilon > 0$. The *open ball* of radius ε centered at x (or the ε-neighborhood of x) is the set

$$B_\varepsilon^d(x) = \{\, y \in X : d(y, x) < \varepsilon \,\}.$$

When there is no risk of confusion, or when the metric is clear from the context, we omit the superscript and simply write $B_\varepsilon(x)$.

We can also define a notion of a *neighborhood around a set*, which is the next definition.

Definition 1.2.2 (ε-neighborhood). Let (X, d) be a metric space. For a subset $A \subseteq X$ and $\varepsilon > 0$, the *ε-neighborhood of A* is defined as

$$B_\varepsilon(A) := \{y \in X : d(y, A) < \varepsilon\}.$$

Remark 1.2.3. If X is a normed vector space with norm $\|\cdot\|$, then the metric induced by the norm is given by $d(x, y) = \|x - y\|$. In this case,

$$B_\varepsilon^{\|\cdot\|}(x) = \{\, y \in X : \|y - x\| < \varepsilon \,\}.$$

Example 1.2.4. In $(\mathbb{R}, |\cdot|)$, the open balls are precisely the open intervals. Indeed, if $a \in \mathbb{R}$ and $\varepsilon > 0$, then

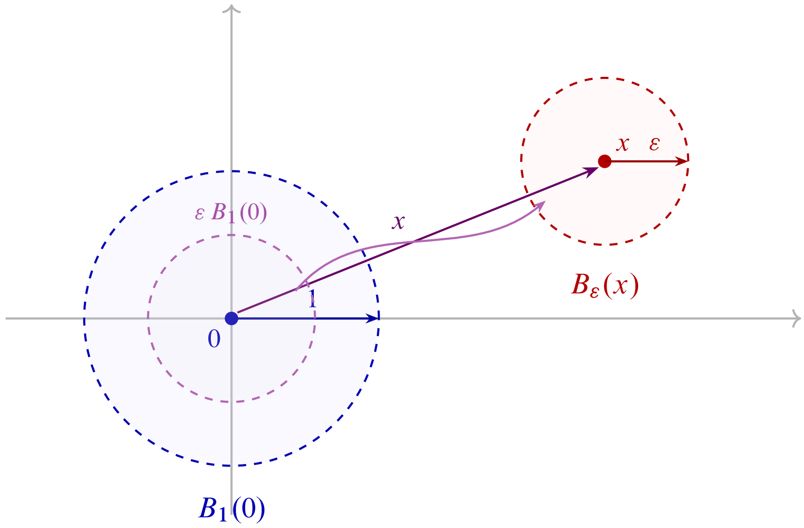
$$B_\varepsilon^{|\cdot|}(a) = \{\, b \in \mathbb{R} : |b - a| < \varepsilon \,\} = (a - \varepsilon,\, a + \varepsilon).$$

Conversely, every open interval in $\mathbb{R}$ is an open ball. If $a < b$, then

$$(a, b) = B_\varepsilon^{|\cdot|}(c)\,,$$

where

$$c = \frac{a+b}{2} \quad \text{and} \quad \varepsilon = \frac{1}{2}|b - a| = \left|\frac{a+b}{2} - a\right|.$$



$$B_\varepsilon(x) = x + \varepsilon\, B_1(0) = \{\, y \in V : \|y - x\| < \varepsilon \,\}$$

Figure 1.1: Translation and dilation of the unit ball in a normed vector space.

***Example* 1.2.5.** As figure 1.1 illustrates, in a normed vector space every open ball can be obtained from the open unit ball by a dilation and a translation. More precisely,

$$B_\varepsilon(x) = x + \varepsilon\, B_1(0)\,. \tag{1.2.6}$$

The ball $B_\varepsilon(x)$ can be obtained from $B_1(0)$ in two steps: first dilate by the factor ε, and then translate by the vector x.

Exercise 1.2.A. Let V be a normed vector space with norm $\|\cdot\|$. Verify the validity of equation (1.2.6).

***Remark* 1.2.7.** The identity

$$B_\varepsilon(x) = x + \varepsilon\, B_1(0)$$

relies on two distinct properties of normed spaces: translation invariance and homogeneity.

If (V, d) is merely a vector space endowed with a *translation invariant metric*, meaning

$$d(x+z, y+z) = d(x, y) \quad \text{for all } x, y, z \in V,$$

then we still have

$$B_\varepsilon(x) = x + B_\varepsilon(0)\,.$$

However, the further identity

$$B_\varepsilon(0) = \varepsilon\, B_1(0)$$

requires the homogeneity property of a norm and does not hold for an arbitrary translation invariant metric.

Example 1.2.8. In $(\mathbb{R}^2, \|\cdot\|)$, the unit ball depends on the chosen norm.

a) If $\|(x, y)\|_1 = |x| + |y|$, then

$$B_1(0) = \{(x, y) \in \mathbb{R}^2 : |x| + |y| < 1\}.$$

b) If $\|(x, y)\|_2 = \sqrt{x^2 + y^2}$, then

$$B_1(0) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}.$$

c) If $\|(x, y)\|_\infty = \max\{|x|, |y|\}$, then

$$B_1(0) = \{(x, y) \in \mathbb{R}^2 : |x| < 1,\ |y| < 1\}.$$

Figure 1.2 illustrates the geometric shape of the unit ball in each of these three cases.

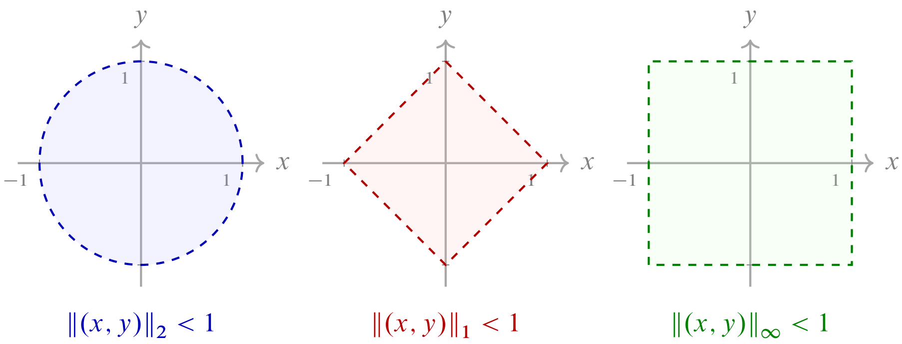


Figure 1.2: Balls induced by the standard norms in $\mathbb{R}^2$.

Example 1.2.9. Let $p > 0$.

a) If $p \geq 1$, consider $\mathbb{R}^2$ endowed with the p-norm $\|(x, y)\|_p$. Then the open unit ball centered at 0 is

$$B_1(0) = \{(x, y) \in \mathbb{R}^2 : \|(x, y)\|_p < 1\} = \{(x, y) \in \mathbb{R}^2 : |x|^p + |y|^p < 1\}.$$

b) If $0 < p < 1$, define d on $\mathbb{R}^2$ by

$$d_p\big((x_1, x_2), (y_1, y_2)\big) = |x_1 - y_1|^p + |x_2 - y_2|^p.$$

Then the open unit ball centered at 0 (with respect to d) is

$$B_1^d(0) = \{(x, y) \in \mathbb{R}^2 : d\big((x, y), (0, 0)\big) < 1\} = \{(x, y) \in \mathbb{R}^2 : |x|^p + |y|^p < 1\}.$$

Figure 1.3 illustrates these two situations for $p = 5$ and $p = \frac{1}{2}$.

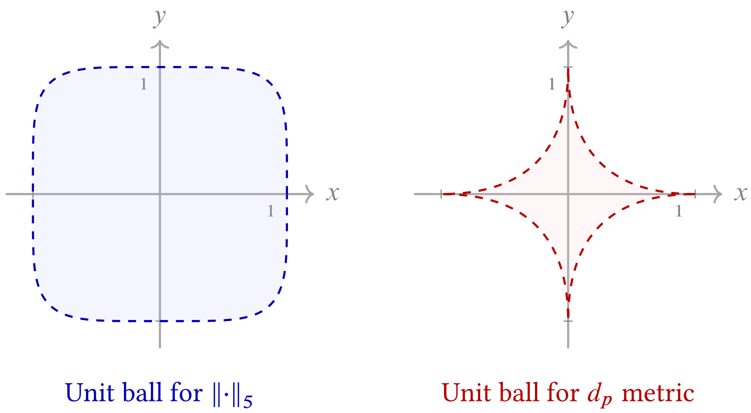


Figure 1.3: The set $\{(x, y) \in \mathbb{R}^2 : |x|^p + |y|^p < 1\}$ for $p = 5$ and $p = \frac{1}{2}$.

The preceding examples show how the geometry of a space can change radically depending on how distance is measured. However, as we will see soon, from a topological point of view all norms on $\mathbb{R}^n$ are indistinguishable: the neighborhoods (the basic objects of topology) do not change when we pass from one norm to another. This invariance is, in fact, the spirit of topology: two objects that can be continuously deformed into one another are regarded as the same from a topological perspective. Think, for example, of a rubber disk (the unit ball with respect to $\|\cdot\|_2$) deformed into a rubber square (the unit ball with respect to $\|\cdot\|_\infty$). The equivalence between norms is expressed as follows.

***Definition* 1.2.10** (Equivalent norms)**.** Let X be a vector space. Two norms $\|\cdot\|$ and $|||\cdot|||$ on X are *equivalent* if there exist constants $a, b > 0$ such that

$$a\|x\| \le |||x||| \le b\|x\|,$$

for all $x \in X$.

***Example* 1.2.11.** In $\mathbb{R}^n$, the norms $\|x\|_2$ and $\|x\|_\infty$ are equivalent. Our task is to find constants a and b such that

$$a\,\|x\|_\infty \le \|x\|_2 \le b\,\|x\|_\infty, \quad \text{for all } x \in \mathbb{R}^n.$$

First observe that

$$\|x\|_2 = \left(\sum_{i=1}^n |x_i|^2\right)^{1/2} \ge \max\{|x_i| : i = 1, \dots, n\} = \|x\|_\infty.$$

Thus we may take $a = 1$.

On the other hand,

$$\|x\|_2 = \left(\sum_{i=1}^n |x_i|^2\right)^{1/2} \le \left(\sum_{i=1}^n \max\{|x_i|\}^2\right)^{1/2} = \sqrt{n}\,\|x\|_\infty.$$

Hence we may take $b = \sqrt{n}$.

Moreover, these constants are optimal: $a = 1$ is the largest possible value and $b = \sqrt{n}$ is the smallest possible value for which the inequalities hold.

Changing the norm alters the geometry of the space, and some norms may therefore be more convenient than others depending on the problem at hand. At a first level of refinement, geometric features such as strict convexity and smoothness become relevant. Norms induced by inner products, such as $\|\cdot\|_2$ in $\mathbb{R}^n$, have "more spherical" unit balls, whereas norms such as $\|\cdot\|_1$ or $\|\cdot\|_\infty$ exhibit flat faces.

It is important to distinguish geometric differences from topological ones. Although the shapes of unit balls vary, the notion of equivalence of norms introduced above is a very strong requirement: it implies that the corresponding metrics generate the same topology. In fact, in $\mathbb{R}^n$—and more generally in any finite-dimensional normed vector space—all norms turn out to be equivalent. Thus, despite geometric differences, finite-dimensional normed spaces possess only one topology compatible with a norm. The proof of this fundamental result will be given later (see Exercise 1.5.A).

Exercise 1.2.B.🐾 Let $\|\cdot\|$ and $|||\cdot|||$ be equivalent norms on a vector space X. That is, there exist constants $a, b > 0$ such that

$$a\,\|x\| \le |||x||| \le b\,\|x\|, \qquad \text{for all } x \in X.$$

Show that the corresponding unit balls satisfy

$$B_a^{|||\cdot|||}(0) \subseteq B_1^{\|\cdot\|}(0) \subseteq B_b^{|||\cdot|||}(0)\,.$$

Exercise 1.2.C. Show that the norms $\|x\|_1$ and $\|x\|_\infty$ on $\mathbb{R}^n$ are equivalent. Use the previous exercise and Example 1.2.11 to deduce that $\|x\|_1$ and $\|x\|_2$ are also equivalent.

Exercise 1.2.D. Let (X, d) be a metric space. Let $x^* \in X$ and $\varepsilon > 0$. Show that if $z \in B_\varepsilon(x^*)$, then $B_\varepsilon(z) \subseteq B_{2\varepsilon}(x^*)$.

Exercise 1.2.E. Let (X, d) be a metric space. Let $x^* \in X$ and $\varepsilon > 0$. Show that if $z \in B_\varepsilon(x^*)$, then there exists $r > 0$ such that $B_r(z) \subseteq B_\varepsilon(x^*)$.

Exercise 1.2.F. Let (X, d) be a metric space and let $x_0, x_1 \in X$ be distinct points. Let $\varepsilon > 0$.

a) Show that if $B_\varepsilon(x_0) \cap B_\varepsilon(x_1) \neq \emptyset$, then $d(x_0, x_1) < 2\varepsilon$.

b) Show that if $\varepsilon \leq \frac{1}{2} d(x_0, x_1)$, then $B_\varepsilon(x_0) \cap B_\varepsilon(x_1) = \emptyset$.

Exercise 1.2.G. Let (X, d) be a metric space and let $x_0, x_1 \in X$ be distinct points. Let $r_0, r_1 > 0$. Show that if $r_0 + r_1 \leq d(x_0, x_1)$, then $B_{r_0}(x_0) \cap B_{r_1}(x_1) = \emptyset$.

1.2.2 Open and Closed Sets in Metric Spaces

1.3 Sequences, Complete Spaces, and Separable Spaces

1.4 Continuity

1.5 Compactness

Exercise 1.5.A. Let X be a finite-dimensional vector space and let $\|\cdot\|$ and $|||\cdot|||$ be two norms on X.

a) Show that the function
$$f(x) = |||x|||$$
is continuous on $(X, \|\cdot\|)$.

b) Let
$$S = \{x \in X : \|x\| = 1\}$$
be the unit sphere with respect to $\|\cdot\|$. Show that S is compact.

c) Deduce that f attains a minimum and a maximum on S. Show that there exist constants $a, b > 0$ such that

$$a \leq |||x||| \leq b, \qquad \text{for all } x \in S.$$

d) Conclude that

$$a\,\|x\| \leq |||x||| \leq b\,\|x\|, \qquad \text{for all } x \in X.$$

Conclude that all norms on a finite-dimensional vector space are equivalent.

1.6 Connectedness

1.7 Convexity

1.7.1 Convexity of Sets

In microeconomic theory, convexity stands out as perhaps the most critical mathematical characteristic. Its significance becomes evident when we consider what happens in its absence: without convex preferences, demand and supply functions lose their continuity, which in turn prevents competitive markets from reaching equilibrium states. The power of convexity is further demonstrated through the highly effective tools of mathematical programming and duality theory, both of which rely fundamentally on the presence of convex structures. When we relax the convexity assumption by allowing production technologies that exhibit increasing returns to scale or by permitting consumer preferences to be non-convex (such as those favoring corner solutions), the analytical framework becomes considerably more complex. Convex production sets have a natural economic interpretation as technologies with constant or decreasing returns to scale, while convex indifference curves represent preferences that diminish in their marginal rates of substitution. Unfortunately, our understanding of general equilibrium models that incorporate non-convexities remains limited, with rigorous results available only for highly stylized cases, such as economies populated by infinitely many agents.

While metric spaces have served us well up to this point, the study of convexity requires additional structure: we need a coherent way to add points together and to multiply them by constants. This naturally brings us to the framework of vector spaces. Readers seeking the relevant development and definitions are encouraged to consult Appendix F.

In what follows, we will only consider real vector spaces, i.e., a vector space V over the field $\mathsf{F} = \mathbb{R}$.

Definition 1.7.1 (Convex combination). Let V be a real vector space and consider $x_1, \dots, x_n \in V$. A vector $z \in V$ is called a *convex combination* of $x_1, \dots, x_n$ if there exist $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ such that $\lambda_i \geq 0$ for all i, and $\sum_{i=1}^{n} \lambda_i = 1$, and

$$z = \sum_{i=1}^{n} \lambda_i x_i.$$

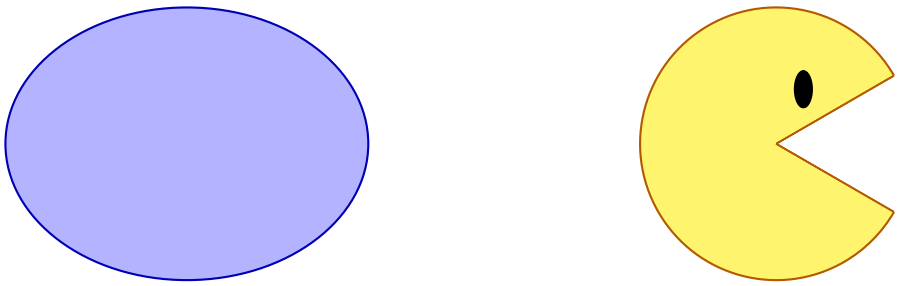
Remark 1.7.2. In the special case of definition 1.7.1 in which we take only two vectors, a convex combination of $x, y \in V$ is any vector of the form

$$\lambda x + (1 - \lambda) y, \qquad \lambda \in [0, 1].$$

Definition 1.7.3 (Convex set). Let V be a real vector space. A subset $C \subset V$ is called *convex* if for all $x, y \in C$ and all $\lambda \in [0, 1]$,

$$\lambda x + (1 - \lambda) y \in C.$$

Please see figure 1.1 for examples of a convex and a non-convex set.



Convex Set

Mr. Pacman—A Non-Convex Set

Figure 1.1: Illustration of convex and non-convex sets.

Joke 1.7.4. Mr. Pac-Man tried to join the Convex Sets Club, but they told him he didn't have the right shape for their group. He took it like a champ, given that he's used to having gaps in his social circle.

Definition 1.7.5 (Set of Convex Combinations). Let V be a real vector space. For a subset $S \subseteq V$, define

$$\widehat{S} := \left\{ \sum_{i=1}^{n} \lambda_i x_i \;\middle|\; n \in \mathbb{N},\ x_i \in S,\ \lambda_i \geq 0\ \forall i,\ \sum_{i=1}^{n} \lambda_i = 1 \right\}.$$

The set $\widehat{S}$ is the set of all convex combinations of finitely many elements of S.

***Remark* 1.7.6.** For every $S \subset V$ we have $S \subset \widehat{S}$.

Theorem 1.7.7. *Let V be a real vector space. For a subset $S \subseteq V$, the following are equivalent:*

a) S *is convex.*

b) $S = \widehat{S}$.

Proof. ($\Leftarrow$) Suppose $S = \widehat{S}$. Let $x, y \in S$ and $\lambda \in [0, 1]$. Then

$$\lambda x + (1 - \lambda) y$$

is a convex combination of elements of S, hence belongs to $\widehat{S} = S$. Thus S is convex.

($\Rightarrow$) Suppose that S is convex. We show that $\widehat{S} \subseteq S$.

We argue by induction on $n \in \mathbb{N}$. For $n = 1$, the claim is trivial.

Fix $n \geq 2$ and assume that every convex combination of $n - 1$ elements of S belongs to S. Let $x_1, \dots, x_n \in S$ and let $\lambda_1, \dots, \lambda_n \geq 0$ satisfy

$$\sum_{i=1}^{n} \lambda_i = 1.$$

If $\lambda_n = 1$, then

$$\sum_{i=1}^{n} \lambda_i x_i = x_n \in S.$$

Hence we may assume $\lambda_n < 1$ and define

$$y := \sum_{i=1}^{n-1} \frac{\lambda_i}{1 - \lambda_n} x_i .$$

Since $\sum_{i=1}^{n-1} \frac{\lambda_i}{1-\lambda_n} = 1$ and $\frac{\lambda_i}{1-\lambda_n} \geq 0$, the induction hypothesis implies $y \in S$. Now observe that

$$\sum_{i=1}^{n} \lambda_i x_i = \lambda_n x_n + (1 - \lambda_n) y.$$

By convexity of S, the right-hand side belongs to S. Thus every convex combination of n elements of S lies in S.

Therefore $\widehat{S} \subseteq S$, and hence $S = \widehat{S}$. /ᐢ.ᐢ\

We now introduce two important operations on subsets of a vector space: set addition and scalar multiplication of a set.

***Definition* 1.7.8** (Minkowski sum). Let V be a real vector space. For subsets $A, B \subseteq V$, the *Minkowski sum* of A and B is

$$A + B := \{\, a + b \mid a \in A,\ b \in B \,\}.$$

***Definition* 1.7.9** (Scalar multiplication of a set). Let V be a real vector space. For $\lambda \in \mathbb{R}$ and $S \subseteq V$, define

$$\lambda S := \{\, \lambda x \mid x \in S \,\}.$$

***Remark* 1.7.10.** In Definitions 1.7.8 and 1.7.9, the sets under consideration are *arbitrary* subsets of V. They are not assumed to be vector subspaces.

In particular, $A + B$ need not be a subspace even if A and B are merely subsets of V, and λS is defined for every $\lambda \in \mathbb{R}$, without any invariance assumptions on S.

Exercise 1.7.A.🐾 Let V be a real vector space and let $\{S_i\}_{i \in I}$ be a family of convex subsets of V, where I is an arbitrary index set. Show that

$$\bigcap_{i \in I} S_i$$

is convex.

Exercise 1.7.B.🐾 Let V be a real vector space and let $S, T \subseteq V$ be convex. Show that the Minkowski sum $S + T$ is convex.

Exercise 1.7.C.🐾 Let V be a real vector space and let $S \subseteq V$ be convex. Show that for every $\lambda \geq 0$, the set λS is convex.

The preceding discussion relied only on the linear structure of V. To introduce closure and interior, we now assume that V is a normed real vector space equipped with its induced metric topology. For the necessary background, see Chapter G.

Exercise 1.7.D.🐾 Let V be a normed real vector space and let $S \subseteq V$. Show that S is convex if and only if its closure $\overline{S}$ is convex.

Exercise 1.7.E.🐾 Let V be a normed real vector space and let $S \subseteq V$ be convex with nonempty interior. Show that S° is dense in $\overline{S}$, i.e., Show that

$$\overline{S} = \overline{S^\circ}.$$

Exercise 1.7.F. Let V be a normed real vector space with induced metric d. Let $X \subseteq V$ be a closed and convex set, and let $x \notin X$. Then there exists a unique point $y \in X$ such that $d(x, X) = d(x, y)$.

Exercise 1.7.G. Let V be a real normed vector space with induced metric d, and let $X \subseteq V$ be nonempty, closed, and convex. Define a function $g : V \to X$ as follows: for each $x \in V$, let $g(x)$ denote a point in X satisfying

$$d(x, g(x)) = d(x, X),$$

that is, $g(x)$ is a closest point in X to x.

Show that for all $x, \hat{x} \in V$,

$$d(g(x), g(\hat{x})) \leq d(x, \hat{x}).$$

Definition **1.7.11** (Convex hull). Let V be a real vector space and let $S \subseteq V$. The *convex hull* of S is defined by

$$\operatorname{co}(S) := \bigcap \{\, G \subseteq V \mid S \subseteq G \text{ and } G \text{ is convex} \,\}.$$

Equivalently, $\operatorname{co}(S)$ is the smallest convex superset of S.

Theorem 1.7.12. *Let V be a real vector space and let $S \subseteq V$. Then*

$$\widehat{S} = \operatorname{co}(S)\,.$$

Proof. We first show that $\widehat{S} \subseteq \operatorname{co}(S)$. Fix $x \in \widehat{S}$. Then there exist $n \in \mathbb{N}$, points $x_1, \ldots, x_n \in S$, and scalars $\lambda_1, \ldots, \lambda_n \geq 0$ such that $\sum_{i=1}^{n} \lambda_i = 1$ and

$$x = \sum_{i=1}^{n} \lambda_i x_i\,.$$

Let G be any convex set such that $S \subseteq G$. Then $x_1, \ldots, x_n \in G$, and by convexity of G we have $x \in G$. Since G was arbitrary, it follows that $x \in \operatorname{co}(S)$. Hence $\widehat{S} \subseteq \operatorname{co}(S)$.

Next, we show that $\operatorname{co}(S) \subseteq \widehat{S}$. Since $S \subseteq \widehat{S}$ and $\widehat{S}$ is convex, it follows that $\widehat{S}$ is a convex superset of S. By the definition of $\operatorname{co}(S)$ as the intersection of all convex supersets of S, we obtain $\operatorname{co}(S) \subseteq \widehat{S}$.

Therefore, $\widehat{S} = \operatorname{co}(S)$. ^. .^)9

Exercise 1.7.H. Let V be a real vector space and let $A_1, A_2 \subseteq V$. Show that

$$\operatorname{co}(A_1 + A_2) = \operatorname{co}(A_1) + \operatorname{co}(A_2)\,.$$

Exercise 1.7.I. Let V be a normed real vector space and let $A \subseteq V$. Show that if A is open, then $\mathrm{co}(A)$ is open.

Exercise 1.7.J. Give an example of a closed set $A \subseteq \mathbb{R}^2$ such that $\mathrm{co}(A)$ is not closed.

Exercise 1.7.K.🐾 (ϵ-neighborhoods are convex.) Let V be a normed real vector space and let $A \subseteq V$ be convex. Show that for every $\varepsilon > 0$, the sets $B_\varepsilon(A)$ and $\overline{B_\varepsilon(A)} = \{y \in V : d(y, A) \leq A\}$ are convex.

1.7.2 Separation Theorems

A key characteristic of convex sets is their ability to be separated by hyperplanes when they don't overlap. This principle plays an important role in economics, particularly in establishing price systems that achieve Pareto-efficient resource distributions. In such systems, prices guide both consumers and producers toward choices that result in efficient allocations. In the simplest possible scenario, suppose Y represents a production possibilities set, and I denotes the highest indifference curve that shares a point with Y; let this point be z. Then z is called a Pareto-efficient allocation, and the hyperplane H, defined by the vector x satisfying $p \cdot x = M$, serves as the separating boundary, where M separates both Y and the upper contour set $P(z)$ bounded by I and containing the point z. At prices p, producers maximize their profits while consumers maximize their utility within their budget constraint, and the resulting outcome is Pareto-efficient. See Figure 1.2 for an illustration.

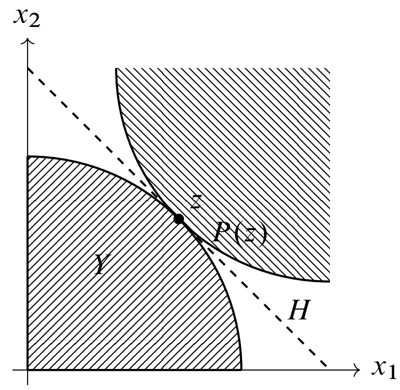
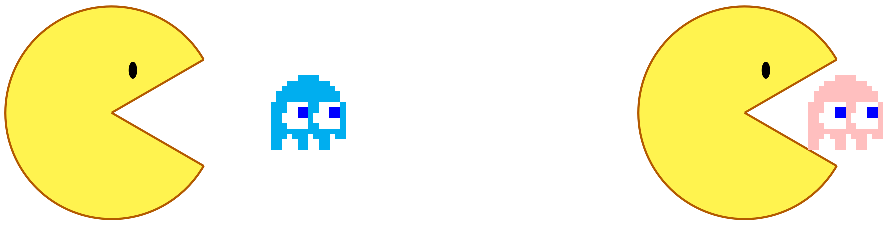


Figure 1.2: Illustration of Pareto efficiency.

***Remark* 1.7.13.** While convex sets are not the only sets that can be separated by hyperplanes, it is in some sense easier to establish conditions for such separation when dealing with convex sets. An illustration of this issue can be found in Figure 1.3.

Our next order of business is to define hyperplanes rigorously. To do so, we will need additional structure on our normed vector spaces: specifically, we require the norm to be induced by an inner product. This inner product structure will enable us to define orthogonality, perpendicularity, and projections, which are essential concepts for characterizing hyperplanes. The relevant background material on inner product spaces can be found in Section G.2 in appendix G.



(a) Separable (b) Non-Separable

Figure 1.3: Separation of sets. Case (a) Separable, Case (b) Non-Separable

***Definition* 1.7.14** (Hyperplane). Let V be a real inner product space. Let $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$. The set

$$H(p, \alpha) := \{x \in V : \langle p, x \rangle = \alpha\}$$

is called an (affine) hyperplane with normal vector p.

***Definition* 1.7.15** (Closed half-spaces). Let V be a real inner product space. Let $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$. The sets

$$H^{-}(p, \alpha) := \{x \in V : \langle p, x \rangle \leq \alpha\}, \qquad H^{+}(p, \alpha) := \{x \in V : \langle p, x \rangle \geq \alpha\}$$

are called the closed half-spaces determined by $H(p, \alpha)$.

***Definition* 1.7.16** (Open half-spaces). Let V be a real inner product space. Let $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$. The sets

$$H^{+\circ}(p, \alpha) := \{x \in V : \langle p, x \rangle < \alpha\}, \qquad H^{-\circ}(p, \alpha) := \{x \in V : \langle p, x \rangle > \alpha\}$$

are called the open half-spaces determined by $H(p, \alpha)$.

Proposition 1.7.17. *Let V be a real inner product space. Every open or closed half-space in V is convex.*

Exercise 1.7.L. Prove Proposition 1.7.17.

Exercise 1.7.M.🐾 Let V be a real inner product space. For $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$, show that

$$H^{+}(p,\alpha) = H^{-}(-p,-\alpha)\,.$$

Exercise 1.7.N. Let V be a real inner product space. For every pair of vectors $x, y \in V$, show that

$$x \in H^{+}(x-y, \langle x-y, y\rangle)\,.$$

Exercise 1.7.O. Let V be a real inner product space and let $x, y \in V$ be distinct vectors. Prove the following:

a) $y \in H\,(y-x, \langle y-x, y\rangle)$.

b) The hyperplane $H\,(y-x, \langle y-x, y\rangle)$ is perpendicular to $y-x$, i.e., for every $z \in H\,(y-x, \langle y-x, y\rangle)$, $\langle y-x,\ y-z\rangle = 0$.

c) y is the unique point in $H\,(y-x, \langle y-x, y\rangle)$ that is closest to x, that is, $\langle z-x,\ z-x\rangle > \langle y-x,\ y-x\rangle$ for all $z \in H\,(y-x, \langle y-x, y\rangle)\,,\ z \neq y$.

Now we are ready to define some important terminology about separation by hyperplanes.

Definition **1.7.18** (Bounding hyperplane). Let V be a real inner product space and let $S \subseteq V$. Let $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$. The hyperplane $H\,(p,\alpha)$ is called a *bounding hyperplane* for S if S is contained in one of the two closed half-spaces determined by it, that is,

$$S \subseteq H^{-}(p,\alpha) \quad \text{or} \quad S \subseteq H^{+}(p,\alpha)\,.$$

Definition **1.7.19** (Supporting hyperplane). Let V be a real inner product space and let $S \subseteq V$ be nonempty. Let $p \in V \setminus \{0\}$ and $\alpha \in \mathbb{R}$. The hyperplane $H\,(p,\alpha)$ is called a *supporting hyperplane* for S if it is a bounding hyperplane for S and

$$\alpha = \inf_{x \in S} \langle p, x\rangle.$$

Remark **1.7.20**. If the infimum in Definition 1.7.19 is attained at some $\bar{x} \in S$, then $\bar{x} \in \partial S$ and $\bar{x} \in H\,(p,\alpha)$. In particular, the supporting hyperplane intersects the boundary of S.

Exercise 1.7.P. Let V be a real inner product space and let $S \subseteq V$ be nonempty. Show that a hyperplane $H(p, \alpha)$ is a supporting hyperplane for S if and only if it is a bounding hyperplane for S and either

$$\alpha = \inf_{x \in S} \langle p, x \rangle \quad \text{or} \quad \alpha = \sup_{x \in S} \langle p, x \rangle.$$

In particular, the two characterizations are equivalent after replacing p by $-p$.

***Definition* 1.7.21** (Separation by a hyperplane). Let V be a real inner product space and let $S, T \subseteq V$ be nonempty. A hyperplane $H(p, \alpha)$ is said to *separate* S and T if

$$\langle p, x \rangle \leq \alpha \leq \langle p, y \rangle \quad \text{for all } x \in S,\ y \in T.$$

Figure 1.4 illustrates definitions 1.7.18, 1.7.19, and 1.7.21.

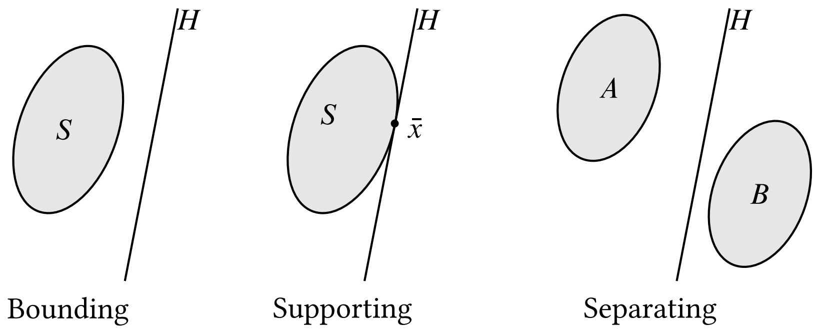


Figure 1.4: Bounding, supporting, and separating hyperplanes.

We now turn to one of the central geometric features of convex sets: their separation by hyperplanes. The results that follow develop this principle in increasing generality.

We begin with the separation of a single point from a closed convex set. From this we derive the existence of supporting hyperplanes at boundary points of convex sets. Finally, we extend the separation principle to pairs of convex sets, obtaining the classical Minkowski's Hyperplane Separation Theorem.

Theorem 1.7.22 (Strong Separation (Point–Set) Theorem). *Let V be a finite-dimensional real inner product space*[5] *and let $X \subseteq V$ be nonempty, closed, and convex. If $y \in V \setminus X$, then there exists $p \in V \setminus \{0\}$ such that*

$$\langle p, y \rangle > \sup_{x \in X} \langle p, x \rangle.$$

[5] Isomorphic to $\mathbb{R}^n$.

Figure 1.5 illustrates Theorem 1.7.22 and the geometric idea underlying its proof.

Proof. Let V be a finite-dimensional real inner product space and let $\|\cdot\|$ denote the norm induced by the inner product. Let $X \subseteq V$ be nonempty, closed, and convex, and fix $y \in V \setminus X$.

Choose[6] an arbitrary point $x_0 \in X$ and consider the closed ball

$$W := \{ w \in V : \|y - w\| \leq \|y - x_0\| \}.$$

Define

$$X' := X \cap W.$$

Then $x_0 \in X'$, so X' is nonempty. Moreover, X' is closed as the intersection of closed sets.

Since W is bounded, X' is bounded as well. In particular, when V is finite-dimensional, X' is compact. Hence, by the Weierstrass theorem, there exists a point $x^* \in X'$ such that

$$\left\| y - x^* \right\| = \min_{x \in X'} \|y - x\|.$$

By construction, this x^* also minimizes the distance from y to X: indeed, for any $x \in X \setminus W$ we have $\|y - x\| > \|y - x_0\|$, while $x_0 \in X'$, so the minimizer over X' is a minimizer over X.

Define

$$p := y - x^*.$$

Since $y \notin X$ and $x^* \in X$, we have $p \neq 0$.

Now let $x \in X$ be an arbitrary point and let v^μ be the point given by $v^\mu = \mu x + (1-\mu)x^*$, for some $\mu \in [0, 1]$. By convexity of X we know that $v^\mu \in X$. Thus, by definition of x^*, $0 < \|y - x^*\| \leq \|y - v^\mu\|$ for all $\mu \in [0, 1]$, and:

$$\begin{aligned}
0 &\geq \left\| y - x^* \right\|^2 - \|y - v^\mu\|^2 \\
&= \langle p, p \rangle - \big\langle y - \big(\mu x + (1-\mu)x^*\big), y - \big(\mu x + (1-\mu)x^*\big) \big\rangle \\
&= \langle p, p \rangle - \big\langle p + \mu(x^* - x), p + \mu(x^* - x) \big\rangle \\
&= \langle p, p \rangle - \langle p, p \rangle - 2\mu\big\langle p, x^* - x \big\rangle - \mu^2 \big\langle x^* - x, x^* - x \big\rangle \\
&= -2\mu\big\langle p, x^* - x \big\rangle - \mu^2 \left\| x^* - x \right\|^2.
\end{aligned}$$

[6] The goal in this part of the proof is to construct a point $x^* \in X$ that is at *minimal* distance from the point y. If the reader has done exercise 1.7.F, this step is immediate.

This implies that:

$$\langle p, x^* - x \rangle \geq -\frac{1}{2}\mu \| x^* - x \| \mu \xrightarrow[\mu \to 0]{} 0$$

Hence $\langle p, x^* \rangle \geq \langle p, x \rangle$. Since x was arbitrary, this implies $\langle p, x^* \rangle = \max_X \langle p, x \rangle$. Finally, notice that $0 < \langle p, p \rangle = \langle p, y - x^* \rangle$ and thus $\langle p, y \rangle > \langle p, x^* \rangle$. ^. .^)9

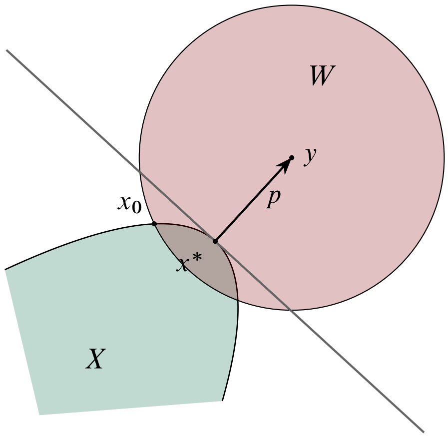


Figure 1.5: Illustration of theorem 1.7.22

.

Theorem 1.7.23 (Supporting Hyperplane Theorem). *Let V be a finite-dimensional real inner product space*[7] *and let $X \subseteq V$ be nonempty and convex. If $y^* \in \partial X$, then there exists $p \in V \setminus \{0\}$ such that*

$$\langle p, y^* \rangle \geq \sup_{x \in X} \langle p, x \rangle.$$

Equivalently, the hyperplane

$$H\left(p, \langle p, y^* \rangle\right)$$

is a supporting hyperplane for $\overline{X}$ at y^*.

Figure 1.6 illustrates Theorem 1.7.23 and the idea underlying its proof, which exploits the construction in Theorem 1.7.22.

Proof. Let V be a finite-dimensional real inner product space, and let $X \subset V$ be noempty and convex. Consider a boundary point $y^* \in \partial X$. By definition of

[7] Once again, isomorphic to $\mathbb{R}^n$.

the boundary of a set, there exists a sequence $\{y_n\}$ such that $y_n \in (V \setminus \overline{X})^\circ$ for each $n \in \mathbb{N}$, and such that $\lim_{n\to\infty} y_n = y^*$. By theorem 1.7.22, there exists a sequence $\{z_n\}$, with $z_n \in V\setminus\{0\}$, for each $n \in \mathbb{N}$, such that $\langle z_n, y_n\rangle > \sup_{x\in\overline{X}}\langle z_n, x\rangle$ for all $n \in \mathbb{N}$. For every $n \in \mathbb{N}$, we have that $z_n \neq 0$ and, consequently, $\|z_n\| > 0$. We can thus define the sequence $\{p_n\}$ given by $p_n = z_n/\|z_n\|$ for each $n \in \mathbb{N}$. The sequence $\{p_n\}$ is a subset of $B = \{v \in V : \|v\| = 1\}$, i.e., the unit circle in V. This transformation preserves the inequalities $\langle p_n, y_n\rangle > \langle p_n, x\rangle$ for all $x \in \overline{X}$ and all $n \in \mathbb{N}$. Since the set B is compact, we can extract a convergent subsequence from $\{p_n\}$ converging to some limit $p \in B$. The inequality is preserved under the limit and thus we obtain that $\langle p, y\rangle \geq \langle p, x\rangle$ for all $x \in \overline{X}$. Consequently, since $X \subseteq \overline{X}$, we have that $\langle p, y\rangle \geq \sup_{x\in X}\langle p, x\rangle$.

/ᐠ｡ꞈ｡ᐟ\

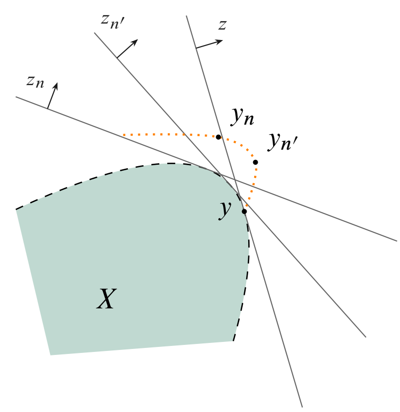


Figure 1.6: Illustration of theorem 1.7.23

.

Theorem 1.7.24 (Minkowski's Separating Hyperplane Theorem). *Let V be a finite-dimensional real inner product space* [8] *and let $X, Y \subseteq V$ be nonempty and convex. If $X^\circ \cap Y^\circ = \emptyset$, then there exist $p \in V \setminus \{0\}$ and $\mu \in \mathbb{R}$ such that*

$$\sup_{y\in Y}\langle p, y\rangle \leq \mu \leq \inf_{x\in X}\langle p, x\rangle.$$

Proof. Let $X, Y \subseteq V$ be convex and have disjoint interiors and let $W = Y^\circ - X^\circ \subseteq V$. Since $X^\circ \cap Y^\circ = \emptyset$, we know that $0 \notin W$. Exercise 1.7.B shows that W is convex. From the previous theorems, it follows that there exists $p \in V \setminus \{0\}$ such that $0 = \langle p, 0\rangle \geq \langle p, y - x\rangle$ for all $x \in X$ and $y \in Y$ (If $0 \notin \partial W$, use

[8] Isomorphic to $\mathbb{R}^n$.

Theorem 1.7.22, otherwise use Theorem 1.7.23). Therefore, we have that $\langle p, x\rangle \geq \langle p, y\rangle$ for all $x \in X$ and all $y \in Y$, and hence $\sup_{y\in Y} \langle p, y\rangle \leq \sup_{x\in X} \langle p, x\rangle$.

Exercise 1.7.Q. Let V be a finite-dimensional real inner product space. Let $H(p, \alpha)$ be a hyperplane and let $x \notin H(p, \alpha)$. Let $y \in H(p, \alpha)$ be the point in $H(p, \alpha)$ that is closest to x.

Show that

$$H(p, \alpha) = H(y - x, \langle y - x, y\rangle).$$

Exercise 1.7.R. Let V be a finite-dimensional real inner product space. Let $H(p, \alpha)$ be a hyperplane and let $x \notin H(p, \alpha)$. Define

$$y := x + \frac{\alpha - \langle p, x\rangle}{\langle p, p\rangle} p.$$

Prove the following:

a) $y \in H(p, \alpha)$.

b) $H(p, \alpha) = H(y - x, \langle y - x, y\rangle)$.

Exercise 1.7.S. Let V be a finite-dimensional real inner product space. Suppose that $H(p, \alpha)$ separates a closed and convex set $S \subseteq V$ from x, and suppose that $H(\widehat{p}, \widehat{\alpha})$ separates a closed and convex $\widehat{S}$ from a vector $\widehat{x}\ \not n \widehat{S}$.

Does the hyperplane

$$H(p + \tilde{p}, \alpha + \tilde{\alpha})$$

separate $S + \widehat{S}$ from $x + \widehat{x}$?

Either prove that this is true, or provide a counterexample.

Exercise 1.7.T. Let V be a finite-dimensional real inner product space. Let $S \subseteq V$ be closed (not necessarily convex) and let $x \notin S$.

Must there exist a hyperplane separating x from S? Either prove that this is true, or provide a counterexample.

Exercise 1.7.U. Each of the following presents a closed and convex set $S \subseteq \mathbb{R}^n$ and a vector $x \notin S$. For each pair, determine whether or not there is a hyperplane separating x from S. If your answer is affirmative, find such a hyperplane. If your answer is negative, justify your answer. Notation: for every $x, y \in \mathbb{R}^n$, denote the line segment connecting x and y by $[x, y]$, i.e., $[x, y] = \operatorname{co}(x, y)$.

a) $S = \{z \in \mathbb{R}^2 : z_1^2 + z_2^2 \leq 1\}$, $x = (0, 0)$.

b) $S = \{z \in \mathbb{R}^2 : z_1^2 + z_2^2 \leq 1\}$, $x = (1, 1)$.

c) $S = \{z \in \mathbb{R}^2 : z_1^2 + z_2^2 \leq 1\}$, $x = (0, 1)$.

d) $S = [(0, 0), (1, 1)] \cup [(0, 0), (-1, 1)]$, $x = (0, \frac{1}{2})$.

e) $S = [(0, 0), (1, 1)] \cup [(0, 0), (-1, 1)]$, $x = (\frac{1}{2}, 1)$.

f) $S = [(0, 0), (1, 1)] \cup [(0, 0), (-1, 1)]$, $x = (\frac{1}{4}, 2)$.

g) $S = \{z \in \mathbb{R}^3 : z_1^2 + z_2^2 + z_3^2 = 1\}$, $x = (0, 0, 0)$.

h) $S = \{z \in \mathbb{R}^3 : z_1^2 + z_2^2 + z_3^2 = 1\}$, $x = (0, 1, 1)$.

Exercise 1.7.V. Each of the following presents a closed and convex set $S \subseteq \mathbb{R}^n$ and a vector $x \notin S$. For each pair, find a hyperplane separating x from S, as described in Theorem 1.7.22.

a) $S = \{z \in \mathbb{R}^3 : \max\{|z_1|, |z_2|, |z_3|\} \leq 1\}$, $x = (2, 2, 2)$.

b) $S = \{z \in \mathbb{R}^3 : \max\{|z_1|, |z_2|, |z_3|\} \leq 1\}$, $x = (2, 3, 4)$.

c) $S = \{z \in \mathbb{R}^3 : z_1^2 + z_2^2 + z_3^2 = 1\}$, $x = (2, 2, 2)$.

d) $S = \{z \in \mathbb{R}^2 : z_1 \geq 0,\ z_1 + z_2 \leq 1,\ z_2 \leq 1\}$, $x = (1, 2)$.

e) $S = \{z \in \mathbb{R}^2 : z_1 \geq 0,\ z_1 + z_2 \leq 1,\ z_2 \leq 1\}$, $x = (2, 3)$.

We conclude this section with an application of the separation theorems we have established: Farkas' Lemma, a fundamental result concerning the existence of nonnegative solutions to systems of linear equations.

Lemma 1.7.25 (Farkas' Lemma). *Let $v \in \mathbb{R}^n$, and let T be an $n \times m$ matrix. The following statements are equivalent:*

a) For every $u \in \mathbb{R}^n$ satisfying

$$T^\intercal u \geq 0,$$

we have

$$u \cdot v \geq 0.$$

b) There exists $w \in \mathbb{R}^m$ with $w \geq 0$ such that

$$Tw = v.$$

Exercise 1.7.W.🐾🐾 (Guided proof of Lemma 1.7.25.) To prove that the first claim implies the second claim, define the set

$$A := \{ Tw : w \in \mathbb{R}^m,\ w \geq 0 \} \subseteq \mathbb{R}^n,$$

and suppose, toward a contradiction, that $v \notin A$. Show that there exists a hyperplane $H(p, \beta)$ separating A from v, and that one may assume without loss of generality that $\beta = 0$. Prove that $T^\top p \geq 0$, and derive a contradiction.

Exercise 1.7.X.🐾🐾🐾 (Infinite-dimensional detour.) Let V be a real inner product space of infinite dimension. Investigate to what extent the separation theorems proved in this section remain valid.

a) Show that closed balls in V need not be compact.

b) Identify where compactness was used in the finite-dimensional proofs.

c) Determine which separation statements remain true and which require additional structure.

(Advanced hint: In infinite dimensions, separation holds in locally convex spaces via the Hahn–Banach Theorem, while compactness arguments must be replaced by weak or weak-$*$ compactness arguments (e.g., Banach–Alaoglu).)

1.7.3 Carathéodory and Shapley–Folkman Theorems

TO BE COMPLETED.

1.8 Convex, Concave, quasiconcave, and quasiconcave functions

1.8.1 Convex functions

We start this section with a definition.

***Definition* 1.8.1.** Let X be a real vector space. A *linear functional* on X is a function $f\colon X \to \mathbb{R}$ satisfying the following two properties:

a) *Additivity*: for all $x_1, x_2 \in X$,

$$f(x_1 + x_2) = f(x_1) + f(x_2).$$

b) *Homogeneity*: for all $x \in X$ and all $\alpha \in \mathbb{R}$,

$$f(\alpha x) = \alpha f(x).$$

Linear functionals play a central role in linear algebra and its applications. However, in many economic settings they impose strong structural restrictions. For instance, linear production functions necessarily exhibit constant returns to scale, while linear utility functions rule out satiation, since utility increases without bound along any positive direction.

For this reason, it is often useful to consider broader classes of functions that relax linearity while preserving some of its key features. In particular, convex and homogeneous functions generalize important aspects of linear functionals and provide more flexible functional forms for economic modeling.

Definition **1.8.2** (Convex function). Let X be a real vector space and let $S \subseteq X$ be a convex set. A function $f: S \to \mathbb{R}$ is said to be *convex* if for every $x_1, x_2 \in S$ and every $\alpha \in [0, 1]$,

$$f(\alpha x_1 + (1-\alpha)x_2) \leq \alpha f(x_1) + (1-\alpha) f(x_2).$$

Equivalently, the value of f at any convex combination of two points is no greater than the corresponding convex combination of the function values at those points.

A function $f: S \to \mathbb{R}$ is *strictly convex* if the above inequality is strict for all distinct $x_1, x_2 \in S$ and all $\alpha \in (0, 1)$.

Remark **1.8.3**. Strictly speaking, when X is an abstract vector space one should refer to *convex functionals* rather than convex functions. Nevertheless, the term *convex function* is standard and will be used throughout.

Example **1.8.4**. The familiar functions $f(x) = x^2$ and $f(x) = \exp x$ are illustrated in figure 1.1.

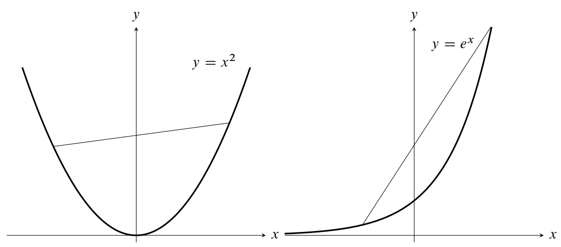


Figure 1.1: Two examples of convex functions.

Exercise 1.8.A. Show that $f(x) = x^2$ and $f(x) = \exp(x)$ are convex in $\mathbb{R}$ using the definition 1.8.2.

Exercise 1.8.B. Show that the power functions $f(x) = x^n$, $n = 1, 2, \dots$ are convex on $\mathbb{R}_+$.

***Example* 1.8.5** (Competitive firm and profit function). A competitive firm buys and sells at fixed prices $p \in \mathbb{R}^n \setminus 0$. Let $Y \subseteq \mathbb{R}^n$ be a nonempty, convex set representing the production possibilities of a competitive firm. Given a price vector p, the profit generated by a production plan $y \in Y$ is

$$f(y, p) := \sum_{i=1}^{n} p_i y_i = p \cdot y.$$

The firm chooses a feasible production plan to maximize profit, that is,

$$\sup_{y \in Y} f(y, p).$$

The associated value function

$$\Pi(p) := \sup_{y \in Y} p \cdot y$$

is called the *profit function*.

We claim that Π is a convex function of prices. Let $p_1, p_2 \in \mathbb{R}^n$ and let $\alpha \in [0, 1]$. Set $\bar{p} := \alpha p_1 + (1 - \alpha) p_2$. For any $\varepsilon > 0$, choose $y_\varepsilon \in Y$ such that

$$\Pi(\bar{p}) - \varepsilon < \bar{p} \cdot y_\varepsilon.$$

Then

$$\begin{aligned} \Pi(\bar{p}) - \varepsilon < (\alpha p_1 + (1 - \alpha) p_2) \cdot y_\varepsilon &= \alpha\, p_1 \cdot y_\varepsilon + (1 - \alpha)\, p_2 \cdot y_\varepsilon \\ &\leq \alpha \Pi(p_1) + (1 - \alpha) \Pi(p_2) \end{aligned}$$

Since ε is arbitrary, it follows that

$$\Pi(\alpha p_1 + (1 - \alpha) p_2) \leq \alpha \Pi(p_1) + (1 - \alpha) \Pi(p_2),$$

and hence Π is convex.

Geometrically, the graph of a convex function lies below the line segment joining any two points of the graph. This observation reveals a close connection between convex functions and convex sets. In particular, convexity of a function can be characterized in terms of convexity of its epigraph (definition B.2.18):

$$\operatorname{epi}(f) = \{(x, y) \in X \times \mathbb{R} : y \geq f(x)\}.$$

Proposition 1.8.6 (Convexity and epigraphs). *Let X be a real vector space, let $S \subseteq X$ be a convex set, and let $f : S \to \mathbb{R}$. Then f is convex if and only if* $\operatorname{epi}(f)$ *is a convex subset of $X \times \mathbb{R}$.*

Proof. Assume first that f is convex. Let $(x_1, y_1), (x_2, y_2) \in \operatorname{epi}(f)$. Then $f(x_1) \le y_1$ and $f(x_2) \le y_2$. For any $\alpha \in [0, 1]$, define

$$\bar{x} := \alpha x_1 + (1 - \alpha)x_2, \qquad \bar{y} := \alpha y_1 + (1 - \alpha)y_2.$$

By convexity of f,

$$f(\bar{x}) = f(\alpha x_1 + (1 - \alpha)x_2) \le \alpha f(x_1) + (1 - \alpha)f(x_2) \le \alpha y_1 + (1 - \alpha)y_2 = \bar{y}.$$

Hence $(\bar{x}, \bar{y}) \in \operatorname{epi}(f)$, and therefore $\operatorname{epi}(f)$ is convex.

Conversely, assume that $\operatorname{epi}(f)$ is convex. Let $x_1, x_2 \in S$, and set $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Then $(x_1, y_1), (x_2, y_2) \in \operatorname{epi}(f)$. For any $\alpha \in [0, 1]$, define

$$\bar{x} := \alpha x_1 + (1 - \alpha)x_2, \qquad \bar{y} := \alpha y_1 + (1 - \alpha)y_2.$$

By convexity of $\operatorname{epi}(f)$, we have $(\bar{x}, \bar{y}) \in \operatorname{epi}(f)$, and hence $f(\bar{x}) \le \bar{y}$. That is,

$$f(\alpha x_1 + (1 - \alpha)x_2) \le \alpha f(x_1) + (1 - \alpha)f(x_2),$$

so f is convex. /ᐠ｡ꞈ｡ᐟ\

Corollary 1.8.7 (Convex cross sections). *Let X be a real vector space, let $S \subseteq X$ be convex, and let $f : S \to \mathbb{R}$. For $x_1, x_2 \in S$, define $h : [0, 1] \to \mathbb{R}$ by*

$$h(t) := f\big((1 - t)x_1 + tx_2\big).$$

Then f is convex if and only if h is a convex function on $[0, 1]$ *for every $x_1, x_2 \in S$.*

Proof. The epigraph of h is

$$\operatorname{epi}(h) = \{(t, y) \in [0, 1] \times \mathbb{R} : h(t) \le y\}.$$

For $(t, y) \in [0, 1] \times \mathbb{R}$, note that

$$(t, y) \in \operatorname{epi}(h) \iff \big((1 - t)x_1 + tx_2,\ y\big) \in \operatorname{epi}(f).$$

Assume $\operatorname{epi}(f)$ is convex. Take $(t_1, y_1), (t_2, y_2) \in \operatorname{epi}(h)$ and let $\alpha \in [0, 1]$. Define

$$z_1 := (1 - t_1)x_1 + t_1 x_2, \qquad z_2 := (1 - t_2)x_1 + t_2 x_2.$$

Then $(z_1, y_1), (z_2, y_2) \in \operatorname{epi}(f)$. By convexity of $\operatorname{epi}(f)$,

$$(\alpha z_1 + (1-\alpha)z_2,\ \alpha y_1 + (1-\alpha)y_2) \in \operatorname{epi}(f).$$

But

$$\alpha z_1 + (1-\alpha)z_2 = \big(1-\bar{t}\big)x_1 + \bar{t}x_2, \qquad \bar{t} := \alpha t_1 + (1-\alpha)t_2 \in [0,1].$$

Hence

$$\big(\bar{t},\ \alpha y_1 + (1-\alpha)y_2\big) \in \operatorname{epi}(h),$$

so $\operatorname{epi}(h)$ is convex.

Conversely, assume $\operatorname{epi}(h)$ is convex. Take $(z_1, y_1), (z_2, y_2) \in \operatorname{epi}(f)$ with $z_1, z_2 \in \{(1-t)x_1 + tx_2 : t \in [0,1]\}$. Choose $t_1, t_2 \in [0,1]$ such that $z_i = (1-t_i)x_1 + t_i x_2$ for $i = 1, 2$. Then $(t_1, y_1), (t_2, y_2) \in \operatorname{epi}(h)$. By convexity of $\operatorname{epi}(h)$, for any $\alpha \in [0,1]$,

$$(\bar{t},\ \alpha y_1 + (1-\alpha)y_2) \in \operatorname{epi}(h), \qquad \bar{t} := \alpha t_1 + (1-\alpha)t_2.$$

Therefore

$$\big((1-\bar{t})x_1 + \bar{t}x_2,\ \alpha y_1 + (1-\alpha)y_2\big) \in \operatorname{epi}(f),$$

so $\operatorname{epi}(f)$ is convex (along the segment determined by x_1 and x_2).

By Proposition 1.8.6, $\operatorname{epi}(h)$ is convex if and only if h is convex, and $\operatorname{epi}(f)$ is convex if and only if f is convex. Hence h is convex if and only if f is convex.

/ᐠ｡ꞈ｡ᐟ\

As usual, a picture is worth a thousand words. An illustration of why corollary 1.8.7 is given in figure 1.2.

Exercise 1.8.C.🐾 (Jensen's inequality.) A function $f : S \to \mathbb{R}$ is convex if and only if

$$f\Big(\sum_{i=1}^{n} \alpha_i x_i\Big) \le \sum_{i=1}^{n} \alpha_i f(x_i)$$

for all $\alpha_i \ge 0$, $x_i \in S$, $i = 1, \dots, n$, $\sum_{i=1}^{n} = \alpha_i = 1$,

Exercise 1.8.D. (Weighted AM–GM inequality.) Let $x_1, \dots, x_n \in \mathbb{R}_+$ and let $\alpha_1, \dots, \alpha_n \ge 0$ satisfy $\sum_{i=1}^{n} \alpha_i = 1$. Show that

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \le \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

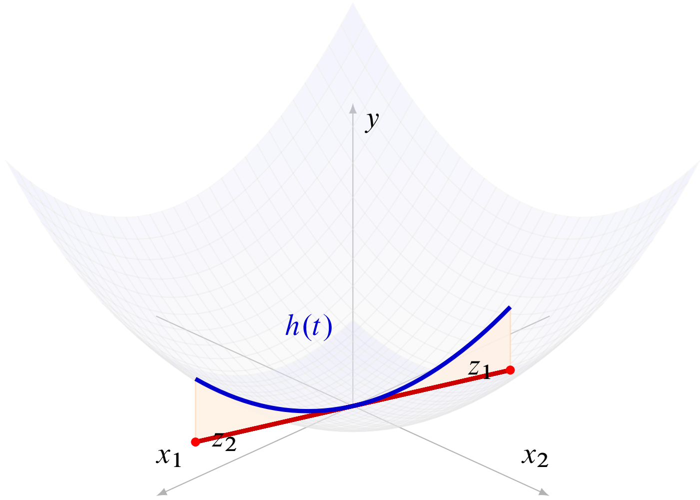


Figure 1.2: Illustration of the function $h(t)$.

Deduce that the arithmetic mean of positive numbers is greater than or equal to the geometric mean, that is,

$$\frac{1}{n}\sum_{i=1}^{n} x_i \geq \left(\prod_{i=1}^{n} x_i\right)^{1/n}.$$

Hint: Use the fact that the function $x \mapsto e^x$ is convex.

Concave functions are even more common in Economics, as the reader may remember from countless examples in the classical theory of the consumer and the producer under competitive markets.

Definition **1.8.8** (Concave function). Let X be a real vector space and let $S \subseteq X$ be a convex set. A function $f\colon S \to \mathbb{R}$ is said to be *concave* if for every $x_1, x_2 \in S$ and every $\alpha \in [0, 1]$,

$$f(\alpha x_1 + (1-\alpha)x_2) \geq \alpha f(x_1) + (1-\alpha) f(x_2).$$

Equivalently, the value of f at any convex combination of two points is no less than the corresponding convex combination of the function values at those points.

A function $f\colon S \to \mathbb{R}$ is *strictly concave* if the above inequality is strict for all distinct $x_1, x_2 \in S$ and all $\alpha \in (0, 1)$.

Exercise 1.8.E. f is concave if and only if $-f$ is convex.

Similarly to convex functions, concavity of a function can be characterized in terms of convexity of its hypograph (definition B.2.19):

$$\operatorname{hypo}(f) = \{(x, y) \in X \times \mathbb{R} : y \leq f(x)\}.$$

Proposition 1.8.9 (Concavity and hypographs). *Let X be a real vector space, let $S \subseteq X$ be a convex set, and let $f: S \to \mathbb{R}$. Then f is concave if and only if* $\operatorname{hypo}(f)$ *is a convex subset of $X \times \mathbb{R}$.*

Exercise 1.8.F. Prove propostion 1.8.9 and state and prove and analogue of corollary 1.8.7 for concave functions.

***Example* 1.8.10** (Inverse functions). Let $f: \mathbb{R} \to \mathbb{R}$ be invertible with inverse $g = f^{-1}$. Then

$$\operatorname{hypo}(f) = \{(x, y) \in \mathbb{R}^2 : y \leq f(x)\} = \{(x, y) \in \mathbb{R}^2 : g(y) \leq x\},$$

while

$$\operatorname{epi}(g) = \{(y, x) \in \mathbb{R}^2 : g(y) \leq x\}.$$

In particular, $\operatorname{hypo}(f)$ is convex if and only if $\operatorname{epi}(g)$ is convex. Therefore, f is concave if and only if g is convex.

The next battery of examples are a sequel to example 1.8.5 and continue developing important concepts in producer theory under competitive markets.

***Example* 1.8.11** (Production function). The technology of a firm producing a single output from n inputs can be represented by its production function f, where

$$y = f(x)$$

is the maximum output attainable from inputs $x \in X \subseteq \mathbb{R}^n_+$.

If the production function is concave, the technology exhibits nonincreasing returns to scale. If the production function is strictly concave, the technology exhibits decreasing returns to scale.

***Example* 1.8.12** (Production possibility set). The relationship between a production function f and the underlying production possibility set Y is slightly delicate because of the convention that inputs have negative sign in the production set Y.

Given a production function f, define the function

$$g(x) = f(-x) \qquad \text{for every } x \in \mathbb{R}^n_-.$$

The function g, under this convention of inputs entering with a negative sign, is usually called the *net output function*. Then the production possibility set Y is the hypograph of the function g, $Y = \text{hypo}(g)$. The production function f is concave if and only if the production possibility set Y is convex. See figure 1.3 for an illustration.

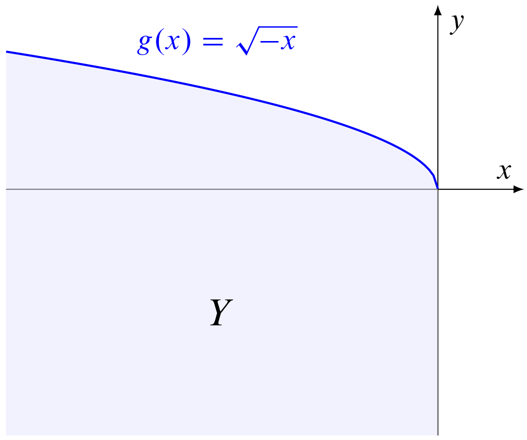


Figure 1.3: The production set induced by the production function $f(x) = \sqrt{x}$ and its net output function $g(x) = \sqrt{-x}$.

Example **1.8.13.** Suppose that the technology of a firm producing a single output y can be represented by the production function $f : X \to \mathbb{R}$, $X \subseteq \mathbb{R}^n_+$. The *input requirement sets* are the upper contours of f (see definition B.2.20):

$$V(y) := \{x \in X : f(x) \geq y\}.$$

Example **1.8.14** (Cost function). In another useful model of the producer, also relevant for the analysis of monopolies and oligopolies, the firm takes input prices as given and seeks to minimize the cost of producing a given level of output.

For simplicity, suppose the firm produces a single output. Let $V(y) \subseteq \mathbb{R}^n_+$ denote the input requirement set for each output level y. Given input prices $w \in \mathbb{R}^n_+ \setminus \{0\}$, the cost of an input bundle x is $w \cdot x$.

The associated value function

$$c(w, y) = \inf_{x \in V(y)} w \cdot x$$

is called the *cost function*.

1.8.2 Properties of Convex Functions

We record here some useful rules for combining convex functions. Analogous rules apply for concave functions. The proof of all of the results in this section are left as an exercise for the reader. In all the subsequent definitions, X is a real vector space, and $S \subset X$ with S convex.

EXERCISE 1.8.G.🐾 Let $f, g \in \mathbb{R}^S$ be convex functions. Prove that:

a) $f + g$ is convex.

b) αf is convex for every $\alpha \geq 0$.

Moreover, if f is strictly convex, then

a) $f + g$ is strictly convex.

b) αf is strictly convex for every $\alpha > 0$.

EXERCISE 1.8.H. Construct an example in which $f + g$ is strictly convex, but neither f nor g are strictly convex.

EXERCISE 1.8.I.🐾 Let $\{f_i\}_{i \in I}$ be a family of convex functions in $\mathbb{R}^S$. Assume that the function $F \in \mathbb{R}^S$ defined by

$$F(x) = \sup_{i \in I} f_i(x) \qquad \text{for every } x \in S$$

is well-defined; that is, $F(x) \in \mathbb{R}$ for every $x \in S$. Prove that F is convex.

EXERCISE 1.8.J.🐾 (Composition.) Let $f \in \mathbb{R}^S$ and $g \in \mathbb{R}^{\mathbb{R}}$, and suppose that g is increasing. Prove that:

a) If f and g are convex, then $g \circ f$ is convex.

b) If f and g are concave, then $g \circ f$ is concave.

EXERCISE 1.8.K. (Log transformation.) Logarithmic transformations are often used in analysis. It is useful to know that they preserve concavity.

Since log is concave and increasing, exercise 1.8.J implies that, if f is nonnegative,

$$f \text{ concave} \implies \log f \text{ concave}.$$

Convex and concave functions occupy a central role in analysis because their geometric structure allows one to promote local information into global conclusions. In general, local regularity properties do not propagate: a function may behave nicely near one point and be highly irregular elsewhere. For instance, continuity at a point implies boundedness in a neighborhood of that point, but boundedness at a single point has no implications for continuity in general.

Convexity radically changes this picture. For a convex function defined on an open convex set, boundedness above in a neighborhood of a single point already forces continuity on the entire domain. The geometric constraint imposed by convexity ties together the values of the function along line segments, preventing wild oscillations and controlling its slopes. As a result, a seemingly weak local condition becomes a global regularity statement.

In what follows, we assume that X is a real normed vector space and endow it with the metric induced by its norm.

Proposition 1.8.15 (Continuity of convex functions). *Let f be a convex function defined on an open convex set S in a normed linear space. If f is bounded from above in a neighborhood of a single point $x_0 \in S$, then f is continuous on S.*

The following important corollary implies that any convex function on a finite-dimensional space is continuous on the interior of its domain.

Corollary 1.8.16. *Let f be a convex function on an open convex set S in a finite-dimensional normed linear space. Then f is continuous.*

***Remark* 1.8.17.** The role of finite dimensionality is to ensure local boundedness. In finite-dimensional normed spaces, a convex function is automatically locally bounded on the interior of its domain. Combined with Proposition 1.8.15, this yields continuity.

In contrast, in infinite-dimensional normed spaces there exist convex functions on open convex sets that fail to be locally bounded and therefore fail to be continuous. Finite dimensionality prevents this pathological behavior.

***Remark* 1.8.18.** The hypothesis that the domain be open is essential in the continuity results above. If the domain is merely closed and convex, a convex function need not be continuous at boundary points of the domain. Examples 1.8.19 and 1.8.20 illustrate this phenomenon.

***Example* 1.8.19** (Boundary discontinuity in one dimension). Let $S = \mathbb{R}_+$ and define $f : S \to \mathbb{R}$ by

$$f(x) = \begin{cases} 1, & x = 0, \\ 0, & x > 0. \end{cases}$$

Then f is convex on S, but it is not continuous at 0. This example shows that convex functions may fail to be continuous at boundary points.

***Example* 1.8.20** (Boundary discontinuity in higher dimension). Let $S = \{x \in \mathbb{R}^2 : \|x\|_2 \leq 1\}$ be the closed unit disk, and define $f : S \to \mathbb{R}$ by

$$f(x) = \begin{cases} \|x\|_2, & \|x\|_2 < 1, \\ 2, & \|x\|_2 = 1. \end{cases}$$

Then f is convex on S, but it is not continuous on $\partial S = \{x \in \mathbb{R}^2 : \|x\|_2 = 1\}$. Again, the discontinuity occurs only at boundary points of the domain.

The proofs of the proposition 1.8.15 and corollary 1.8.16 are left as exercises. They can be established by following a natural sequence of intermediate results, which will be developed below, also in the form of exercises.

Exercise 1.8.L. Let $S \subseteq X$ be an open set and let $f : S \to \mathbb{R}$ be convex. Suppose that there exist $x_0 \in S$, $M \in \mathbb{R}$, and $r > 0$ such that

$$B_r(x_0) \subseteq S \quad \text{and} \quad f(x) \leq M \quad \text{for every } x \in B_r(x_0)\,.$$

a) Show that for every $x \in B_r(x_0)$ and every $\alpha \in [0, 1]$,

$$f\big(\alpha x + (1-\alpha)x_0\big) \leq \alpha M + (1-\alpha) f(x_0).$$

b) Fix $x \in B_r(x_0)$ and $\alpha \in [0, 1]$. Let $z = \alpha x + (1-\alpha)x_0$. Show that

$$x_0 = \frac{1}{1+\alpha} z + \frac{\alpha}{1+\alpha}(2x_0 - x).$$

c) Deduce that $)f(x_0) - f(z) \leq \alpha\big(M - f(x_0)\big)$.

d) Conclude that f is continuous at x_0.

Exercise 1.8.M. Let $S \subseteq X$ be an open set and let $f : S \to \mathbb{R}$ be convex. Suppose that there exist $x_0 \in S$, $M \in \mathbb{R}$, and $r > 0$ such that

$$B_r(x_0) \subseteq S \quad \text{and} \quad f(x) \leq M \quad \text{for every } x \in B_r(x_0)\,.$$

Let $x_1 \in S$ be arbitrary.

a) Show that there exists $t > 1$ such that $z = x_0 + t(x_1 - x_0) \in S$.

b) Define
$$T = \{(1-\alpha)x + \alpha z : x \in B_r(x_0)\,, \alpha \in [0, 1]\}\,.$$
Show that there exists $\delta > 0$ such that $B_\delta(x_1) \subseteq T$.

c) Show that f is bounded above on T.

Exercise 1.8.N. Let f be a convex function on an open set S that is bounded at a single point. Show that f is locally bounded. That is, for every $x \in S$ there exist $r > 0$ and $M \in \mathbb{R}$ such that

$$B_r(x) \subseteq S \quad \text{and} \quad \left|f(x')\right| \leq M \quad \text{for every } x' \in B_r(x)\,.$$

Exercise 1.8.O. Prove Proposition 1.8.15

Exercise 1.8.P. Prove Corollary 1.8.16

We close this section by stating and proving an interesting result about *midpoint convexity*. It turns out that if a function is continuous, it suffices to verify the convexity inequality only at the midpoint in order to conclude that the function is convex. The statement is not only quite beautiful, but its proof relies on a less commonly encountered induction argument (see Exercise C.1.C).[9]

Proposition 1.8.21. *Suppose $f : \mathbb{R}^N \to \mathbb{R}$ is continuous. Then f is convex if and only if for all $x_1, x_2 \in \mathbb{R}^N$*

$$f\left(\frac{x_1 + x_2}{2}\right) \geq \frac{f(x_1)}{2} + \frac{f(x_2)}{2}$$

Proof. First, we will prove that for all $n \in \mathbb{N}$ and $x_1, \ldots x_n \in \mathbb{R}^N$ we have that

$$f\left(\frac{x_1 + \cdots + x_n}{n}\right) \geq \frac{1}{n} f(x_1) + \ldots \frac{1}{n} f(x_n)$$

Denote the proposition that the inequality above holds as $P(n)$. We will show the following:

a) If $P(n)$ is true, then $P(2n)$ is true.

b) If $P(n)$ is true, then $P(n-1)$ is true.

Make sure you understand why the inequality then follows for all $n \in \mathbb{N}$ (see ex. C.1.C). Now let's proceed to the proof.

[9] I thank Abuzer Abuov for reminding me of this beautiful result and for kindly providing its proof. Absolute Cinema!

(1): Suppose $P(n)$ holds and let $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{R}^N$. Denote $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ and $\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$. Then

$$f\left(\frac{x_1 + \ldots x_n + y_1 + \ldots y_n}{2n}\right) = f\left(\frac{\bar{x}+\bar{y}}{2}\right) \geq \frac{1}{2}\left(f(\bar{x}) + f(\bar{y})\right) \geq$$

$$\geq \frac{1}{2} f\left(\frac{1}{n}\sum_{i=1}^{n} x_i + \frac{1}{n}\sum_{i=1}^{n} y_i\right) = \frac{1}{2n} f\left(\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i\right)$$

Where the first inequality follows from the problem condition and the second inequality follows from $P(n)$.

(2): Suppose $P(n)$ holds and let $x_1, \ldots, x_{n-1} \in \mathbb{R}^N$. Denote $\bar{x} = \frac{1}{n-1}\sum_{i=1}^{n-1} x_i$. Note that

$$\bar{x} = \frac{x_1 + \ldots x_{n-1} + \bar{x}}{n}$$

Then from $P(n)$ we know that

$$f(\bar{x}) = f\left(\frac{x_1 + \cdots + x_{n-1} + \bar{x}}{n}\right) \geq \frac{1}{n}\left(f(x_1) + \ldots f(x_{n-1}) + f(\bar{x})\right)$$

By multiplying both sides of the inequality by n we get

$$(n-1) f(\bar{x}) \geq \sum_{i=1}^{n-1} f(x_i) \implies f(\bar{x}) \geq \frac{1}{n-1}\sum_{i=1}^{n-1} f(x_i)$$

Which is exactly what we wanted to prove.

Now we're going to prove that for all $x_1, x_2 \in \mathbb{R}^N$ and for all rational $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}$ such that $\frac{p_1}{q_1} + \frac{p_2}{q_2} = 1$ we have

$$f\left(\frac{p_1}{q_1}x_1 + \frac{p_2}{q_2}x_2\right) \geq \frac{p_1}{q_1} f(x_1) + \frac{p_2}{q_2} f(x_2)$$

Indeed, note that since we can bring both rational to the common denominator, we may assume, without loss of generality, that $q_1 = q_2 = q$ and $p_1 + p_2 = q$. Then consider the list that consists of x_1 repeated p_1 times and x_2 repeated p_2 times. By applying $P(q)$ to this list, we get exactly what we wanted to prove. The convexity of f then follows from the continuity of f and density of rationals over $\mathbb{R}$. ^. .^)9

1.8.3 Quasiconcave Functions

Convex and concave functions play a central role in economic analysis, but they remain somewhat restrictive for many economic models. In particular, convexity and concavity are not preserved under the ordinal transformations of utility functions, that is, under strictly increasing monotonic transformations. Thus, properties based purely on convexity may fail to be invariant under changes of utility representation.

Definition **1.8.22** (Quasiconcave and strictly quasiconcave functions). Let X be a real vector space and let $S \subseteq X$ be a convex set. A function $f : S \to \mathbb{R}$ is said to be *quasiconcave* if, for every $x_1, x_2 \in S$ and every $\alpha \in [0, 1]$,

$$f(\alpha x_1 + (1 - \alpha)x_2) \geq \min\{f(x_1), f(x_2)\}.$$

The function f is said to be *strictly quasiconcave* if, for every distinct $x_1, x_2 \in S$ and every $\alpha \in (0, 1)$,

$$f(\alpha x_1 + (1 - \alpha)x_2) > \min\{f(x_1), f(x_2)\}.$$

We also present the definition of quasiconvexity for completeness sake.

Definition **1.8.23** (Quasiconvex and strictly quasiconvex functions). Let X be a real vector space and let $S \subseteq X$ be a convex set. A function $f : S \to \mathbb{R}$ is said to be *quasiconvex* if, for every $x_1, x_2 \in S$ and every $\alpha \in [0, 1]$,

$$f(\alpha x_1 + (1 - \alpha)x_2) \leq \max\{f(x_1), f(x_2)\}.$$

The function f is said to be *strictly quasiconvex* if, for every distinct $x_1, x_2 \in S$ and every $\alpha \in (0, 1)$,

$$f(\alpha x_1 + (1 - \alpha)x_2) < \max\{f(x_1), f(x_2)\}.$$

Convexity and concavity impose strong geometric restrictions: for a concave function, the graph must lie above every secant line joining two points. Quasiconcavity weakens this requirement substantially. It does not control the full secant line, but only prevents the function from falling below the smaller of the two endpoint values along the segment. Thus, while concavity is a statement about all secant lines, quasiconcavity is a statement about horizontal secants.

In economic applications, quasiconcave functions arise far more frequently than quasiconvex ones, so we will focus on the former in this section. The function whose graph resembles the mantle of a ghost is quasiconcave and is illustrated in Figure 1.4.

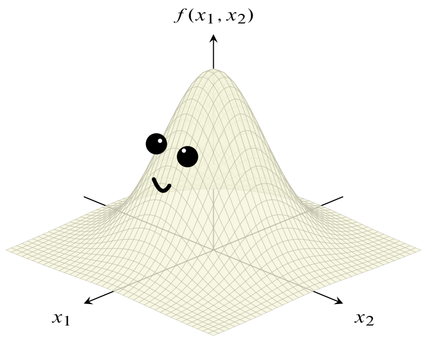


Figure 1.4: Example of a quasiconcave function: A ghost-shaped function.

***Joke* 1.8.24.** Some people call the graph of the function illustrated in figure 1.4 the bivariate standard normal density:

$$f(x) = \frac{1}{2\pi} \exp\left(-\frac{1}{2}\|x\|_2^2\right),$$

where $x \in \mathbb{R}^2$. In these notes, however, it shall be known simply as a ghost.

Next we state some properties and results about quasiconcave functions. For the remainder of the section, X denotes a real vector space and let $S \subseteq X$ a convex set.

Exercise 1.8.Q. A function $f : S \to \mathbb{R}$ is quasiconcave if and only if $-f$ is quasiconvex.

Exercise 1.8.R.🐾 Every concave function is quasiconcave.

Similarly to convex and concave functions, quasiconcave and quasiconvex functions have an analogous characterization in terms of some special sets, i.e., their upper and lower contour sets (see definitions B.2.20 and B.2.21).

Proposition 1.8.25 (Quasiconcavity). *Let X be a real vector space and let $S \subseteq X$ be convex. A function $f : S \to \mathbb{R}$ is quasiconcave if and only if $U_f(c)$ is convex for every $c \in \mathbb{R}$, where*

$$U_f(c) = \{x \in S : f(x) \geq c\}.$$

Proof. Assume that f is quasiconcave and fix $c \in \mathbb{R}$. If $U_f(c)$ is empty, there is nothing to prove. Otherwise, let $x_1, x_2 \in U_f(c)$. Then $f(x_1) \geq c$ and $f(x_2) \geq c$. For every $\alpha \in [0, 1]$, quasiconcavity yields

$$f(\alpha x_1 + (1-\alpha)x_2) \geq \min\{f(x_1), f(x_2)\} \geq c.$$

Thus $\alpha x_1 + (1-\alpha)x_2 \in U_f(c)$, and $U_f(c)$ is convex.

Conversely, assume that $U_f(c)$ is convex for every $c \in \mathbb{R}$. Let $x_1, x_2 \in S$ and define $c = \min\{f(x_1), f(x_2)\}$. Then $x_1, x_2 \in U_f(c)$. By convexity of $U_f(c)$, for every $\alpha \in [0,1]$,

$$\alpha x_1 + (1-\alpha)x_2 \in U_f(c).$$

Hence

$$f(\alpha x_1 + (1-\alpha)x_2) \geq c = \min\{f(x_1), f(x_2)\}.$$

Therefore f is quasiconcave. /ᐠ｡ꞈ｡ᐟ\

Exercise 1.8.S. Let X be a real vector space and let $S \subseteq X$ be convex. A function $f\colon S \to \mathbb{R}$ is quasiconvex if and only if $L_f(c)$ is convex for every $c \in \mathbb{R}$, where

$$L_f(c) = \{x \in S : f(x) \leq c\}.$$

Example **1.8.26**. Recall the input requirement set of a single output firm

$$V(y) = \{x \in X : f(x) \geq y\} = U_f(y).$$

The firm's technology is convex, i.e., $V(y)$ is convex for every y, if and only if the production function f is quasiconcave. This is less restrictive than assuming that the production function f is concave, which is equivalent to the assumption that the production possibility set is convex (see example 1.8.12). The assumption of a convex technology $V(y)$, which is saying that $V(y)$ is convex or f quasiconcave) is typical in economic models, since it allows us to consider increasing returns to scale.

Unlike concavity, quasiconcavity is not preserved under addition. Thus, there is no analogue of the additivity properties enjoyed by concave functions.

Example **1.8.27**. Let $f(x) = -2x$ and $g(x) = x^3 + x$ on $\mathbb{R}$. Then f is concave and g is quasiconcave, but

$$(f+g)(x) = x^3 - x$$

is neither concave nor quasiconcave.

The following proposition captures one of the central reasons for the use of quasiconcave functions in economics: quasiconcavity is invariant under increasing transformations.

Proposition 1.8.28 (Monotonic transformations). *Let $S \subseteq X$ be convex and let $f\colon S \to \mathbb{R}$ be quasiconcave. If $g\colon \mathbb{R} \to \mathbb{R}$ is increasing, then $g \circ f$ is quasiconcave.*

Proof. Let $x_1, x_2 \in S$ and $\alpha \in [0, 1]$. Since f is quasiconcave,

$$f(\alpha x_1 + (1-\alpha)x_2) \geq \min\{f(x_1), f(x_2)\}.$$

Because g is increasing,

$$g(f(\alpha x_1 + (1-\alpha)x_2)) \geq g(\min\{f(x_1), f(x_2)\}).$$

Monotonicity of g implies

$$g(\min\{f(x_1), f(x_2)\}) = \min\{g(f(x_1)), g(f(x_2))\}.$$

Hence

$$g \circ f(\alpha x_1 + (1-\alpha)x_2) \geq \min\{g \circ f(x_1), g \circ f(x_2)\}.$$

Therefore $g \circ f$ is quasiconcave. /°^°\

Definition **1.8.29.** Let $S \subseteq X$ be a convex set. A function $f : S \to \mathbb{R}$ is said to be *concavifiable* if there exists a strictly increasing transformation $G : \mathrm{Im}\,(f) \to \mathbb{R}$ such that the composite function $h : X \to \mathbb{R}$ defined by

$$h(x) = G \circ f(x)$$

is a concave function on S.

Remark **1.8.30.** Every concavifiable function is quasiconcave 1.8.28. However, the converse is not true in general, since there exist quasiconcave functions that are not concavifiable.

Exercise 1.8.T. Let $S \subset \mathbb{R}$ be a convex set. If $f : S \to \mathbb{R}$ is strictly increasing then it is concavifiable.

1.9 Homogeneous and Homothetic Functions

1.9.1 Homogeneous Functions

Concave and convex functions generalize the additivity property of linear functionals. On the other hand, homogeneous functions generalize homogeneity.

Before we can define homogeneity, we need to introduce the notion of a *cone*.

Definition **1.9.1.** Let X be a real vector space. A set $S \subseteq X$ is a *cone* if $\alpha S \subseteq S$ for all $\alpha \geq 0$.

With the definition of a cone, we can define homogeneous functions.

Definition **1.9.2.** Let X be a real vector space and let $S \subseteq X$ be a cone. We say that the functional $f : S \to \mathbb{R}$ is *homogeneous of degree* k if for every $x \in S$,

$$f(tx) = t^k f(x) \qquad \text{for every } t > 0.$$

Remark **1.9.3.** Definition 1.9.2 relaxes the homogeneity requirement of a linear functions and dispenses with additivity.

Example **1.9.4** (Power function). The general power function $f : \mathbb{R}_+ \to \mathbb{R}$

$$f(x) = x^a$$

is homogeneous of degree a, since $f(tx) = (tx)^a = t^a f(x)$.

Exercise 1.9.A.❀ A function $f : \mathbb{R}_+ \to \mathbb{R}$ is homogeneous of degree a if and only if it is a multiple of a power function, that is,

$$f(x) = Ax^a \qquad \text{for some } a \in \mathbb{R}.$$

Exercise 1.9.B. (Cobb–Douglas.) Fix $n \in \mathbb{N}$ and let $a_1, \ldots, a_n \in \mathbb{R}$. Define $f : \mathbb{R}^n_{++} \to \mathbb{R}_{++}$ by

$$f(x) = \prod_{i=1}^{n} x_i^{a_i}, \qquad x = (x_1, \ldots, x_n) \in \mathbb{R}^n_{++}.$$

Show that f is homogeneous of degree $a_1 + \cdots + a_n$, i.e., for every $t > 0$ and every $x \in \mathbb{R}^n_{++}$,

$$f(tx) = t^{a_1 + \cdots + a_n} f(x).$$

Exercise 1.9.C. (CES function.) Fix $n \in \mathbb{N}$, let $a_1, \ldots, a_n \in \mathbb{R}_{++}$ and let $\rho \in \mathbb{R} \setminus \{0\}$. Define $f : \mathbb{R}^n_{++} \to \mathbb{R}_{++}$ by

$$f(x) = \left(a_1 x_1^\rho + a_2 x_2^\rho + \cdots + a_n x_n^\rho\right)^{1/\rho}, \qquad x = (x_1, \ldots, x_n) \in \mathbb{R}^n_{++}.$$

Show that f is homogeneous of degree one.

The explicit characterization of homogeneous functions on $\mathbb{R}_+$ from exercise 1.9.A can help us understand the structure of homogeneous functions on more general domains.

Proposition 1.9.5 (Ray characterization of homogeneity). *Let X be a real vector space and let $S \subseteq X$ be a cone. Fix $k \in \mathbb{R}$ and let $f : S \to \mathbb{R}$.*

For each $x \in S$, define the ray cross-section *of f along the ray generated by x by*

$$h_x : \mathbb{R}_{++} \to \mathbb{R}, \qquad h_x(t) := f(tx).$$

Then the following are equivalent:

a) f is homogeneous of degree k, that is,

$$f(tx) = t^k f(x) \quad \text{for every } x \in S \text{ and every } t > 0.$$

b) For every $x \in S$, the function h_x satisfies

$$h_x(t) = t^k h_x(1) \quad \text{for every } t > 0.$$

The proof of proposition 1.9.5 is trivial, and is left as an exercise.

Exercise 1.9.D. Prove proposition 1.9.5.

***Remark* 1.9.6.** Proposition 1.9.5 implies that any homogeneous function looks like a power function when viewed along a ray.

***Example* 1.9.7** (Cobb-Douglas). The two-variable Cobb-Douglas function

$$f(x_1, x_2) = x_1^{a_1} x_2^{a_2}$$

is homogeneous of degree $a_1 + a_2$. In figure 1.1 we illustrate a Cobb-Douglas function that is homogeneous of degree 2 and its cross-section, which looks like a quadratic t^2 along any ray.

Homogeneous functions play a central role in economic analysis. Homogeneity restricts how a function behaves when all its arguments are scaled by the same factor. In production theory, this corresponds to changing the scale of operation while keeping input proportions fixed. Constant returns to scale means that the production function is homogeneous of degree one. In price-based functions (for instance, profit functions), scaling all arguments corresponds to multiplying all prices by the same positive factor, leaving relative prices unchanged. The degree of homogeneity k may be positive, negative, or zero. In applications, the most frequently encountered cases are degrees 0 and 1. Functions homogeneous of degree 0 are constant along each ray. Functions homogeneous of degree 1 are linear along every ray.

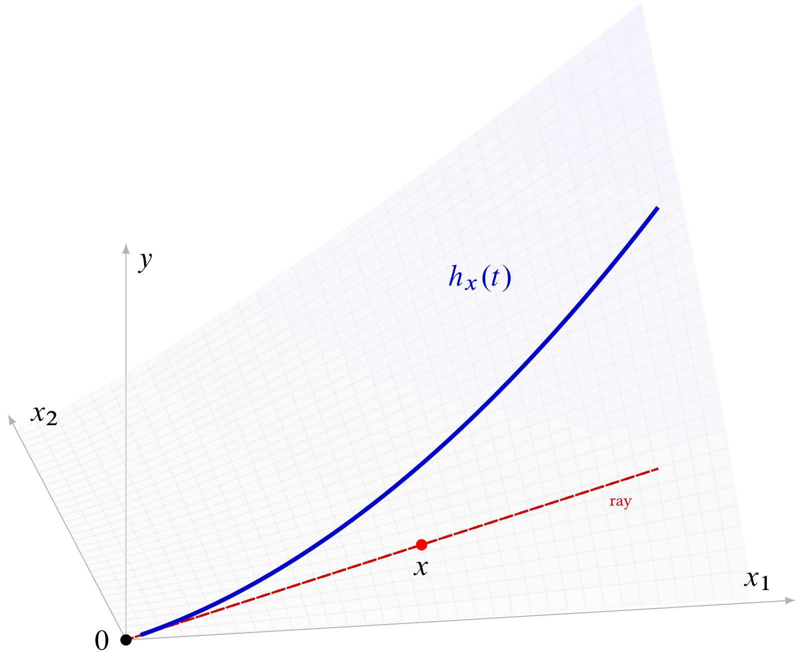


Figure 1.1: Cobb-Douglas: $f(x_1, x_2) = x_1^{1.2} x_2^{0.8}$ and cross section along ray passing through point (1.5, 1)

Definition **1.9.8** (Linearly homogeneous). Let X be a real vector space and let $S \subseteq X$ be a cone. A function $f \colon S \to \mathbb{R}$ is said to be *linearly homogeneous* if it is homogeneous of degree one, that is,

$$f(tx) = tf(x) \quad \text{for every } x \in S \text{ and every } t > 0.$$

Example **1.9.9** (Profit function). Let $Y \subseteq \mathbb{R}^n$ be a production set, let $p \in \mathbb{R}^n \setminus \{0\}$ and recall the profit function

$$\Pi(p) = \sup_{y \in Y} \sum_{i=1}^{n} p_i y_i = \sup_{y \in Y} p \cdot y.$$

Then Π is homogeneous of degree one. To prove this, fix $p \in \mathbb{R}^n \setminus \{0\}$ and $t > 0$. We first show that $\Pi(tp) \leq t\Pi(p)$. Let $\varepsilon > 0$. By definition of the supremum, there exists $y_\varepsilon \in Y$ such that

$$\Pi(tp) - \varepsilon < (tp) \cdot y_\varepsilon,$$

but then,

$$\Pi(tp) - \varepsilon < (tp) \cdot y_\varepsilon = tp \cdot y_\varepsilon \leq t\Pi(p).$$

Since $\varepsilon > 0$ was arbitrary, we get $\Pi(tp) \leq t\Pi(p)$.

For the reverse inequality, we start from

$$(tp) \cdot y_\varepsilon > \Pi(tp) - \varepsilon,$$

and notice that

$$\Pi(p) \geq p \cdot y_\varepsilon > \frac{1}{t}\Pi(tp) - \frac{\varepsilon}{t}.$$

Since $\varepsilon > 0$ was arbitrary, we get

$$\Pi(p) \geq \frac{1}{t}\Pi(tp),$$

from where we obtain $t\Pi(p) \geq \Pi(tp)$. Combining both inequalities shows that $\Pi(tp) = t\Pi(p)$. Thus Π is homogeneous of degree one.

***Example* 1.9.10** (Demand function). Let $u\colon \mathbb{R}^n_+ \to \mathbb{R}$ be continuous and strictly concave. For $p \in \mathbb{R}^n_{++}$ and $w > 0$, define the budget set

$$B(p, w) = \{x \in \mathbb{R}^n_+ : p \cdot x \leq w\}.$$

The consumer's demand function is defined as the unique solution to the utility maximization problem

$$x(p, w) = \operatorname*{arg\,max}_{x \in B(p,w)} u(x).$$

Since u is continuous and strictly concave, the maximizer is unique, so the demand function is well defined.

We claim that the demand function is homogeneous of degree zero, that is,

$$x(tp, tw) = x(p, w) \quad \text{for every } t > 0.$$

To verify this, observe that for every $x \in \mathbb{R}^n_+$,

$$p \cdot x \leq w \quad \Longleftrightarrow \quad (tp) \cdot x \leq tw.$$

Hence

$$B(tp, tw) = B(p, w) \quad \text{for every } t > 0.$$

Since the feasible set is unchanged and the objective function is the same, the unique maximizer must also be unchanged. Therefore,

$$x(tp, tw) = x(p, w).$$

Thus the demand function is homogeneous of degree zero.

Exercise 1.9.E. (Cost function.) Let $Y \subseteq \mathbb{R}^n$ be a production set and recall the the cost function from example 1.8.14

$$c(w, y) = \inf\{w \cdot x : x \in V(y)\}.$$

Show that $c(w, y)$ is homogeneous of degree one in input prices w.

Exercise 1.9.F. (Cost function with constant returns to scale.) Suppose the production function for a single output firm $f(x)$ is homogeneous of degree one. Show that the cost function $c(w, y)$ is homogeneous of degree one in output, that is,

$$c(w, y) = y\, c(w, 1).$$

There is an analogous result to proposition 1.8.6 for characterizing linearly homogeneous functions in terms of their epigraphs.

Exercise 1.9.G. Let X be a real vector space and $S \subseteq X$ a cone. A function $f : S \to \mathbb{R}$ is linearly homogeneous if and only if $\operatorname{epi}(f)$ is a cone.

It turns out that, for a strictly positive function, quasiconcavity and homogeneity combine to produce full concavity. Quasiconcavity ensures convexity of the upper contour sets, while homogeneity of degree $k \leq 1$ strengthens this to convexity of the hypograph. In order to state this result in the classical language of most of the literature, we need the following definition.

Definition **1.9.11** (Definite function). Let X be a set and let $f : X \to \mathbb{R}$. We say that f is *definite* if it does not change sign on X, that is, if one of the following holds:

(strictly positive definite)	$f(x) > 0$	for every $x \in X$,
(non-negative definite)	$f(x) \geq 0$	for every $x \in X$,
(non-positive definite)	$f(x) \leq 0$	for every $x \in X$,
(strictly negative definite)	$f(x) < 0$	for every $x \in X$.

Proposition 1.9.12. *Let X be a real vector space and let $S \subseteq X$ be a convex cone. Let $f : S \to \mathbb{R}$ be strictly positive definite, and suppose that f is homogeneous of degree k with $0 < k \leq 1$. Then f is quasiconcave if and only if f is concave.*

Proof. The "if" part follows from exercise 1.8.R. The "only if" part is developed in exercises 1.9.H through 1.9.J. ^. .^)9

Exercise 1.9.H.🐾 Let X be a real vector space and let $S \subseteq X$ be a convex cone. Suppose that $f : S \to \mathbb{R}$ is strictly positive definite, quasiconcave, and homogeneous of degree one. Show that f is superadditive, that is,

$$f(x_1 + x_2) \geq f(x_1) + f(x_2) \quad \text{for every } x_1, x_2 \in S.$$

Exercise 1.9.I.🐾 Let X be a real vector space and let $S \subseteq X$ be a convex cone. Suppose that $f : S \to \mathbb{R}$ is strictly positive definite, quasiconcave, and homogeneous of degree one. Using exercise 1.9.H, show that f is concave.

Exercise 1.9.J.🐾 Let X be a real vector space and let $S \subseteq X$ be a convex cone. Suppose that $f : S \to \mathbb{R}$ is strictly positive definite, quasiconcave, and homogeneous of degree k with $0 < k \leq 1$. Generalize exercise 1.9.I to complete the proof of proposition 1.9.12.

1.9.2 Homothetic Functions

Analogous to the generalization from concave to quasiconcave functions, there is a corresponding generalization of homogeneity. While homogeneity restricts how function values scale along each ray, homotheticity imposes a weaker requirement: it preserves the ordering of points along rays.

***Definition* 1.9.13** (Homothetic function). Let X be a real vector space and let $S \subseteq X$ be a convex cone. A function $f : S \to \mathbb{R}$ is said to be *homothetic* if

$$f(x_1) = f(x_2) \quad \Longrightarrow \quad f(tx_1) = f(tx_2)$$

for every $x_1, x_2 \in S$ and every $t > 0$.

***Remark* 1.9.14.** Clearly, every homogeneous function is homothetic, but not every homothetic function is homogeneous.

***Example* 1.9.15.** Define $f : \mathbb{R}^2_{++} \to \mathbb{R}$ by

$$f(x_1, x_2) = \log x_1 + \log x_2.$$

Then f is homothetic but not homogeneous, since for $t > 0$,

$$f(tx_1, tx_2) = 2 \log t + f(x_1, x_2),$$

so f is not homogeneous. If $f(x^1) = f(x^2)$, then

$$f(tx^1) = 2 \log t + f(x^1) = 2 \log t + f(x^2) = f(tx^2),$$

hence f is homothetic.

Exercise 1.9.K. Let X be a real vector space and let $S \subseteq X$ be a convex cone. Suppose that $f\colon S \to \mathbb{R}$ is a monotonic transformation of a homogeneous function.

Show that f is a monotonic transformation of a linearly homogeneous function.

Exercise 1.9.L. Let X be a real vector space and let $S \subseteq X$ be a convex cone. Let $h\colon S \to \mathbb{R}$ be homogeneous and let $g\colon \mathbb{R} \to \mathbb{R}$ be strictly increasing.

Show that $g \circ h$ is homothetic.

Exercise 1.9.M. Let X be a real vector space and let $S \subseteq X$ be a convex cone. Let $f\colon S \to \mathbb{R}$ be strictly increasing and homothetic.

Show that there exist a linearly homogeneous function $h\colon S \to \mathbb{R}$ and a strictly increasing function $g\colon \mathbb{R} \to \mathbb{R}$ such that

$$f = g \circ h.$$

Hint. Fix $x_0 \in S$ and define $g(\alpha) = f(\alpha x_0)$. Show that $h = g^{-1} \circ f$ is homogeneous of degree one.

Exercises 1.9.L and 1.9.M provide an equivalent characterization of homethetic-ity for strictly increasing functions that is quite useful in Economics.

Proposition 1.9.16 (Homotheticity). *Let X be a real vector space and let $S \subseteq X$ be a convex cone. Let $f\colon S \to \mathbb{R}$ be strictly increasing.*

Then f is homothetic if and only if it is a monotonic transformation of a homogeneous function.

Proof. The "if" part follows from exercise 1.9.L. The "only if" part follows from exercise 1.9.M.

***Example* 1.9.17** (Log-linear function). Let $a_1, \ldots, a_n \in \mathbb{R}$ and define $f\colon \mathbb{R}^n_{++} \to \mathbb{R}$ by

$$f(x) = \sum_{i=1}^{n} a_i \log x_i$$

This function is commonly used in empirical work. It is not homogeneous, since for $t > 0$,

$$\begin{aligned} f(tx) &= \sum_{i=1}^{n} a_i \log(tx_i) = \sum_{i=1}^{n} a_i \log t + \sum_{i=1}^{n} a_i \log x_i \\ &= \sum_{i=1}^{n} a_i \log t + f(x) \end{aligned}$$

However, f is homothetic. Indeed, consider the Cobb–Douglas function

$$h(x) = \prod_{i=1}^{n} x_i^{a_i},$$

which is homogeneous (see example 1.9.B). Then $f(x) = \log h(x)$, and since the logarithm is strictly increasing, f is a monotonic transformation of a homogeneous function. Therefore f is homothetic.

Exercise 1.9.N. (Homothetic technology.) Let $Y \subseteq \mathbb{R}^n_+$ be a production set and let $c(w, y)$ denote the associated cost function. Suppose that the production function is homothetic.

Show that the cost function is separable in output, that is,

$$c(w, y) = \varphi(y)\, c(w, 1)$$

for some function $\varphi\colon \mathbb{R}_+ \to \mathbb{R}_+$. *Hint.* Use exercise 1.9.F.

Exercise 1.9.O. (Concavifiability.) Let X be a real vector space and let $S \subseteq X$ be a convex cone. Suppose that $f\colon S \to \mathbb{R}$ is strictly positive, definite, strictly increasing, homothetic, and quasiconcave. Show that f is concavifiable, that is, there exists a strictly increasing function $G\colon \mathrm{Im}\,(f) \to \mathbb{R}$ such that $G \circ f$ is concave.

1.10 Correspondences

1.10.1 Motivation and Definition of a Correspondence

Many of the most natural objects in economics and optimization are not functions. When we ask “what does an agent choose?”, “what is the solution to this problem?”, or “what inputs are consistent with this output?”, the honest answer is often a *set*—possibly empty, possibly containing many elements—that varies as parameters change. The theory of **correspondences** (also called set-valued maps or multifunctions) is precisely the language built to handle such objects.

Budget sets. The budget set

$$B(p, w) \;=\; \left\{ x \in \mathbb{R}^n_+ \,:\, p \cdot x \le w \right\}$$

assigns to each price–wealth pair (p, w) not a point but a whole set of affordable bundles. Demand theory studies selections from $B(p, w)$, and the existence, compactness, and continuity properties of demand descend from structural properties of this constraint correspondence.

Parameterized maximization. Given a problem $\max_{x\in\Gamma(\theta)} f(x,\theta)$, the *argmax correspondence*

$$X^*(\theta) \;=\; \arg\max_{x\in\Gamma(\theta)} f(x,\theta)$$

collects all maximizers at parameter θ. Even when f is smooth and well-behaved, $X^*(\theta)$ need not be single-valued: indifference, binding constraints, or symmetry can all produce ties. The central question is how $X^*(\theta)$ varies with the parameter θ—this is the subject of the *Maximum Theorem*.

Best responses in games. In a strategic setting, the best response of player i to a profile of opponents' strategies s_{-i} is

$$BR_i(s_{-i}) \;=\; \arg\max_{s_i} u_i(s_i, s_{-i}).$$

This is generically a correspondence. Nash equilibria are fixed points of the joint best-response correspondence $BR : S \rightrightarrows S$, and their existence follows from fixed-point theorems—Kakutani's, in particular—that apply precisely to correspondences with suitable continuity and convexity properties.

Ill-posed inverse problems. Given an operator A and an observation y, an inverse problem asks for x such that $Ax = y$. When uniqueness fails, the inverse map is not a function but a correspondence:

$$A^{-1}(y) \;=\; \{\, x \;:\; Ax = y \,\},$$

which may be empty or contain many elements. Understanding how this preimage varies with y naturally leads to the study of continuity for set-valued maps.

Optimal control. In many control problems, the feasible controls depend on the current state. Let $\Gamma(x)$ denote the set of admissible controls at state x, and let $f(x,u)$ describe the instantaneous objective or dynamics under control u. The induced correspondence

$$F(x) \;=\; f\big(x, \Gamma(x)\big) \;=\; \{\, f(x,u) \;:\; u \in \Gamma(x) \,\}$$

collects all feasible objective values (or state velocities) at x. The evolution of the system then takes the form of a differential inclusion

$$x'(t) \in F\big(x(t)\big),$$

rather than an ordinary differential equation. Even the dynamics of the system are thus governed by a correspondence.

Subgradients and supergradients. Non-smooth analysis leads naturally to set-valued derivatives. For a convex function f, the *subdifferential*

$$\partial f(x) \;=\; \{\, g \;:\; f(y) \geq f(x) + g \cdot (y - x) \;\text{ for all } y \,\}$$

is the set of all subgradients at x. At differentiable points it reduces to the singleton $\{\nabla f(x)\}$; at non-differentiable points it becomes a non-singleton convex set. An entirely symmetric construction arises for concave functions via the superdifferential.

Across all these settings a common thread emerges: we want to know whether small perturbations in parameters produce small changes in the solution set. But what does "small change" mean when outputs are sets rather than points? This requires a notion of continuity for correspondences. Two distinct concepts—*upper hemicontinuity* and *lower hemicontinuity*—formalize different ways in which solution sets can behave well under perturbation. Neither implies the other; both capture essential aspects of stability.

The unifying thread is that set-valuedness is not a pathology to be avoided but a structural feature to be analyzed. Correspondences are the right objects, and the remainder of this section develops their theory accordingly.

***Definition* 1.10.1** (Correspondence). Let X and Y be sets. A *correspondence* from X to Y is a map

$$\varphi : X \rightrightarrows Y$$

that assigns to each $x \in X$ a subset $\varphi(x) \subseteq Y$.

***Definition* 1.10.2** (Graph). Let $\varphi : X \rightrightarrows Y$. The *graph* of φ is the subset of $X \times Y$ defined by

$$\operatorname{graph}(\varphi) \;=\; \{\, (x, y) \in X \times Y \;:\; y \in \varphi(x) \,\}.$$

***Definition* 1.10.3** (Image of a set). Let $\varphi : X \rightrightarrows Y$ and let $F \subseteq X$. The *image* of F under φ is

$$\varphi(F) \;=\; \bigcup_{x \in F} \varphi(x).$$

***Definition* 1.10.4** (Domain). Let $\varphi : X \rightrightarrows Y$. The *domain* of φ is

$$\operatorname{Dom}(\varphi) \;=\; \{\, x \in X \;:\; \varphi(x) \neq \emptyset \,\}.$$

***Remark* 1.10.5**. A function $f : X \to Y$ may be identified with the correspondence $x \mapsto \{f(x)\}$.

1.10.2 Inverse Images

***Definition* 1.10.6** (Upper and lower inverse). Let $\varphi : X \rightrightarrows Y$ be a correspondence and let $E \subseteq Y$.

The *upper inverse* (or *strong inverse*) of E under φ is

$$\varphi^u [E] = \{ x \in X : \varphi(x) \subseteq E \}.$$

The *lower inverse* (or *weak inverse*) of E under φ is

$$\varphi^\ell [E] = \{ x \in X : \varphi(x) \cap E \neq \emptyset \}.$$

***Remark* 1.10.7.** Let $\varphi : X \rightrightarrows Y$ and let $y \in Y$. For any $y \in Y$, the *lower section* (or *fiber*) of φ at y is

$$\varphi^{-1} [y] = \varphi^\ell [\{y\}] .$$

***Example* 1.10.8** (Upper and lower inverse in a finite game). Consider the following two-player finite game:

	t_1	t_2	t_3	t_4
s_1	$(1,1)$	$(1,1)$	$(0,0)$	$(0,0)$
s_2	$(0,0)$	$(2,2)$	$(2,2)$	$(0,0)$
s_3	$(1,1)$	$(1,1)$	$(0,0)$	$(3,3)$

Player 2's best-response correspondence $\varphi_2 : S_1 \rightrightarrows S_2$ is given by

$$\varphi_2(s_1) = \{t_1, t_2\}, \qquad \varphi_2(s_2) = \{t_2, t_3\}, \qquad \varphi_2(s_3) = \{t_4\}.$$

Let $E = \{t_2, t_3\} \subseteq S_2$.

Inspecting the values of φ_2, we see that only $\varphi_2(s_2) = \{t_2, t_3\}$ is contained in E. Hence

$$\varphi_2^u [E] = \{s_2\}.$$

Since both $\varphi_2(s_1)$ and $\varphi_2(s_2)$ intersect E, while $\varphi_2(s_3)$ does not, we obtain

$$\varphi_2^\ell [E] = \{s_1, s_2\}.$$

Thus in this example,

$$\varphi_2^u [E] \subsetneq \varphi_2^\ell [E] .$$

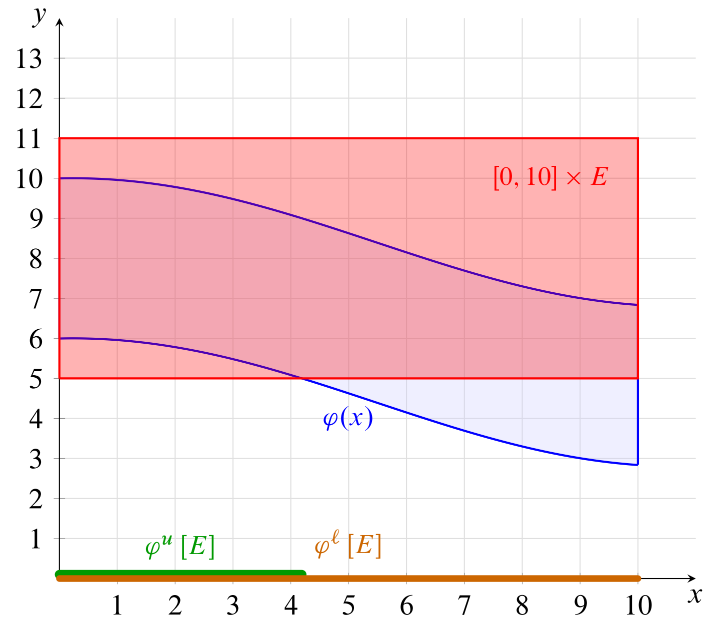


Figure 1.1: Illustration of Upper and lower inverses of graph(φ).

Example **1.10.9** (Geometric interpretation of inverse images). Let $\varphi : X \rightrightarrows Y$ and let $E \subseteq Y$. Viewing graph(φ) as a subset of $X \times Y$, the lower inverse $\varphi^\ell[E]$ consists of all $x \in X$ for which the vertical section $\{x\} \times Y$ intersects the band $X \times E$. The upper inverse $\varphi^u[E]$ consists of those x for which the entire vertical section lies inside $X \times E$. Figure 1.1 illustrates the distinction.

Remark **1.10.10**. If φ is nonempty-valued, then for every $E \subseteq Y$,

$$\varphi^u[E] \subseteq \varphi^\ell[E].$$

Indeed, if $\varphi(x) \subseteq E$ and $\varphi(x) \neq \varnothing$, then necessarily $\varphi(x) \cap E \neq \varnothing$.

If empty values are permitted, the inclusion may fail: whenever $\varphi(x) = \varnothing$, we have $\varphi(x) \subseteq E$ for every E, but $\varphi(x) \cap E = \varnothing$.

Remark **1.10.11**. For every $y \in Y$,

$$\begin{aligned}\varphi^{-1}[y] &= \varphi^\ell[\{y\}] \\ &= \{x \in X : \varphi(x) \cap \{y\} \neq \emptyset\} \\ &= \{x \in X : y \in \varphi(x)\} \supseteq \varphi^u[\{y\}]\end{aligned}$$

Remark **1.10.12**. When studying inverse images, it is often convenient to restrict attention to the domain Dom(φ), since only there are the values of φ

nonempty.

***Remark* 1.10.13.** Let $y \in \varphi(\mathrm{Dom}\,(\varphi))$. Then

$$\varphi^{-1}\,[y] = \varphi^{\ell}\,[\{y\}] = \{x \in X : y \in \varphi(x)\}.$$

Moreover, on $\mathrm{Dom}\,(\varphi)$ one has

$$\varphi^{u}\,[\{y\}] \subseteq \varphi^{-1}\,[y]\,.$$

1.11 Fixed point theorems

2 Exchange Economies

3 Production Economies

4 Core Convergence Results

5 Extensions

Appendix A

The basics of mathematical logic

> Everything is vague to a degree you do not realize till you have tried to make it precise.
>
> Bertrand Russell, *The Philosophy of Logical Atomism*

The purpose of this appendix is to recall basic elements of *mathematical logic*, understood as the language in which rigorous mathematical arguments are formulated. While this material is not a direct component of the economic theory developed in these notes, it underlies virtually every definition, theorem, and proof that follows. It is included to fix terminology, clarify logical structure, and provide a reference when precision is essential.

Mathematical logic provides a framework in which the validity of a conclusion is guaranteed, provided the initial hypotheses are correct and the deductive steps are sound. This rigor distinguishes being *convinced* of a statement from being certain of its objective validity. In advanced economic theory, many apparent difficulties arise not from economic content, but from imprecise handling of implications, quantifiers, or logical equivalence. The goal of this appendix is to eliminate such ambiguities.

In professional mathematical discourse, informal or heuristic arguments are often used to convey intuition efficiently. Such arguments can be valuable for communication, but they are not substitutes for logically rigorous proofs. Throughout these notes, results are stated and proved formally, even when the underlying ideas admit an intuitive explanation.

Logical reasoning is frequently viewed as an innate skill employed in everyday thought[1]. However, its systematic application to abstract mathematical statements requires training and careful attention to structure. Mastery of logic is not achieved through memorization of rules, but through understanding why those

[1] In practice, this capacity is unevenly developed and far from universally exercised. So my claim is best interpreted as *aspirational*.

rules hold and how they constrain valid reasoning. The material collected here is assumed in the main text and will not be revisited there.

A.1 Propositional logic

We begin by distinguishing between *expressions* and *statements*. An expression is a syntactic object: a string of symbols formed according to prescribed rules. By itself, an expression need not carry a truth value. A *statement* is an expression that can be meaningfully asserted to be either true or false. Only statements admit truth values.

For example, the string

$$2 + 3 \times 5$$

is a well-formed expression, but not a statement: it does not assert anything and therefore cannot be assigned a truth value. In contrast, the sentence

$$2 + 3 \times 5 = 17$$

is a statement, since it makes a definite assertion that can be evaluated as either true or false.

In this appendix, we restrict attention to statements whose truth value is unambiguous. Such statements are referred to as *propositions*. Propositions will be denoted by capital letters such as P, Q, and R. At this stage, propositions are treated as atomic objects: their internal structure is irrelevant, and only their truth values matter.

As an illustration, the statement "$2 + 2 = 4$" is a proposition and is true, whereas the statement "$2 + 2 = 5$" is a proposition and is false. Both are well-formed statements, even though only one of them is true.

Given propositions P and Q, new propositions may be formed using standard logical connectives. The most commonly used are negation, conjunction, disjunction, implication, and equivalence, denoted respectively by

$$\neg P, \qquad P \wedge Q, \qquad P \vee Q, \qquad P \Rightarrow Q, \qquad P \Leftrightarrow Q.$$

Each connective produces a new proposition whose truth value depends solely on the truth values of the constituent propositions.

The meaning of these connectives is fixed formally by *truth tables*, which specify the truth value of a compound proposition for every possible assignment of truth values to its components. For example, the implication $P \Rightarrow Q$ is false only when P is true and Q is false, and true in all other cases. This formal definition must be kept distinct from informal uses of "if–then" in natural language, which often carry causal or temporal interpretations absent from logical implication.

A proposition that is true for all possible truth assignments is called a *tautology*. A proposition that is false for all such assignments is called a *contradiction*. Two propositions are said to be *logically equivalent* if they take the same truth value under every possible assignment of truth values to their constituent propositions. Logical equivalence concerns identity of logical content, not similarity of linguistic expression.

Logical equivalence allows propositions to be rewritten without altering their meaning. For example, the implication $P \Rightarrow Q$ is logically equivalent to $\neg P \vee Q$, and De Morgan's laws imply

$$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q),$$
$$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q).$$

Such equivalences are used routinely, often implicitly, in mathematical arguments and proofs.

Finally, not every string of symbols is even a well-formed expression. For instance, the sequence "$\wedge PQ$" does not conform to the syntactic rules of propositional logic and is therefore ill-formed. As such, it is neither an expression with semantic content nor a statement to which a truth value could be assigned.

A.2 Logical implication and equivalence

Logical implication is a central construct in mathematical reasoning. Given two propositions P and Q, the implication $P \Rightarrow Q$ is itself a proposition whose truth value is determined by the truth values of P and Q. Formally, $P \Rightarrow Q$ is false only in the case where P is true and Q is false, and true in all other cases.

It is essential to distinguish this formal notion of implication from informal uses of "if–then" in natural language. In everyday discourse, conditional statements often suggest causality, explanation, or temporal ordering. None of these interpretations are part of the logical implication. The statement $P \Rightarrow Q$ asserts only that the joint truth of P and falsity of Q is ruled out; it makes no claim about why Q holds when it does.

Logical implication is commonly described using the language of necessary and sufficient conditions. The statement "P is sufficient for Q" means that $P \Rightarrow Q$ holds. Equivalently, "Q is necessary for P" also means that $P \Rightarrow Q$ holds. These two formulations express the same logical relationship, but from opposite perspectives. Confusing necessity with sufficiency is a frequent source of error in mathematical and economic arguments.

Associated with any implication $P \Rightarrow Q$ are three related statements. The *converse* is $Q \Rightarrow P$. The *inverse* is $\neg P \Rightarrow \neg Q$. The *contrapositive* is $\neg Q \Rightarrow \neg P$. Among these, only the contrapositive is logically equivalent to the original implication. That is, $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ always have the same truth value. Neither the converse nor the inverse is, in general, equivalent to $P \Rightarrow Q$.

As an illustration, consider the statement "If a figure is a square, then it is a rectangle." This is a true implication. Its contrapositive, "If a figure is not a rectangle, then it is not a square," is also true. By contrast, the converse "If a figure is a rectangle, then it is a square" is false, since a rectangle need not have equal sides. Similarly, the inverse "If a figure is not a square, then it is not a rectangle" is false.

An implication is said to hold in both directions when $P \Rightarrow Q$ and $Q \Rightarrow P$ are both true. In this case, P and Q are *logically equivalent*, and the equivalence is denoted by $P \Leftrightarrow Q$. Logical equivalence asserts that the two propositions have identical truth values under all possible truth assignments. In mathematical writing, equivalence is used deliberately, particularly in definitions, where a concept is characterized by a collection of conditions that are jointly necessary and sufficient.

A.3 Quantifiers

Before introducing quantifiers, it is useful to clarify the role of variables. A *variable* is a symbol that serves as a placeholder for an object drawn from a specified domain. An expression containing a variable does not, by itself, assert anything definite, since its truth value depends on how the variable is instantiated. Such indeterminacy may be resolved either by fixing a specific value for the variable, or by using quantifiers to specify how the variable is to be interpreted within a statement.

The two fundamental quantifiers are the universal quantifier, denoted by $\forall$, and the existential quantifier, denoted by $\exists$.

A quantified expression becomes a *statement* only once all variables appearing in it are *bound* by quantifiers. An expression containing free variables does not have a truth value and therefore does not constitute a proposition. This distinction mirrors the earlier separation between expressions and statements in propositional logic.

The universal quantifier $\forall x$ is read as "for all x," and asserts that a given statement holds for every admissible value of x in the relevant domain. The existential quantifier $\exists x$ is read as "there exists an x," and asserts that the statement holds for at least one admissible value of x. In both cases, the quantifier applies to a statement and binds the variable x within its scope.

Quantifiers, like logical connectives, have scope. The scope of a quantifier determines the part of the expression to which it applies. Ambiguity in scope leads to ambiguity in meaning, and must be avoided. Parentheses are often used to make scope explicit, particularly in statements involving multiple quantifiers or logical connectives.

In many contexts, variables appear as arguments of a *property*. A property is a rule that associates to each admissible tuple of values a truth value. For instance, $P(x)$ denotes a property of a single variable, while $P(x, y)$ denotes a property of two variables. Such expressions are not statements until the variables are either assigned specific values or bound by quantifiers.

When multiple quantifiers appear in a statement, their order matters. In general, the statements

$$\forall x\, \exists y\; P(x, y) \qquad \text{and} \qquad \exists y\, \forall x\; P(x, y)$$

are not logically equivalent. The first asserts that for each admissible value of x there exists a corresponding value of y (possibly depending on x) such that $P(x, y)$ holds. The second asserts the existence of a single value of y that works simultaneously for all admissible values of x. Interchanging the order of quantifiers changes the logical content of the statement.

As an illustration, consider the statements "For every real number x there exists a real number y such that $y > x$," and "There exists a real number y such that for every real number x, $y > x$." The first statement is true, while the second is false. The difference lies entirely in the order of the quantifiers.

Negation interacts with quantifiers in a systematic way. The negation of a universally quantified statement is an existentially quantified negation, and vice versa. Formally,

$$\neg\big(\forall x\; P(x)\big) \;\Leftrightarrow\; \exists x\, \neg P(x), \qquad \neg\big(\exists x\; P(x)\big) \;\Leftrightarrow\; \forall x\, \neg P(x).$$

These equivalences express that asserting the failure of a universal claim amounts to exhibiting a counterexample, while denying the existence of an object requires showing that no admissible value satisfies the stated property.

Careful attention to quantifiers and their scope is essential in reading and writing mathematical arguments. Many errors in advanced economic theory arise not from incorrect economic reasoning, but from misinterpreting the logical structure of quantified statements.

A.4 Statements Involving Quantifiers

Building on the basic notions introduced in the previous subsection, we now examine in more detail the logical structure of statements involving quantifiers. The focus here is not on introducing new concepts, but on correctly reading and interpreting quantified statements as they appear in mathematical arguments.

Quantified statements arise when properties are combined with quantifiers to form propositions. Such statements are ubiquitous in mathematical writing, and their correct interpretation depends critically on the placement, scope, and order of the quantifiers involved.

A common source of confusion is the informal reading of quantified statements expressed in natural language. Phrases such as "for every," "there exists," "for some," or "for all" often admit multiple interpretations unless the logical structure is made explicit. Mathematical notation serves precisely to remove this ambiguity, but only if it is read with care.

Consider a statement of the form

$$\forall x\ P(x).$$

This asserts that the property P holds for every admissible value of x. By contrast, the statement

$$\exists x\ P(x)$$

asserts that there is at least one admissible value of x for which P holds. Although the two statements may appear similar linguistically, they make fundamentally different claims.

More complex statements involve multiple quantifiers. For example,

$$\forall x\, \exists y\ P(x, y)$$

asserts that for each admissible value of x there exists a (possibly different) value of y such that $P(x, y)$ holds. In contrast,

$$\exists y\ \forall x\ P(x, y)$$

asserts the existence of a single value of y that works simultaneously for all admissible values of x. Interchanging the order of quantifiers changes the content of the statement and, in general, the two forms are not equivalent.

The scope of quantifiers must be read carefully; parentheses are used to delimit the part of the expression to which a quantifier applies. For instance, the statements

$$\forall x\ \big(P(x) \Rightarrow Q(x)\big) \qquad \text{and} \qquad \big(\forall x\ P(x)\big) \Rightarrow \big(\forall x\ Q(x)\big)$$

are not logically equivalent. The first is a *stronger* claim, asserting that the implication $P(x) \Rightarrow Q(x)$ holds for every admissible value of x. The second is a *weaker* claim, asserting only that the universal truth of P implies the universal truth of Q.

To illustrate the distinction, consider a domain consisting of two individuals, *Akbobek* and *Balzhan*. Let $P(x)$ be the property "x is an economist" and $Q(x)$ be "x is a theorist." Suppose that Akbobek is an economist but not a theorist, and Balzhan is not an economist.

- The first statement is *false*, as the implication $P(\text{Akbobek}) \Rightarrow Q(\text{Akbobek})$ fails.

- The second statement is *true*. Since Balzhan is not an economist, the antecedent $\forall x\, P(x)$ ("everyone is an economist") is false. In classical logic, an implication with a false antecedent is vacuously true.

Similarly, care must be taken when distributing the existential quantifier over an implication. The statements

$$\exists x \left(P(x) \Rightarrow Q(x)\right) \qquad \text{and} \qquad \left(\exists x\, P(x)\right) \Rightarrow \left(\exists x\, Q(x)\right)$$

are logically distinct. The second statement is *stronger* than the first. It asserts that if there is at least one individual with property P, then there must be at least one (potentially different) individual with property Q. The first statement is surprisingly *weak*; in classical logic, $\exists x(P(x) \Rightarrow Q(x))$ is true if there is any x that is not P, or any x that is Q.

To illustrate, consider again our domain of *Akbobek* and *Balzhan*. Let $P(x)$ be "x is an economist" and $Q(x)$ be "x is a theorist." Suppose Akbobek is an economist and Balzhan is not an economist. Furthermore, suppose neither of them is a theorist.

- The first statement is *true*. We only need to find one x such that $P(x) \Rightarrow Q(x)$ holds. For Balzhan, the antecedent $P(\text{Balzhan})$ is false, making the implication $P(\text{Balzhan}) \Rightarrow Q(\text{Balzhan})$ true.

- The second statement is *false*. The antecedent $\exists x P(x)$ is true (Akbobek is an economist), but the consequent $\exists x Q(x)$ is false (neither is a theorist). Thus, the overall implication $\mathrm{T} \Rightarrow \mathrm{F}$ is false.

Negation of quantified statements must also be handled with care. As discussed in the previous section, negation reverses the type of quantifier and moves the negation operator inside the scope:

$$\neg(\forall x\, P(x)) \iff \exists x\,(\neg P(x)) \qquad \text{and} \qquad \neg(\exists x\, P(x)) \iff \forall x\,(\neg P(x)).$$

Thus, denying a universally quantified statement amounts to asserting the existence of a counterexample, while denying an existential statement amounts to asserting that no admissible value satisfies the stated property. Failure to apply these transformations correctly is a frequent source of logical error.

When reading or writing mathematical arguments, it is often useful to restate quantified statements informally in several equivalent ways, while keeping the logical structure fixed. Doing so helps ensure that the intended meaning has been captured correctly. Throughout these notes, statements involving quantifiers will be written precisely, and their logical form should always be identified before attempting to interpret or manipulate them.

A.5 Methods of proof

Mathematical proofs are structured arguments that establish the truth of a statement by logical deduction from stated assumptions. Although proofs may vary widely in style and length, most arguments encountered in these notes rely on a small number of standard proof methods. These methods differ in form, but all are grounded in the logical principles discussed in the preceding sections.

Direct proof. A direct proof of an implication $P \Rightarrow Q$ proceeds by assuming that P holds and then deducing, through a sequence of logically valid steps, that Q must also hold. This is the most common proof technique in mathematics. When a statement is universally quantified, a direct proof typically begins by fixing an arbitrary admissible element and showing that the claimed property holds for that element.

Proof by contrapositive. Instead of proving $P \Rightarrow Q$ directly, one may prove its contrapositive $\neg Q \Rightarrow \neg P$. Since an implication is logically equivalent to its contrapositive, establishing either suffices. This method is often preferable when the negation of the conclusion has a simpler or more tractable structure than the original assumption.

Proof by contradiction. A proof by contradiction establishes a statement by assuming that it is false and deriving a logical contradiction. For an implication $P \Rightarrow Q$, this typically amounts to assuming that P holds while Q fails, and then showing that this leads to an impossibility. The validity of this method rests on classical logic, in which a statement cannot be both true and false.

Existence proofs. Statements asserting the existence of an object may be proved in different ways. A *constructive* existence proof explicitly exhibits an object satisfying the required properties. A *non-constructive* existence proof establishes existence indirectly, for example by showing that the non-existence of such an object would contradict known facts. Both forms of proof are logically valid, though they differ in informational content.

Uniqueness proofs. To prove that an object satisfying a given property is unique, one must show that any two objects with that property coincide. Typically, this is done by assuming the existence of two such objects and demonstrating that they must be equal. Uniqueness proofs often accompany existence results, but they are logically distinct and require separate arguments.

Proofs involving quantified statements. Many proofs involve statements with multiple quantifiers. In such cases, careful attention must be paid to the order of quantification. For instance, proving a statement of the form $\forall x\, \exists y\ P(x, y)$ requires showing that for each admissible value of x one can identify a corresponding value of y satisfying P. By contrast, a statement of the form $\exists y\, \forall x\ P(x, y)$ requires the identification of a single value of y that works uniformly for all admissible values of x. Confusing these two tasks leads to incorrect arguments.

Throughout these notes, proofs will be written in a style that emphasizes logical structure and clarity. When reading a proof, it is often helpful to identify explicitly the assumptions being made, the logical form of the statement being proved, and the proof method being employed.

A.6 Logical structure of definitions, theorems, and other mathematical results

Logical structure plays a central role in the way mathematical results are stated and interpreted. Definitions, theorems, and other results are distinguished not by their subject matter, but by their underlying logical form. Failure to distinguish among them leads to systematic misreadings of mathematical arguments, particularly in economic theory.

Definitions. A mathematical definition introduces a concept by stipulating an equivalence. Typically, a definition has the logical form

$$\text{Object } x \text{ satisfies Property } P \iff \text{Conditions } A(x), B(x), \ldots \text{ hold.}$$

Both directions of the biconditional are part of the definition itself. Note that in mathematical practice, definitions are often written using the word "if" (e.g., "A function is continuous if…"), though the logical meaning is always a biconditional. Neither direction is a theorem, and neither requires proof. Definitions fix terminology by decree: once adopted, the equivalence is taken as given throughout the development of the discussion.

Theorems. In contrast, a theorem usually asserts an implication. A theorem has the logical form

$$\text{Assumptions} \;\Rightarrow\; \text{Conclusion.}$$

The assumptions are sufficient for the conclusion, but are not necessarily claimed to be necessary. The theorem does not assert that the conclusion fails when the assumptions are violated, nor that the assumptions are minimal. Reading a theorem as a biconditional, or assuming its converse holds, is a logical error unless explicitly justified.

Characterizations. In economics, the term *characterization* is used to describe a result that establishes a biconditional by proof. A characterization shows that an object satisfies certain properties *if and only if* a given set of conditions holds. Logically, a characterization consists of two implications:

- *Necessity*: if the object satisfies the stated properties, then the conditions must hold.
- *Sufficiency*: if the conditions hold, then the object satisfies the stated properties.

Unlike a definition, a characterization is not stipulated; both directions must be proved. Characterizations are ubiquitous in economic theory, for example in the analysis of equilibria, optimality conditions, and incentive compatibility.

Necessary and sufficient conditions. The distinction between necessity and sufficiency is essential when reading mathematical results. A theorem may establish that certain conditions are sufficient for a conclusion, without claiming that they are necessary. In the context of economic optimization, for instance, a first-order condition may be necessary for a maximum, but it is not sufficient without additional assumptions like concavity. A characterization, by contrast, establishes both necessity and sufficiency. Careful attention must be paid to which direction has been proved, and which has not.

Logical equivalence and reduction arguments. Arguments introduced with phrases such as "without loss of generality" rely on logical equivalence or symmetry. Such arguments reduce the analysis to representative cases without excluding any relevant possibilities. The validity of a reduction must be justified; "without loss of generality" is not a license to discard cases arbitrarily.

Common logical misreadings. Typical logical errors include treating characterizations as definitions, assuming converses of theorems without proof, confusing existence with uniqueness, and misidentifying sufficient conditions as necessary ones. Avoiding these mistakes requires careful attention to the logical form of each statement, not merely to its mathematical content.

Exercise A.6.A. Negate the following statements:

a) Every prime number such that, if you divide it by 4, you obtain a remainder of 1, is the sum of two squares.

b) For all $x \in \mathbb{R}$ and for all $\varepsilon > 0$, there exists $\delta > 0$ such that for all $y \in \mathbb{R}$, if $|y - x| < \delta$, then $|y^2 - x^2| < \varepsilon$.

c) For all $\varepsilon > 0$, there exists $\delta > 0$ such that for all $x, y \in \mathbb{R}$, if $|y - x| < \delta$, then $|y^2 - x^2| < \varepsilon$.

Exercise A.6.B. Explain why one of the following statements is true and the other is false:

$$(\forall \text{ man } M)(\exists \text{ woman } W)\ \big(W \text{ is the mother of } M\big)$$

$$(\exists \text{ woman } W)(\forall \text{ man } M)\ \big(W \text{ is the mother of } M\big)$$

Appendix B

Sets and Functions

A set is a Many that allows itself to be thought of as a One.

GEORG CANTOR, *Gesammelte Abhandlungen*, pp. 378–439

B.1 Naive Set Theory

The formal definition of a *set* is rather technical and delicate. Starting from our intuitive definition of a set, the great thinkers of Mathematics and Logic have constructed an entire theoretical edifice which, although necessary to provide solid foundations for mathematics, is full of logical-philosophical conflicts, which we shall not concern ourselves in these notes. For a more detailed introduction to set theory, the interested reader may consult Fraenkel (1966) or consult the classic reference Cantor (1955).

For our purposes, it will suffice for the reader to use the notion of a set that we all carry intuitively engraved in our minds: a collection of objects, perhaps defined by some property. The notation for sets that we will use is the canonical one: uppercase letters to indicate sets, and if the set is defined by some property, say $P(x)$, the notation will be: $\{x : P(x)\}$, or $\{x \mid P(x)\}$ (read as the set of x's such that $P(x)$).

We will call the objects that constitute a set elements of the set, and the membership relation is denoted in the usual way: if A is a set and x is an element of A, we will write $x \in A$. Similarly, if x is not an element of the set A, we will write $x \notin A$. A very important set is the set without elements, called the empty set, which will be denoted by $\emptyset$.

Let us look at some examples of sets:

a) The set of poker suits $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$.

b) The set of natural numbers $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.

c) The set of integers $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$.

d) The set of prime numbers

$$\{p \in \mathbb{N} : p \text{ is a prime number}\} = \{2, 3, 5, 7, 11, 13, \ldots\}.$$

The membership relation allows us to compare sets: if A and B are sets, we say that A is a *subset* of B if every element of the set A is an element of the set B. Note, for example, that every set is a subset of itself and that the empty set is a subset of any set. The symbol $\subseteq$ will be used to denote the containment relation: $A \subseteq B$ is read as A is a subset of B (or, equivalently, B contains A).

The negation: A is not contained in B (what does this mean?) will be denoted by $A \nsubseteq B$, and when A is contained in B but there exist elements of B that are not in A (i.e. A is a proper subset of B), we write $A \subseteq B$.

By being able to compare sets via containment, we obtain a way to decide whether two sets are equal or not:

Definition **B.1.1**. If A and B are sets, we say that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Observe that, in particular, Definition B.1.1 shows that there is a unique empty set. Another interesting example of a set is the following.

Definition **B.1.2**. If X is a set, we define the *power set* of X, denoted by 2^X as

$$2^X = \{\, A : A \text{ is a set and } A \subseteq X \,\}.$$

For example, if X is a set with three elements, say $X = \{a, b, c\}$, then

$$2^X = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Definition **B.1.3** (Basic set operations). Let X be a set and let A and B be subsets of X. Then we define:

a) $A \cap B = \{\, x \in X : x \in A \text{ and } x \in B \,\}$ (*intersection of A and B*).

b) $A \cup B = \{\, x \in X : x \in A \text{ or } x \in B \,\}$ (*union of A and B*).

c) $A \setminus B = \{\, x \in X : x \in A \text{ and } x \notin B \,\}$ (*complement of B in A*).

d) $X \setminus A = \{\, x \in X : x \notin A \,\}$ (*complement of A*).

e) $A \triangle B = (A \setminus B) \cup (B \setminus A)$ (*symmetric difference of A and B*).

When it is clear from the context which set is the universal set X, the set $X \setminus A$ is denoted by A^c. Some simple properties of set operations are listed in the following proposition; their verification is left to the reader as a good exercise in working with Definition B.1.1. In some cases it is useful to give a graphical representation using the well-known Venn diagrams[1], which the reader is surely already familiar with.

Proposition B.1.4. *Let X be a set and let A, B, C be subsets of X. Then:*

a) $A \cup A = A$, $A \cap A = A$ *(*idempotence*).*

b) $A \cup B = B \cup A$, $A \cap B = B \cap A$ *(*commutativity*).*

c) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$ *(*associativity*).*

d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(*distributivity*).*

e) $A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

f) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$, $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$ *(*De Morgan's laws[2]*).*

De Morgan's laws can also be written in a more compact form as

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c.$$

Exercise B.1.A.🐾 Prove Proposition B.1.4.

Exercise B.1.B. Let E be a set, with subsets $A \subseteq E$ and $B \subseteq E$, and let $*$ be the operation

$$A * B = (E \setminus A) \cap (E \setminus B).$$

Express the sets: $A \cup B$, $A \cap B$, $E \setminus A$, using A, B, and $*$.

Set operations can be extended to arbitrary families of sets. If J denotes an index set and $\{A_j : j \in J\}$ is a family of subsets of a set X (intuitively, we think of having at most as many sets A_j as there are elements in the index set J), then

$$\bigcup_{j \in J} A_j = \{x \in X : x \in A_j \text{ for some } j \in J\},$$

[1] John Venn, 1834–1923.
[2] Augustus De Morgan, 1806–1871.

$$\bigcap_{j \in J} A_j = \{ x \in X : x \in A_j \text{ for every } j \in J \}.$$

Using logical quantifiers, whose traditional notation is ∀ and ∃, the union and intersection operations can be written as follows:

$$\bigcup_{j \in J} A_j = \{ x \in X : (\exists j \in J)\ x \in A_j \},$$

$$\bigcap_{j \in J} A_j = \{ x \in X : (\forall j \in J)\ x \in A_j \}.$$

We conclude this section with one more set operation, the *Cartesian product*:

Definition **B.1.5**. If A and B are sets, the Cartesian product of A and B, $A \times B$, is the set of ordered pairs

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

where each ordered pair (a, b) is in turn defined as the set $\{\{a\}, \{a, b\}\}$.

The set-theoretic definition of ordered pairs given above allows us, among other things, to show that two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$. Some useful properties of the Cartesian product related to the basic operations on sets are listed in the exercises.

Exercise B.1.C. If A and B are arbitrary sets, prove that

a) $A \cap B = A \setminus (A \setminus B)$.

b) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Exercise B.1.D. Prove that $A \subseteq B$ if and only if $A \cap B^c = \varnothing$.

Exercise B.1.E. Let X be an arbitrary set and let $\mathcal{J}$ be an index set. If A_j is a subset of X for each $j \in \mathcal{J}$, prove that

$$X \setminus \left(\bigcap_{j \in \mathcal{J}} A_j \right) = \bigcup_{j \in \mathcal{J}} (X \setminus A_j),$$

and

$$X \setminus \left(\bigcup_{j \in \mathcal{J}} A_j \right) = \bigcap_{j \in \mathcal{J}} (X \setminus A_j).$$

Exercise B.1.F. If B_1 and B_2 are subsets of B such that $B = B_1 \cup B_2$, verify that

$$A \times B = (A \times B_1) \cup (A \times B_2).$$

B.2 Functions

Without a doubt, one of the most important notions in Mathematics, and more generally in human thought, is the concept of a *function*. The same intuitive definition, as a rule of correspondence between two sets, say A and B, which assigns to each element of the set A one and only one element of the set B, immediately provides an innumerable list of examples.

The formal definition of a function is as follows:

Definition B.2.1. A subset $f \subseteq A \times B$ is a function if whenever $(a, b) \in f$ and $(a, b') \in f$, then $b = b'$. Alternatively, we say that f is a function from A to B if f is a rule of correspondence that assigns to each element of A one and only one element of B.

We shall use the usual notation and terminology for functions. The expression $f : A \to B$ will denote the function f from A to B. Traditionally, the element of B associated by f to an element a is denoted by $f(a)$. The function f is called the *rule of correspondence* of the function, while A and B are called the *domain* and the *codomain* of the function, respectively. Note that, *a fortiori*, for each $a \in A$ there must exist an element $f(a)$, whereas if $b \in B$, then b is not necessarily of the form $f(a)$ for some $a \in A$.

We now proceed to give some examples of functions.

Example B.2.2. Let $f : \{a, b, c\} \to \{a, b, c\}$ be defined by $f(a) = a$, $f(b) = c$, $f(c) = c$. Although the domain is a rather simple set, f is a function. On the other hand, let $g : \{a, b, c\} \to \{a, b, c\}$ be defined by $g(a) = a$, $g(a) = b$, $g(b) = c$, $g(c) = b$. Then g is not a function, since two elements of the codomain are associated to the element a.

Example B.2.3. If A and B are sets and $b_0 \in B$, the function $f : A \to B$ defined by $f(a) = b_0$ for every $a \in A$ is a function, called the *constant function*.

Example B.2.4. If A is a set, let $\mathrm{id}_A : A \to A$ be defined by $\mathrm{id}_A(a) = a$ for every $a \in A$. We obtain the so-called *identity function* on A.

Example B.2.5. The function $f : A \to 2^A$ defined by $f(a) = \{a\}$ is a function.

Certainly, the functions encountered in your calculus courses (polynomials, trigonometric functions, logarithms, exponentials, etc.) are examples of functions: real-valued functions of a real variable. These functions constitute the main object of study in Analysis.

Definition B.2.6. Let $f : A \to B$ be a function.

a) The subset of B defined by

$$\mathrm{Im}\,(f) = \{\, b \in B : b = f(a) \text{ for some } a \in A \,\}$$

is called the *image* of A under f, or simply the *range* of f. If $C \subseteq A$, then

$$f(C) = \{ f(c) : c \in C \}$$

is called the *image* of C under f.

b) Let $D \subseteq B$. The subset of A defined by

$$f^{-1}[D] = \{a \in A : f(a) \in D\}$$

is called the *inverse image* of D under f. If B is a singleton, i.e., $B = \{b\}$, then we denote the inverse image of b as $f^{-1}[b]$.

The definition of image is illustrated in figure B.1.

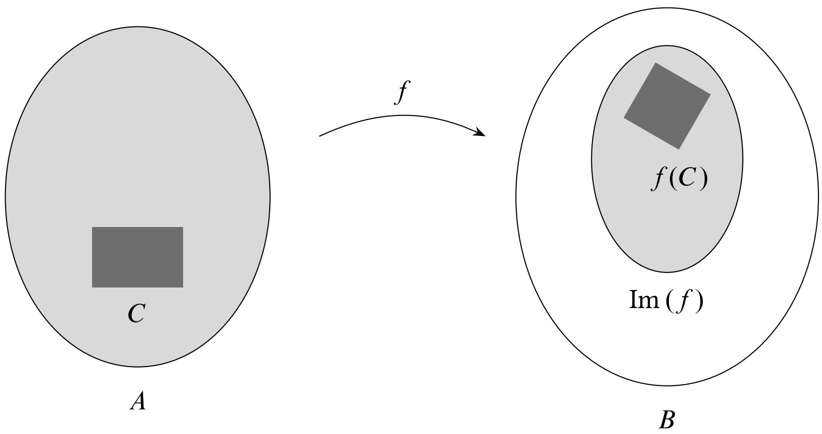


Figure B.1: Given a function $f : A \to B$, the range or image $\operatorname{Im}(f)$ does not need to be equal to the codomain. For any $C \subseteq A$, we have that the image of C under f is contained in $\operatorname{Im}(f)$.

Example **B.2.7.** Let $f : [-1, 1] \to \mathbb{R}$ be the function defined by $f(x) = x^2$. Then the range of f is

$$f([-1, 1]) = f([0, 1]) = [0, 1].$$

Moreover,

$$f^{-1}[\{1/4\}] = \{-1/2,\ 1/2\}, \qquad f^{-1}[\{0\}] = \{0\}, \qquad f^{-1}[(-\infty, -1)] = \varnothing.$$

Example **B.2.8.** Let $g : \mathbb{R} \to \mathbb{R}^2$ be defined by

$$g(t) = (\cos t, \sin t).$$

Then

$$\operatorname{Im}(g) = \{ (\cos t, \sin t) \in \mathbb{R}^2 : t \in \mathbb{R} \}.$$

Geometrically, this set is the circle of radius 1 in $\mathbb{R}^2$.

Example **B.2.9.** In the previous example,

$$g^{-1}[(0,1)] = \{\pi/2 + 2n\pi : n \in \mathbb{Z}\}.$$

If S is the upper arc of the circle joining the points $(1,0)$ and $(-1,0)$, then

$$g^{-1}[S] = \cdots \cup [-3\pi, -4\pi] \cup [-\pi, -2\pi] \cup [0, \pi] \cup [2\pi, 3\pi] \cup \cdots .$$

Definition **B.2.10.** Let $f : A \to B$ be a function. We say that

a) f is *injective*, or *one-to-one*, if whenever $a, a' \in A$ satisfy $a \neq a'$, then $f(a) \neq f(a')$; that is, distinct points in the domain A are mapped by f to distinct points in the codomain B.

b) f is *surjective*, or *onto*, if $\operatorname{Im}(f) = B$. Equivalently, for every $b \in B$ there exists $a \in A$ such that $f(a) = b$.

c) f is *bijective* if it is injective and surjective.

d) If $f : A \to B$ and $g : B \to C$ are functions, then the composition of f followed by g is the function $g \circ f : A \to C$ defined by

$$(g \circ f)(a) = g\big(f(a)\big).$$

Recall that the identity function on a set A is the function $\mathrm{id}_A : A \to A$ such that $\mathrm{id}_A(x) = x$. We have the following proposition, stated without proof.

Proposition B.2.11. *Let $f : A \to B$ be a bijective function. Then there exists a unique function $g : B \to A$ such that*

a) $f \circ g = \mathrm{id}_B$,

b) $g \circ f = \mathrm{id}_A$.

This function is called the inverse function *of f and is denoted by $f^{-1} = g$.*

Now that we have discussed the notion of function, we can present an alternative definition of the *Cartesian Product* over an arbitrary number of sets.

Definition **B.2.12.** Let $\{A_i\}_{i \in \mathcal{I}}$ be a family of sets indexed by a set $\mathcal{I}$. The *Cartesian product* of the family $\{A_i\}_{i \in \mathcal{I}}$ is the set

$$\bigtimes_{i \in \mathcal{I}} X_i = \left\{ f : \mathcal{I} \to \bigcup_{i \in \mathcal{I}} A_i \;\middle|\; f(i) \in A_i \text{ for every } i \in \mathcal{I} \right\}.$$

Definition **B.2.13.** Let $\{A_i\}_{i\in\mathcal{I}}$ be a family of sets. For each $i \in \mathcal{I}$, the *projection* onto A_i is the function

$$\pi_i : \bigtimes_{j\in\mathcal{I}} A_j \to A_i$$

defined by

$$\pi_i(a) = a(i).$$

Remark **B.2.14.** The index set $\mathcal{I}$ in Definition B.2.12 is completely arbitrary. In particular, if all the indexed sets coincide with a single set Y, that is, if $A_i = Y$ for every $i \in X$, then the Cartesian product

$$\bigtimes_{i\in X} Y$$

can be naturally identified with the set of all functions from X to Y.

Definition **B.2.15.** Let X and Y be sets. We define

$$Y^X := \{ f\colon X \to Y \},$$

the set of all functions from X to Y.

We now define a few important sets and terminology.

Definition **B.2.16.** The *graph* of a function $f : A \to B$ is the set

$$\operatorname{graph}(f) = \{(x, y) \in A \times B : y = f(x)\}.$$

In practice, we find that most common functions in economics are those which measure things, such as output, utility, or profit for example. To distinguish this common case, functions whose values are real numbers have a special name.

Definition **B.2.17.** A real-valued function $f : A \to \mathbb{R}$ is called a *functional.*

Analogously to the graph of a function in B.2.16, we can now define some important sets for functionals.

Definition **B.2.18.** The *epigraph* of a function $f : A \to \mathbb{R}$ is the set

$$\operatorname{epi}(f) = \{(x, y) \in A \times \mathbb{R} : y \geq f(x)\}$$

Definition **B.2.19.** The *hypograph* of a function $f : A \to \mathbb{R}$ is the set

$$\operatorname{hypo}(f) = \{(x, y) \in A \times \mathbb{R} : y \leq f(x)\}$$

Definition **B.2.20.** Let $f\colon A \to \mathbb{R}$ and let $c \in \mathbb{R}$. The *upper contour set* of f at level c is the set

$$U_f(c) = \{x \in A : f(x) \geq c\}.$$

***Definition* B.2.21.** Let $f\colon A \to \mathbb{R}$ and let $c \in \mathbb{R}$. The *lower contour set* of f at level c is the set

$$L_f(c) = \{x \in A : f(x) \leq c\}.$$

Exercise B.2.A. Determine whether the following statements are true or false (give a counterexample or a proof, as appropriate, to justify your answers). In each case, let A and B be subsets of the domain of f.

a) $f(A \cap B) = f(A) \cap f(B)$.

b) $f(A \setminus B) = f(A) \setminus f(B)$.

c) $f(A \cup B) = f(A) \cup f(B)$.

d) $f(A \triangle B) = f(A) \triangle f(B)$.

e) There exists a function g such that $(g \circ f)(x) = x$ for all $x \in \mathrm{Dom}\,(f)$ if and only if f is injective.

Exercise B.2.B.🐾 Let $f : X \to Y$. Prove the following properties of the inverse image.

a) If $A \subseteq Y$, then $f^{-1}[A^c] = (f^{-1}[A])^c$.

b) Let $D \subseteq Y$. Then $f^{-1}[D] = \varnothing$ if and only if $D \cap \mathrm{Im}\,(f) = \emptyset$.

c) Let $D \subseteq Y$. Then $f^{-1}[D] = X$ if and only if $\mathrm{Im}\,(f) \subseteq D$.

Exercise B.2.C.🐾 Let $f : X \to Y$ be a function and let $\mathcal{J}$ be an index set. If $A_j \subseteq Y$ for each $j \in \mathcal{J}$, prove that

$$f^{-1}\left[\bigcup_{j \in \mathcal{J}} A_j\right] = \bigcup_{j \in \mathcal{J}} f^{-1}[A_j],$$

and

$$f^{-1}\left[\bigcap_{j \in \mathcal{J}} A_j\right] = \bigcap_{j \in \mathcal{J}} f^{-1}[A_j].$$

Exercise B.2.D. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 1$. Let $\mathcal{J} = (0, \infty)$, and for each $j \in \mathcal{J}$ define $A_j = [0, j)$.

a) Compute $f^{-1}\left[A_j\right]$ for each $j \in \mathcal{J}$.

b) Find $\bigcap_{j\in\mathcal{J}} A_j$ and $\bigcap_{j\in\mathcal{J}} f^{-1}\left[A_j\right]$.

c) Verify that

$$f^{-1}\left[\bigcap_{j\in\mathcal{J}} A_j\right] = \bigcap_{j\in\mathcal{J}} f^{-1}\left[A_j\right].$$

Exercise B.2.E. Compute $f^{-1}[0]$ for $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(t) = t^6 - 14t^4 + 49t^2 - 36,$$

and compute $T^{-1}[0]$ for $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T(x, y) = \tfrac{1}{\sqrt{2}}(x + y,\, x + y).$$

Exercise B.2.F. Let $f : X \to Y$ be an injective function and let $A \subseteq X$. Show that $f^{-1}[f(A)] = A$. Also prove that if f is surjective and $B \subseteq Y$, then $f(f^{-1}[B]) = B$. Are these statements still true if the hypotheses of injectivity and surjectivity are omitted, respectively?

Exercise B.2.G.🐾 Prove that the identity function and the inverse function (defined in Proposition B.2.11) are bijective.

Exercise B.2.H. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function defined by

$$f(m, n) = 2^{m-1}(2n - 1).$$

Prove that f is bijective. Describe the following sets:

$$f^{-1}[2\mathbb{N}], \qquad f^{-1}[2\mathbb{N} - 1], \qquad f^{-1}[7\mathbb{N}].$$

Appendix C

The Natural Numbers, Integers, Rationals & Field Axioms

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
(God made the integers, all the rest is the work of man.)

Leopold Kronecker

C.1 The Natural Numbers

Perhaps the set of numbers with which we are most familiar is the set of *natural numbers*,

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, \dots\}.$$

After all, this is the set of numbers we use for counting. The natural numbers are defined axiomatically via the so-called *Peano axioms*[1]. We will not present the Peano axiomatization in detail here, and we will simply assume, without further justification, that we have an addition operation $(+)$ defined on the natural numbers, as well as the usual order relation $(<)$. However, one of the Peano axioms that we must consider is the well-known *Principle of Mathematical Induction.*

The reader surely had the opportunity to "do proofs by induction" before and will recall that this is the argument used *par excellence* when one wishes to prove that a certain formula or property holds for all natural numbers. The statement of the axiom (or principle) of induction is as follows.

Axiom **C.1.1** (First Principle of Induction). Let $S \subseteq \mathbb{N}$ be such that:

(a) $1 \in S$,

(b) if $k \in S$, then $k + 1 \in S$.

[1] Giuseppe Peano, 1858–1932.

Then $S = \mathbb{N}$.

Example C.1.2. The classical example illustrating the use of the principle of induction is Gauss' formula[2] for computing the sum of the first m natural numbers:

$$1 + 2 + 3 + \cdots + m - 1 + m = \frac{m(m+1)}{2}.$$

Proof. Indeed, let

$$S = \left\{ m \in \mathbb{N} : 1 + 2 + \cdots + m = \frac{m(m+1)}{2} \right\}.$$

Clearly $1 \in S$, since $1 = \frac{1(2)}{2}$. Suppose now that $k \in S$, that is,

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

We must show that $k + 1 \in S$. But

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Thus, $k + 1 \in S$, and therefore $S = \mathbb{N}$. ^. .^)9

It is not always necessary to prove a property of the natural numbers by induction: Gauss' formula can also be proved by writing

$$T = 1 + 2 + \cdots + n,$$

$$T = n + (n-1) + \cdots + 1,$$

and adding term by term, we obtain n summands equal to $n + 1$. That is,

$$2T = \underbrace{(n+1) + (n+1) + \cdots + (n+1)}_{n \text{ times}}.$$

Hence $T = n(n+1)/2$. The story goes that this was the argument Gauss discovered at the age of seven, when he was "invited" by his teacher to add the first 100 natural numbers.

Example **C.1.3** (Bernoulli's Inequality[3]). If $x > -1$, then

$$(1 + x)^n \geq 1 + nx \qquad \text{for all } n \in \mathbb{N}.$$

[2]Johann Carl Friedrich Gauss, 1777–1855.
[3]Jacob Bernoulli, 1654–1705.

Proof. Let

$$S = \{n \in \mathbb{N} : (1+x)^n \geq 1 + nx\}.$$

Note that $(1+x)^1 = 1 + 1 \cdot x$, hence $1 \in S$. On the other hand, if $k \in S$, that is, $(1+x)^k \geq 1 + kx$, then

$$(1+x)^{k+1} = (1+x)(1+x)^k \geq (1+x)(1+kx) = 1+(k+1)x+kx^2 \geq 1+(k+1)x.$$

By the principle of induction we conclude that $S = \mathbb{N}$, that is, the inequality holds for every natural number. /ᐢ∘ᴥ∘ᐢ\

Remark **C.1.4** (Proceeding inductively). The phrase *to proceed inductively* will appear frequently in subsequent sections and deserves special attention, since it is a phrase that allows one to avoid overwhelming the reader with formal details in a given argument. Essentially, it refers to the following idea: in order to exhibit a set X whose elements satisfy some property P, it is sometimes necessary to build the set step by step. We provide an element x_1 that satisfies property P, and we explain how, starting from the element x_1, one obtains a next element x_2 that also satisfies property P.

Having constructed $\{x_1, x_2, \ldots, x_n\}$ with property P, we then explain how to construct a subsequent element x_{n+1} that also satisfies property P, and so on. This argument allows us to obtain, for each $n \in \mathbb{N}$, an element x_n with property P.

There are two alternative ways of formulating the principle of induction. In Theorem C.1.7 we will show that the three principles are equivalent. That is, it is enough to assume any one of the three principles in order to obtain the other two.

Axiom **C.1.5** (Second Principle of Induction). Let $S \subseteq \mathbb{N}$ and suppose that

a) $1 \in S$,

b) if $\{1, 2, \ldots, k\} \subseteq S$, then $k + 1 \in S$.

Then $S = \mathbb{N}$.

Axiom **C.1.6** (Well-Ordering Principle). If $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then S has a first element; that is, there exists an element $m \in S$ such that $m \leq n$ for every $n \in S$.

Theorem C.1.7. *The following axioms are equivalent:*

a) The Well-Ordering Principle (WOP).

b) The First Principle of Induction (FPI).

c) The Second Principle of Induction (SPI).

Proof. *(WOP ⇒ FPI)* To prove that the WOP implies the FPI, let $S \subseteq \mathbb{N}$ satisfy the hypotheses of the FPI. We must show that $S = \mathbb{N}$. Proceed by contradiction and suppose that $S \subsetneq \mathbb{N}$. Then $\mathbb{N} \setminus S \neq \emptyset$. By the WOP, the set $\mathbb{N} \setminus S$ has a first element; call it m. Observe that $m \neq 1$, since $1 \in S$. Moreover, $m - 1 \in S$, because m is the first element of $\mathbb{N} \setminus S$. But then, by the second hypothesis of the FPI, it follows that $m \in S$, which contradicts the fact that $m \in \mathbb{N} \setminus S$. Hence $S = \mathbb{N}$.

(FPI ⇒ SPI) Clearly, the FPI implies the SPI, since if S is as in the SPI, then from $\{1, 2, \ldots, k\} \subseteq S$ it follows that $k + 1 \in S$, and therefore $S = \mathbb{N}$.

(SPI ⇒ WOP) Finally, suppose that the SPI holds, and let $S \subseteq \mathbb{N}$ be nonempty. If S does not have a first element, then $1 \notin S$, hence $1 \in \mathbb{N} \setminus S$. If $\{1, \ldots, k\} \subseteq \mathbb{N} \setminus S$, then $k + 1 \in \mathbb{N} \setminus S$; otherwise, $k + 1$ would be a first element of S. By the SPI, it follows that $\mathbb{N} \setminus S = \mathbb{N}$, and therefore $S = \emptyset$, which contradicts the assumption that $S \neq \emptyset$. Hence S has a first element. ^. .^)9

Definition **C.1.8.** A subset $S \subseteq \mathbb{N}$ is *finite* if there exists $n \in \mathbb{N}$ such that $S \subseteq \{1, 2, \ldots, n\}$. A subset $S \subseteq \mathbb{N}$ is *infinite* if it is not finite. That is, $S \subseteq \mathbb{N}$ is infinite if $S \setminus \{1, 2, \ldots, n\} \neq \emptyset \quad$ for all $n \in \mathbb{N}$.

The well-ordering principle implies the following result.

Theorem C.1.9. *Let $S \subseteq \mathbb{N}$ be an infinite set. Then there exists a function $\phi : \mathbb{N} \to S$ such that:*

a) ϕ is strictly increasing,[4]

b) $\phi(k) \geq k$ for all $k \in \mathbb{N}$,

c) ϕ is bijective.

Proof. Define $S_1 := S$. By the WOP, there exists $n_1 \in \mathbb{N}$, the first element of S_1. Define

$$S_2 := \{n \in S : n > n_1\} = S \setminus \{1, \ldots, n_1\}.$$

Clearly, $S_2 \neq \emptyset$ since S is infinite. By the WOP, there exists $n_2 \in \mathbb{N}$, the first element of S_2.

Proceeding inductively, we obtain $\{n_1, n_2, \ldots\} \subseteq S$ such that n_k is the first element of S_k, where

$$S_{k+1} := \{n \in S : n > n_k\} = S \setminus \{1, \ldots, n_k\}.$$

Define $\phi : \mathbb{N} \to S$ by $\phi(k) = n_k$.

[4] A function $g : \mathbb{N} \to \mathbb{N}$ is strictly increasing if $g(m) < g(n)$ for all $m < n$.

We now show that ϕ is strictly increasing and bijective. Note that

$$S_1 \supset S_2 \supset S_3 \supset \cdots$$

and, since $n_{k+1} \in S_{k+1}$, it follows that $n_{k+1} > n_k$. Therefore,

$$n_1 < n_2 < n_3 < \cdots,$$

which implies that ϕ is strictly increasing. By induction, one can also show that $\phi(k) \geq k$ for all $k \in \mathbb{N}$.

The fact that ϕ is strictly increasing implies that it is injective. We prove surjectivity as follows. Let $\alpha \in S$. Then $n_\alpha = \phi(\alpha) \geq \alpha$, which implies that $\alpha \notin S_{\alpha+1}$. Define

$$B = \{k \in \mathbb{N} : \alpha \notin S_{k+1}\}.$$

By what we have just shown, $B \neq \emptyset$. Let β be the first element of B. If $\beta = 1$, then $\alpha \notin S_2$. However, we always have $\alpha \in S = S_1$. If $\beta > 1$, then it cannot be that $\alpha \notin S_\beta$, since β is the first element of B. In either case, we have $\alpha \in S_\beta$ and $\alpha \notin S_{\beta+1}$. This implies that $\alpha \leq n_\beta$, and since n_β is the first element of S_β, it follows that $\alpha = n_\beta$. Hence, $\phi(\beta) = \alpha$. ^. .^)9

Remark **C.1.10**. In the induction proofs presented in this section, we have been deliberately and, in a sense, excessively formal: we have rigorously—perhaps even pedantically—concluded each argument by explicitly invoking one of the principles of induction, namely the FPI, the SPI, or the WOP. The reader should be aware that, in standard mathematical practice, it is perfectly acceptable to leave the appeal to any of these principles implicit. In formal mathematical discourse, one typically proceeds with a proof by induction by verifying the base case $k = 1$, formulating the inductive hypothesis (the case k or $\{1, \ldots, k\}$ cases), and then checking the validity of the case $k + 1$, without explicitly naming the underlying induction principle being used.

Exercise C.1.A. Use the Principle of Induction to prove the following variant of the Principle of Induction: Let $S \subseteq \mathbb{N}$ be such that for some $n_0 \in \mathbb{N}$ the following hold:

(a) $n_0 \in S$,

(b) if $k \geq n_0$ and $k \in S$, then $k + 1 \in S$.

Then S contains the set $\{n \in \mathbb{N} : n \geq n_0\}$.

Exercise C.1.B. Let $\phi : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function. Prove by induction that $\phi(k) \geq k$ for all $k \in \mathbb{N}$.

Exercise C.1.C.❀ (Cauchy induction.) Let $P(n)$ be a statement for each $n \in \mathbb{N}$. Suppose:

a) $P(1)$ holds;

b) $P(n) \Rightarrow P(2n)$ for every $n \in \mathbb{N}$;

c) $P(m+1) \Rightarrow P(m)$ for every $m \in \mathbb{N}$.

Show that $P(n)$ holds for all $n \in \mathbb{N}$.

Exercise C.1.D. Practice induction.

(a) Verify that $n^3 + 5n$ is divisible by 6 for all $n \in \mathbb{N}$.

(b) Prove that $2^n < n!$ for all $n \geq 4$.

(c) Conjecture a formula for the sum of the first n odd natural numbers, and prove it by induction.

(d) Prove that, for all $n \in \mathbb{N}$,

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}.$$

(e) Prove that, for all $n \in \mathbb{N}$ with $n \geq 2$,

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}.$$

Exercise C.1.E. Use the second principle of induction to prove that every natural number $n \geq 8$ can be written as a sum of the form $n = 3\alpha + 5\beta$, where $\alpha, \beta \in \mathbb{N}$.

Exercise C.1.F. Define recursively the Fibonacci numbers by $f_0 = f_1 = 1$ and $f_{n+2} = f_{n+1} + f_n$. Using the second principle of induction, prove that the following inequalities hold:

$$\left(\frac{3}{2}\right)^{n-1} \leq f_n \leq \left(\frac{7}{4}\right)^n, \qquad \text{for all } n \in \mathbb{N}.$$

Exercise C.1.G.❀ Let $m \in \mathbb{N}$ and let $z > -m$. Prove that, for all $n \in \mathbb{N}$ with $n \geq m$,

$$\left(1 + \frac{z}{n}\right)^n \geq \left(1 + \frac{z}{m}\right)^m.$$

(*Suggestion:* use Bernoulli's inequality from Example C.1.3 with

$$x = \frac{-z}{(n+1)n}\left(1+\frac{z}{n}\right)^{-1}$$

and the induction principle from Exercise C.1.A.)

C.2 The Integers, the Rational Numbers, and Field Axioms

Once we have the set of natural numbers, a simple formal construction (see, for instance, Birkhoff and Mac Lane (1997)) allows one to construct, starting from $\mathbb{N}$, the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

and from these, to construct the rational numbers

$$\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z},\ q \in \mathbb{N}\right\}.$$

Observe that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ and that, from an algebraic point of view, $\mathbb{Z}$ and $\mathbb{Q}$ are distinct structures. For instance, while in both $\mathbb{Z}$ and $\mathbb{Q}$ every element has an additive inverse (a "negative"), in $\mathbb{Z}$ there are elements that do not have a multiplicative inverse, whereas in $\mathbb{Q}$ every nonzero rational number does.The technical terminology for structures such as $\mathbb{Z}$ and $\mathbb{Q}$ is that of an *integral domain* and a *field*, respectively. In order to study arithmetic properties of the rational numbers, and later of the real numbers, we now present the axioms that define a field. The reader may notice that, indeed, the intuitive idea one has of the rational numbers effectively satisfies these axioms, and thus forms a field.

Definition **C.2.1** (Field). A *field* is a nonempty set F on which two arithmetic operations are defined,

$$\oplus : \mathsf{F} \times \mathsf{F} \to \mathsf{F} \qquad \text{and} \qquad \odot : \mathsf{F} \times \mathsf{F} \to \mathsf{F},$$

called *addition* and *multiplication*, respectively, and which satisfy the following properties:

a) **Properties of Addition**:
   i. $a \oplus b = b \oplus a$ for all $a, b \in \mathsf{F}$ (commutativity).
   ii. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ for all $a, b, c \in \mathsf{F}$ (associativity).

iii. There exists an element in F, denoted by 0, such that $a \oplus 0 = a$ for all $a \in \mathsf{F}$ (additive identity).

iv. For every $a \in \mathsf{F}$ there exists $b \in \mathsf{F}$ such that $a \oplus b = 0$ (additive inverse).

b) **Properties of Multiplication**:

i. $a \odot b = b \odot a$ for all $a, b \in \mathsf{F}$ (commutativity).

ii. $a \odot (b \odot c) = (a \odot b) \odot c$ for all $a, b, c \in \mathsf{F}$ (associativity).

iii. There exists an element in F, denoted by 1, such that $1 \neq 0$ and $a \odot 1 = a$ for all $a \in \mathsf{F}$ (multiplicative identity).

iv. For every $a \in \mathsf{F} \backslash \{0\}$ there exists $c \in \mathsf{F}$ such that $a \odot c = 1$ (multiplicative inverse).

c) **Joint Properties**:

i. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ for all $a, b, c \in \mathsf{F}$ (distributivity).

From the definition of a field it is easy to prove that both the additive inverse and the multiplicative inverse are unique. For example, to verify that the additive inverse is unique, suppose that for some $a \in \mathsf{F}$ there exist b and b' in F such that

$$a \oplus b = 0 \qquad \text{and} \qquad a \oplus b' = 0.$$

Then

$$b = b \oplus 0 = b \oplus (a \oplus b') = (b \oplus a) \oplus b' = (a \oplus b) \oplus b' = 0 \oplus b' = b'.$$

Each equality in the previous line is justified by the corresponding field axiom; for instance, the third equality from left to right follows from the associativity of addition. The preceding argument illustrates what is often called the *axiomatic method*: starting from a collection of axioms or basic principles, we can deduce all those arithmetic properties that we use naturally and that may seem surprising at first to be provable statements.

Since the additive and multiplicative inverses of the elements of a field are unique, we denote them by $-a$ and a^{-1} (or $1/a$), respectively.

Remark **C.2.2.** From now on, we will usually write $a + b$ instead of $a \oplus b$, and ab or $a \cdot b$ instead of $a \odot b$.

Example **C.2.3.** We now list some basic arithmetic properties whose proofs are left to the reader as practice in the axiomatic method. Throughout, we assume that all elements mentioned belong to a field F.

a) $a + 0 = a$ and $a \cdot 0 = 0$.

b) $-(-a) = a$.

c) $-a + (-b) = -(a + b)$.

d) If $a + b = a + c$, then $b = c$. *(cancellation law for addition)*

e) If $ab = ac$ and $a \neq 0$, then $b = c$. *(cancellation law for multiplication)*

f) $(a \cdot b^{-1}) \cdot (c \cdot d^{-1}) = (ac)(bd)^{-1}$.

g) $a \cdot b^{-1} + c \cdot d^{-1} = (ad + cb)(bd)^{-1}$.

Exercise C.2.A. Prove all the properties from example C.2.3.

In addition to the arithmetic rules that define a field, in many situations we also have an order relation on the elements of the field; for example, in $\mathbb{Q}$ we can say when one number is smaller than another. In general, the definition of an order is as follows.

Definition C.2.4. Let F be a field. We say that F is *ordered* if there exists a set

$$\mathcal{P} \subseteq \mathsf{F} \setminus \{0\},$$

called the *positive class*, such that the following properties hold:

a) If $a, b \in \mathcal{P}$, then $a + b \in P$ and $ab \in \mathcal{P}$. *(closure)*

b) For every $a \in \mathsf{F}$, exactly one of the following holds: $a \in \mathcal{P}$, or $-a \in \mathcal{P}$, or $a = 0$. *(trichotomy)*

If $a, b \in \mathsf{F}$, we say that a is *less than* b (notation: $a < b$) if $b - a \in \mathcal{P}$. In this case we also say that b is *greater than* a. We say that a is *less than or equal to* b if $a < b$ or $a = b$ (notation: $a \leq b$). Observe that if $b \in P$, then $b > 0$, since $b = b - 0$.

In the case of the field of rational numbers, the positive class P corresponds to the *positive rationals*, that is,

$$\mathcal{P} = \{\, p/q : p, q \in \mathbb{N} \,\}.$$

The following are some order properties that we suggest the reader verify.

Example C.2.5. Let F be an ordered field and let $a, b, c \in \mathsf{F}$. Then:

a) If $a < b$ and $b < c$, then $a < c$. *(transitivity)*

b) For $a, b \in \mathsf{F}$, exactly one of the following holds:

$$a < b, \qquad b < a, \qquad \text{or} \qquad a = b.$$

c) If $a < b$, then $a + c < b + c$.

d) If $a < b$ and $c > 0$, then $ac < bc$.

e) If $a < b$ and $c < 0$, then $bc < ac$.

f) If a^2 is defined as $a \cdot a$, then $a^2 \geq 0$.

Exercise C.2.B. Prove all the properties from example C.2.5.

Exercise C.2.C. In this exercise we show how to construct $\mathbb{Q}$ from $\mathbb{Z}$ and $\mathbb{N}$. Define in $\mathbb{Z} \times \mathbb{N}$ the following relation: $(p, q) \sim (p', q')$ if and only if $pq' = p'q$. Show that $\sim$ is an equivalence relation. Denote by $\mathbf{Q}$ the set of equivalence classes. Define a sum ($\oplus$), a product ($\odot$) and a positive class $\mathcal{P}$ in $\mathbf{Q}$ such that they make $(\mathbf{Q}, \oplus, \odot, \mathcal{P})$ an ordered field. Turns out, this ordered field will be preicsely $\mathbb{Q}$!

Exercise C.2.D. Show that $\mathsf{C} = \mathbb{Q} \times \mathbb{Q}$ is an ordered field if we define the arithmetic operations in the following way:

$$\begin{aligned}(a, b) \oplus (c, d) &= (a + c, b + d)\\ (a, b) \odot (c, d) &= (ac + 2bd, ad + bc).\end{aligned}$$

(*Suggestion:* in this case, the additive identity will be $\mathbf{0} = (0, 0)$ and the multiplicative identity $\mathbf{1} = (1, 0)$. Try to show, on a first instance, that if $(a, b) \neq (0, 0)$, then $a^2 - 2b^2 \neq 0$.)

Exercise C.2.E. For the field defined in exercise C.2.D, show that the following is a positive class.

$$\mathcal{P} = \{(a, b) \in \mathsf{C} : a > 0, a^2 > 2b^2\} \cup \{(a, b) \in \mathsf{C} : b > 0, a^2 < 2b^2\}.$$

(*Suggestion:* Show that if $(a, b) \neq (0, 0)$ then $(a, b) \in \mathcal{P}$ or $-(a, b) \in \mathcal{P}$.)

Appendix D

Cardinality and Equivalence of Sets

> I—I hardly know, sir, just at present—at least I know who I was when I got up this morning, but I think I must have been changed several times since then.
>
> Alice, in Lewis Carroll, *Alice's Adventures in Wonderland*

D.1 Cardinality of Sets

What do we do when we count? Basically, we establish a one-to-one correspondence between the elements of a set and what we might call an *initial segment* of the natural numbers. For example, if we want to make sure that there are indeed 16 kittens in a room, we would take the kittens one by one while simultaneously reciting: one, two, three, ..., sixteen. Being more precise, albeit at the risk of sounding pedantic, we would say that the set of kittens in the room has *cardinality*, or number of elements, equal to 16.

The purpose of this section is to extend this idea of counting to arbitrary sets, e.g. infinite ones.

An observation that will be useful in our subsequent study of cardinality is the fact that the relation "being in bijection with" is an equivalence relation between sets: $A \simeq B$ if and only if there exists a bijection $f : A \to B$. Recall that saying that $\simeq$ is an equivalence relation means that it is reflexive, symmetric, and transitive.

Proposition D.1.1. *The relation $A \simeq B$ is an equivalence relation.*

Proof. We will prove that the relation is reflexive, symmetric, and transitive. We verify each of these properties in turn.

a) To prove that the relation is reflexive, we show that for any arbitrary set A, one has $A \simeq A$. We seek a bijection $f\colon A \to A$. We choose $f = \mathrm{id}_A$. It is easy to see that id_A is a bijection. See Exercise B.2.G.

b) Symmetry is proved as follows. Suppose that $A \simeq B$. We want to show that $B \simeq A$. We know that there exists a bijection $f: A \to B$. Since f is bijective, its inverse f^{-1} is also bijective. See Exercise B.2.G. Therefore, $f^{-1}: B \to A$, which implies $B \simeq A$.

c) Finally, we prove transitivity. Suppose that $A \simeq B$ and $B \simeq C$. Then there exist bijective functions $f: A \to B$ and $g: B \to C$. Consider the function $g \circ f: A \to C$. It remains to show that $g \circ f$ is bijective.

   First, we prove injectivity. Let $a \neq a'$ be elements of A. By the injectivity of f, we have $f(a) \neq f(a')$, and by the injectivity of g, it follows that $g(f(a)) \neq g(f(a'))$. Hence,

$$(g \circ f)(a) \neq (g \circ f)(a'),$$

   and therefore $g \circ f$ is injective.

   Finally, we prove surjectivity. Let $c \in C$. By the surjectivity of g, there exists $b \in B$ such that $g(b) = c$, and by the surjectivity of f, there exists $a \in A$ such that $f(a) = b$. Therefore,

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

   We conclude that $g \circ f$ is surjective.

This completes the proof. /ᐠ｡ꞈ｡ᐟ\

Whenever one has an equivalence relation on a set or family $\mathcal{F}$ (in our case, a family of sets), it induces a partition of the family into equivalence classes. That is, if

$$[A] = \{ B \in \mathcal{F} : B \simeq A \}$$

is the equivalence class of the set A, then $[A] \neq \emptyset$ for every A. Moreover, the following properties hold:

a) if $A, B \in \mathcal{F}$, then either $[A] = [B]$ or $[A] \cap [B] = \emptyset$, and

b) $\mathcal{F} = \bigcup \{ [A] : A \in \mathcal{F} \}$.

The label or name that we will use to identify the equivalence classes of sets under this relation is *cardinal*, and we will denote the cardinal of a set A by $|A|$. Intuitively, two sets in the same equivalence class “have the same number of elements.” For example, the cardinal of the set $\{a, b, c, d\}$ is **4** (here the symbol

4 is the label carried by all sets that are in bijection with $\{a, b, c, d\}$). Counting, then consists of declaring two sets equivalent, and this happens precisely when there exists a bijective function between them.

In definition C.1.8 we established what is meant by finite and infinite for subsets of $\mathbb{N}$. The following definition generalizes those concepts to arbitrary sets.

***Definition* D.1.2.** A set A is *finite* if $A = \emptyset$ or if there exists a bijection

$$f: \{1, 2, \ldots, n\} \to A,$$

for some $n \in \mathbb{N}$. In this case, we say that A has n elements and we write $|A| = n$. If we denote $a_j = f(j)$ for each $j \in \{1, 2, \ldots, n\}$, we say that $\{a_1, a_2, \ldots, a_n\}$ is a *enumeration* of A. A set A is *infinite* if it is not finite.

Exercise D.1.A.🐾 Show that definition D.1.2 generalizes definition C.1.8. That is, if $S \subseteq \mathbb{N}$ is finite or infinite according to definition C.1.8 then it also is according to definition D.1.2

Proposition D.1.3. $\mathbb{N}$ *is infinite.*

Proof. Suppose, by contradiction, that $\mathbb{N}$ is finite. Then there exist $m \in \mathbb{N}$ and a bijection

$$f: \{1, 2, \ldots, m\} \to \mathbb{N}.$$

Let $x_i := f(i)$ for $i = 1, 2, \ldots, m$, and let

$$p = x_1 + \cdots + x_m.$$

Since $p \in \mathbb{N}$ and f is surjective, there exists some i such that $p = x_i$. This is impossible, since $p > x_j$ for every j. Therefore, $\mathbb{N}$ is infinite. /ᐠ｡ꞈ｡ᐟ\

Note that by transitivity, any set that is in bijection with the set of natural numbers is also infinite. For example, the set of odd natural numbers (those of the form $2n - 1$ with $n \in \mathbb{N}$) is infinite.

***Definition* D.1.4.** A set A is *countable* if there exists a bijective function

$$f: \mathbb{N} \to A.$$

If we write $a_j := f(j)$ for $j \in \mathbb{N}$, we say that $\{a_1, a_2, \ldots\}$ is an *enumeration* of A. We further say that A has the cardinality of $\mathbb{N}$ and write $|A| = \aleph_0$. The symbol $\aleph_0$ (read *aleph zero*) denotes $|\mathbb{N}|$. Consequently, if A is countable, then $|A| = \aleph_0$.

***Definition* D.1.5.** The *cardinal number* of a finite set is just the number of elements in the set. The *cardinal number* of the set $\mathbb{N}$ of natural numbers is $\aleph_0$. Any set with cardinality $\aleph_0$ is called a *countably infinite* set and any finite or countable infinite set is called a *countable* set. An infinite set that is not countable is said to be *uncountable.*

***Example* D.1.6.** The set of integers, which at first glance appears to be "larger" than the set of natural numbers, is in fact countable. Indeed, the function $g\colon \mathbb{N} \to \mathbb{Z}$ defined by

$$g(n) = \begin{cases} 0, & \text{if } n = 1, \\ k, & \text{if } n = 2k,\ k \geq 1, \\ -k, & \text{if } n = 2k+1,\ k \geq 1, \end{cases}$$

is bijective.

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & \cdots & 2k & 2k+1 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \\ 0 & 1 & -1 & 2 & -2 & \cdots & k & -k & \cdots \end{array}$$

Essentially, the sets that are equivalent to finite sets or to the set of natural numbers are precisely the sets that we can count. We therefore adopt the following terminology.

***Definition* D.1.7.** A set is *countable* if it is finite or countably infinite.

Let us now look at some properties of countable sets.

Lemma D.1.8. *Let A be a finite set, with $A \neq \emptyset$ and $|A| = n$, and let $a \in A$. Then*

$$|A \setminus \{a\}| = n - 1.$$

Proof. If $|A| = 1$, then $A = \{a\}$. Thus $A \setminus \{a\} = \emptyset$ and $|\emptyset| = 0$.

Now suppose that $|A| = n > 1$, and let $\{a_1, a_2, \ldots, a_n\}$ be an enumeration of A. Then $a = a_i$ for some $i = 1, 2, \ldots, n$. Define a function

$$g\colon \{1, 2, \ldots, n-1\} \to A \setminus \{a\}$$

as follows. If $a = a_1$, then $g(j) = a_{j+1}$ for all $j = 1, \ldots, n-1$. If $a = a_n$, then $g(j) = a_j$ for all $j = 1, \ldots, n-1$. Otherwise, if $1 < i < n$, define

$$g(j) = \begin{cases} a_j, & 1 \leq j \leq i-1, \\ a_{j+1}, & i \leq j \leq n-1. \end{cases}$$

The function g is bijective, and therefore $|A \setminus \{a\}| = n - 1$. /ᐠ｡ꞈ｡ᐟ\

Exercise D.1.B. In this exercise, we state a generalization of lemma D.1.8. Let A be finite and non-empty. Prove that, if $B \subseteq A$ then $|A \setminus B| = |A| - |B|$.

Proposition D.1.9. *If A and B are finite sets, then $A \cup B$ is finite.*

Proof. If $A = \emptyset$ or $B = \emptyset$, then $A \cup B = B$ or $A \cup B = A$, respectively, and the result is immediate.

Assume now that $A \neq \emptyset$ and $B \neq \emptyset$. We proceed by induction on $|B|$. If $|B| = 1$, then $B = \{b\}$. If $A = \{a_1, \ldots, a_n\}$ and $b = a_i$ for some $i = 1, \ldots, n$, then $A \cup B = A$, which is finite. Otherwise, if $b \neq a_i$ for all $i = 1, \ldots, n$, define a function

$$f \colon \{1, 2, \ldots, n+1\} \to A \cup B$$

by

$$f(i) = \begin{cases} a_i, & 1 \leq i \leq n, \\ b, & i = n+1. \end{cases}$$

Then $A \cup B$ is finite and $|A \cup B| = n + 1$.

Now assume that if $|B| = m$, then $A \cup B$ is finite. We must show that if $|B| = m + 1$, then $A \cup B$ is finite. Let $b \in B$. By Lemma D.1.8, the set $B \setminus \{b\}$ has m elements. By the induction hypothesis, $A \cup (B \setminus \{b\})$ is finite. Therefore, $A \cup (B \setminus \{b\}) \cup \{b\}$ is finite, and hence $A \cup B$ is finite. /ᐠ｡ꞈ｡ᐟ\

The previous proposition is easily extended, by induction, to the finite union of finite sets.

Proposition D.1.10. *If $\mathcal{F}$ is a finite family of finite sets, then*

$$\bigcup_{A \in \mathcal{F}} A$$

is finite.

***Remark* D.1.11.** The previous proposition can also be written in a different way. Since $\mathcal{F}$ is a finite family of finite sets, we may enumerate its elements as

$$\mathcal{F} = \{A_1, \ldots, A_n\}.$$

Therefore, if each A_k is finite, then

$$\bigcup_{k=1}^{n} A_k = \bigcup_{A \in \mathcal{F}} A$$

is finite.

Exercise D.1.C.🐾 Prove proposition D.1.10.

Corollary D.1.12. *If A is a finite set and $B \subseteq A$, then B is finite.*

Proof. If $A = \emptyset$, then $B = \emptyset$ and hence B is finite. We now proceed by induction on $|A|$. If $|A| = 1$, then either $B = \emptyset$ or $B = A$, and in either case B is finite.

Assume that if $|A| = n$ and $B \subseteq A$, then B is finite. Let A be a set with $|A| = n + 1$ and let $B \subseteq A$. Choose $a \in A$. By Lemma D.1.8, the set $A \setminus \{a\}$ has n elements.

If $a \notin B$, then $B \subseteq A \setminus \{a\}$, and by the induction hypothesis, B is finite. Finally, if $a \in B$, then $B \setminus \{a\} \subseteq A \setminus \{a\}$, so $B \setminus \{a\}$ is finite. By Proposition D.1.9, the set $(B \setminus \{a\}) \cup \{a\}$ is finite. Therefore, B is finite.

As a consequence of the previous corollary, we obtain the following result.

Corollary D.1.13. *If B is an infinite set and $B \subseteq A$, then A is infinite.*

Proof. If A were finite, then by Corollary D.1.12, B would be finite, which is a contradiction.

In general, given any set A, it is always possible to construct a set whose cardinality is strictly greater than that of A. For example, if $|A| = n$, then $|\mathscr{P}(A)| = 2^n > n = |A|$.

In the case of infinite sets, we can also compare cardinalities. The notion that one cardinal is larger than another is defined as follows. Given two sets X and Y, we say that the cardinality of X is less than the cardinality of Y if $X \not\sim Y$, that is, if X and Y are not equivalent, and if X is equivalent to a subset of Y. We write this as $|X| < |Y|$. In fact, it is always true that for any nonempty set A, $|A| < |\mathscr{P}(A)|$.

Exercise D.1.D. (Cantor's Theorem.) Let E be a nonempty set.

a) Show that E is equivalent to the following subset of $\mathscr{P}(E)$:

$$\{\, \{x\} \in \mathscr{P}(E) : x \in E \,\}.$$

b) Let $\varphi \colon E \to \mathscr{P}(E)$ be a function. Show that the set

$$A = \{\, x \in E : x \notin \varphi(x) \,\}$$

is not in the image of φ, and therefore there does not exist a surjective function $E \to \mathscr{P}(E)$.

c) Show that $E \not\sim \mathscr{P}(E)$ and hence $|E| < |\mathscr{P}(E)|$.

This allows us to define a strictly increasing sequence of infinite cardinals. That is, if $\aleph_0 = \kappa_0 = |\mathbb{N}|$, we define

$$\kappa_1 = |\mathscr{P}(\mathbb{N})|, \quad \kappa_2 = |\mathscr{P}(\mathscr{P}(\mathbb{N}))|,$$

and so on. By Cantor's theorem (Exercise D.1.D),

$$\kappa_0 < \kappa_1 < \kappa_2 < \cdots .$$

The following two propositions show that the infinite cardinal $\aleph_0$, which corresponds to the set of natural numbers, is the smallest possible infinite cardinal.

Proposition D.1.14. *If A is countable and $B \subseteq A$, then B is countable. That is, a countable set contains only finite or countably infinite subsets.*

Proof. Let $f\colon \mathbb{N} \to A$ be a bijective function, and let $S = f^{-1}(B)$. By Definition D.1.2, the set S is finite if and only if B is finite. If B is infinite, then S is infinite, and by Theorem C.1.9 there exists a bijection $\varphi\colon \mathbb{N} \to S$. Clearly, the composition $f \circ \varphi\colon \mathbb{N} \to B$ is bijective, and therefore B is countable. /ᐠ｡ꞈ｡ᐟ\

Remark **D.1.15.** In particular, by Euclid's[1] theorem (which states that the set of prime numbers is infinite) and Proposition D.1.14, it follows that the set of prime numbers is countable. However, no explicit bijective function $f\colon \mathbb{N} \to \{\, p \in \mathbb{N} : p \text{ is prime} \,\}$ is known.

Exercise D.1.E.🐾🐾🐾 Construct explicitly a bijective function $f\colon \mathbb{N} \to \{\, p \in \mathbb{N} : p \text{ is prime} \,\}$ whose definition does not appeal to an oracle, implicit enumeration, or non-constructive existence arguments.

Joke **D.1.16.** The previous exercise was a joke. However, if someday any of you manages to solve Exercise D.1.E in any meaningful or illuminating way, please mention me in your acceptance speech for the Fields Medal, the Abel Prize, or the Wolf Prize in Mathematics. Also, please share with me the one million dollars you will win from the Clay Mathematics Institute. ⊂(^・ω・^)

Remark **D.1.17.** While the set of prime numbers is countable, the lack of an explicit and well-behaved bijection between $\mathbb{N}$ and the primes reflects the profound difficulty of understanding their distribution. This difficulty is intimately connected with one of the so-called *Millennium Problems*: the Riemann[2] Hypothesis, whose resolution would yield deep information about the asymptotic behavior of primes. For its solution, the Clay Mathematics Institute offers a prize of one million dollars.

Proposition D.1.18. *If A is an infinite set, then A contains a countable subset.*

Proof. Since A is infinite, it is in particular nonempty, so there exists $a_1 \in A$. Again, since A is infinite, we have $A \setminus \{a_1\} \neq \emptyset$, and we may choose $a_2 \in A \setminus \{a_1\}$.

[1] Euclid of Alexandria, 325(?)BCE–264BCE

[2] Georg Friedrich Bernhard Riemann, 1826–1866.

Then $A \setminus \{a_1, a_2\} \neq \emptyset$. Proceeding inductively, we obtain a set $B = \{a_1, a_2, \ldots\}$ which is countable. ^. .^)9

Perhaps the first philosophical antithesis encountered when dealing with infinite sets is the fact that the whole is not necessarily larger than each of its parts, at least with respect to cardinality. For example, $\mathbb{N}$ is in bijection with its proper subset $\mathbb{N} \setminus \{1\}$ via the function $n \mapsto n+1$, and also with the set $\{\, n \in \mathbb{N} : n \text{ is even} \,\}$ via the function $m \mapsto 2m$. In general, we have the following proposition, whose proof is left to the reader.

Proposition D.1.19. *A set A is infinite if and only if there exists a proper subset B of A such that $B \simeq A$.*

Perhaps the first unintuitive result we encounter when dealing with infinite sets is that the whole is not necessarily larger than each of its parts, at least as far as cardinality is concerned. For example, $\mathbb{N}$ is in bijection with its proper subset $\mathbb{N} \setminus \{1\}$ via the function $n \mapsto n + 1$, and also with the set $\{n \in \mathbb{N} : n \text{ is even}\}$ via the function $m \mapsto 2m$. In general, we have the following proposition.

Proposition D.1.20. *A set A is infinite if and only if there exists a proper subset $B \subsetneq A$ such that $B \simeq A$.*

Exercise D.1.F. Prove proposition D.1.20.

D.2 Criteria for the equivalence of sets

In this section our interest is to find necessary and sufficient conditions for a set to be countable. There exist general criteria to guarantee the equivalence of sets; the most famous of these is without doubt the Cantor[3]-Schröder[4]-Bernstein[5] theorem, which we state next. A simple, aesthetic,[6] and elegant proof of this result can be found in Birkhoff and Mac Lane (1997, ch. 12, sec. 3, thm. 6, pp. 387–388).

Theorem D.2.1 (Cantor–Schröder–Bernstein). *Two sets A and B are equivalent if and only if A is equivalent to a subset of B and B is equivalent to a subset of A, that is, if there exist injective functions*

$$f\colon A \to B \qquad \text{and} \qquad g\colon B \to A.$$

[3] George Ferdinand Ludwig Philipp Cantor, 1845–1918.
[4] Friedrich Wilhelm Karl Ernst Schröder, 1841–1902.
[5] Sergei Natanovich Bernstein, 1880–1968.
[6] Mindful and demure.

Definition D.2.2. Let A and B be sets. We write

$$|A| \leq |B|$$

if there exists an injective function $f : A \to B$.

Remark D.2.3. By the Cantor–Schröder–Bernstein theorem D.2.1, if

$$|A| \leq |B| \quad \text{and} \quad |B| \leq |A|,$$

then $A \simeq B$. Hence this relation induces a partial order on equivalence classes of sets.

Exercise D.2.A. In this exercise we give an alternative proof of Theorem D.2.1. The original idea can be found in the proof given in Aigner and Ziegler (1998).

Let A and B be arbitrary sets. Suppose there exist injective functions

$$f\colon A \to B \qquad \text{and} \qquad g\colon B \to A.$$

Define

$$C_0 = A \setminus g(B), \qquad C_{n+1} = g\big(f(C_n)\big),$$

and set

$$C = \bigcup_{n=0}^{\infty} C_n.$$

a) Prove that f is injective on C and that $A \setminus C \subseteq g(B)$.

b) Define the function $h\colon A \to B$ by

$$h(x) = \begin{cases} f(x), & x \in C, \\ g^{-1}(x), & x \notin C. \end{cases}$$

Prove that h is well defined and injective.

c) Let $b \in B$ be such that $g(b) \in C$. Prove that there exists $a \in C$ such that $f(a) = b$.

d) Prove that h is surjective and conclude the Cantor–Schröder–Bernstein theorem.

To decide whether a set is countable or not, the following theorem and its corollary are perhaps the most useful tools, since it suffices to exhibit a surjective function from the natural numbers onto the set (or, equivalently, an injective function from the set into the natural numbers).

Theorem D.2.4. *If $A \neq \emptyset$, then A is countable if and only if there exists a surjective function*

$$f\colon \mathbb{N} \to A.$$

Proof. Suppose first that A is countable. If A is finite, let $\{a_1, \dots, a_n\}$ be an enumeration of A and define $f\colon \mathbb{N} \to A$ by

$$f(j) = \begin{cases} a_j, & 1 \leq j \leq n, \\ a_1, & j \geq n+1. \end{cases}$$

Clearly, f is surjective. On the other hand, if A is countably infinite, say $A = \{a_1, a_2, \dots\}$, define $f\colon \mathbb{N} \to A$ by $f(j) = a_j$ for all $j \in \mathbb{N}$, which is again surjective.

To prove sufficiency, let $f\colon \mathbb{N} \to A$ be a surjective function. For each $a \in A$ we may choose $n_a \in \mathbb{N}$ such that $f(n_a) = a$. Define $g\colon A \to \mathbb{N}$ by $g(a) = n_a$. The function g is injective because f is a function. Hence, A and $g(A)$ are equivalent. Since $g(A) \subseteq \mathbb{N}$, the set $g(A)$ is countable, and therefore A is countable. ^. .^)9

Corollary D.2.5. *A set A is countable if and only if there exists an injective function*

$$g\colon A \to \mathbb{N}.$$

Proof. If A is countable, any enumeration of A provides the desired injective function. Conversely, if $g\colon A \to \mathbb{N}$ is injective, define the function $f\colon \mathbb{N} \to A$ by

$$f(n) = \begin{cases} a, & \text{if } g(a) = n, \\ a_0, & \text{if } g(a) \neq n \text{ for all } a \in A, \end{cases}$$

where $a_0 \in A$ is fixed. Then f is surjective. /ᐠ｡ꞈ｡ᐟ\

***Example* D.2.6.** The set $\mathbb{Z}$ is countable. Define $f\colon \mathbb{Z} \to \mathbb{N}$ by

$$f(z) = \begin{cases} -2z+1, & \text{if } z \leq 0, \\ 2z, & \text{if } z > 0. \end{cases}$$

The function f is injective (in fact, bijective).

A set that, *a priori*, might appear to have strictly larger cardinality than the set of natural numbers is the set of rational numbers. Nevertheless, as the next example shows, there are as many rational numbers as natural numbers.

Example **D.2.7.** The set $\mathbb{Q}$ is countable. Recall that

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\ q \in \mathbb{N},\ \gcd(p,q) = 1 \right\}.$$

Define $g\colon \mathbb{Q} \to \mathbb{N}$ by

$$g\left(\frac{p}{q}\right) = \begin{cases} 2^p 3^q, & \text{if } p \geq 0, \\ 5^{-p} 7^q, & \text{if } p < 0. \end{cases}$$

The function g is injective by the Fundamental Theorem of Arithmetic (although it is not surjective).

Example **D.2.8.** The set

$$\mathbb{Q}^+ := \{q \in \mathbb{Q} : q > 0\}$$

is countable. A picture is worth more than a thousand words.

$$\begin{array}{ccccccccccc}
\frac{1}{1} & \rightarrow & \frac{2}{1} & & \frac{3}{1} & \rightarrow & \frac{4}{1} & & \frac{5}{1} & \rightarrow & \cdot \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \cdot & & \cdot \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & & & & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \cdot & & \cdot & & \cdot \\
 & \swarrow & & \nearrow & & & & & & & \\
\frac{1}{4} & & \frac{2}{4} & & \cdot & & \cdot & & \cdot & & \cdot \\
\downarrow & \nearrow & & & & & & & & & \\
\frac{1}{5} & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot \\
\downarrow & & & & & & & & & & \\
\cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot
\end{array}$$

Example **D.2.9.** Let

$$\mathcal{P} = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \{0, 1, \dots\},\ a_i \in \mathbb{Z},\ i \in \{0, 1, \dots, n\}\}$$

be the set of polynomials with integer coefficients and real variable, and let

$$\mathcal{R} = \{\text{real roots of elements of } \mathcal{P}\}.$$

Then $\mathcal{R}$ is countable. This result is a corollary of exercise 2.2 in Rudin (1976, ch. 2, ex. 2, p. 43)

An analogue of Proposition D.1.10 is the following result.

Proposition D.2.10. *Let $\mathcal{F}$ be a countable family of nonempty countable sets. Then the set*

$$\bigcup_{A \in \mathcal{F}} A$$

is countable.

The proof of Proposition D.2.10 is based on the following lemma.

Lemma D.2.11. *If A and B are countable sets, then $A \times B$ is countable.*

Proof. Since A and B are countable, by Theorem D.2.4 there exist surjective functions $f\colon \mathbb{N} \to A$ and $g\colon \mathbb{N} \to B$. Define the function $h\colon \mathbb{N} \times \mathbb{N} \to A \times B$ by $h(n, m) = \big(f(n), g(m)\big)$. The function h is surjective. Since $\mathbb{N} \times \mathbb{N}$ is countable (for example, the function $(n, m) \mapsto 2^{n-1}(2m - 1)$ is a bijection from $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$), it follows that $A \times B$ is countable. ^. .^)9

Proof (Proof of Proposition D.2.10). Since $\mathcal{F}$ is countable, there exists a surjective function $G\colon \mathbb{N} \to \mathcal{F}$. Moreover, for each $A \in \mathcal{F}$ there exists a surjective function $f_A\colon \mathbb{N} \to A$. Define the function

$$h\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{A \in \mathcal{F}} A$$

by $h(n, m) = f_{G(n)}(m)$. The function h is surjective. By Lemma D.2.11, the set $\mathbb{N} \times \mathbb{N}$ is countable, and therefore $\bigcup_{A \in \mathcal{F}} A$ is countable. /ᐠ｡ꞈ｡ᐟ\

Example **D.2.12.** In light of Proposition D.2.10, we can give another proof that the set of rational numbers is countable. Indeed, for each $j \in \mathbb{N}$ consider the set

$$A_j = \left\{ \frac{p}{q} \in \mathbb{Q} : |p| + |q| \leq j \right\}.$$

Each A_j is finite, and clearly $\mathbb{Q} = \bigcup_{j \in \mathbb{N}} A_j$.

Exercise D.2.B. In example D.2.12, what would be an upper bound for the number of elements of each A_j?

We conclude the section with a very useful counting result, known here as the *Cats in Boxes Principle*.

Lemma D.2.13 (Cats in Boxes Principle). *Let A and B be finite sets such that $|A| > |B|$. If $f : A \to B$ is a function, then there exist two distinct elements $a, b \in A$ such that $a \neq b$ and $f(a) = f(b)$.*

Joke **D.2.14.** Think of K cats and M boxes, with $K > M$. Certainly, some cats will have to share boxes, which is something that Panqueque would find unacceptable.

Joke **D.2.15.** In the standard mathematical literature, particularly among authors with a less playful disposition or a stronger affinity for avian metaphors, lemma D.2.13 is referred to as the *Pigeonhole Principle.*

Exercise D.2.C. Prove that if $A \simeq A'$ and $B \simeq B'$, then $A \times B \simeq A' \times B'$.

Exercise D.2.D. Prove that the following function is a bijection:

$$F : \{1, \ldots, n\} \times \{1, \ldots, m\} \to \{1, \ldots, mn\}, \qquad F(p, q) = (p - 1)m + q.$$

Exercise D.2.E.🐾 Prove that if A and B are finite sets, then $|A \times B| = |A|\,|B|$.

Exercise D.2.F. If A is finite with $|A| = n$, prove that $|\mathcal{P}(A)| = 2^n$.

Exercise D.2.G. Suppose that $A \simeq B$ via a bijection $f : A \to B$. Prove that:

a) for every $C \subseteq A$ one has $C \simeq f(C)$ and hence $|C| = |f(C)|$;

b) for every $D \subseteq B$ one has $D \simeq f^{-1}(D)$ and hence $|D| = \left|f^{-1}(D)\right|$.

Exercise D.2.H. Let A be finite with $|A| = n$. Define $\Omega = \{(a, b) \in A \times A : a \neq b\}$. Prove that $\Omega \simeq \{1, \ldots, n\} \times \{1, \ldots, n - 1\}$.

Exercise D.2.I. Let A, B, and C be sets such that $A \subseteq B \subseteq C$. Suppose that $A \simeq C$. Prove that $A \simeq B \simeq C$.

Exercise D.2.J.🐾 Let A be a set. Prove that there exists a bijection between the set $\mathcal{F}(A) = \{g : A \to \{0, 1\}\}$ of functions with domain A and codomain $\{0, 1\}$, and the power set $\mathcal{P}(A) = \{B : B \subseteq A\}$. *Suggestion:* prove that the function $H : \mathcal{F}(A) \to \mathcal{P}(A)$ defined by $H(g) = g^{-1}(\{1\})$ is a bijection.

D.3 Cardinal Arithmetic

After having defined cardinality via the existence of bijections, we can introduce arithmetic operations on cardinal numbers by imitating the corresponding set-theoretic constructions. These operations satisfy many familiar algebraic properties, but behave very differently once infinite sets are involved. In what follows, we record a few basic arithmetic facts about cardinalities, mostly without proof, to be used as tools later on.

***Definition* D.3.1.** Let κ and λ be cardinal numbers. Let S and T be disjoint sets such that $|S| = \kappa$ and $|T| = \lambda$.

a) The *sum* $\kappa + \lambda$ is the cardinal number of $S \cup T$.

b) The *product* $\kappa\lambda$ is the cardinal number of $S \times T$.

c) The *power* κ^{λ} is the cardinal number of S^T.

It can be shown, using D.3.1, that cardinal addition and multiplication are associative and commutative, and that multiplication distributes over addition.

Theorem D.3.2. *Let κ, λ, and μ be cardinal numbers. Then the following properties hold:*

a) (Associativity)
$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu \quad \textit{and} \quad \kappa(\lambda\mu) = (\kappa\lambda)\mu.$$

b) (Commutativity)
$$\kappa + \lambda = \lambda + \kappa \quad \textit{and} \quad \kappa\lambda = \lambda\kappa.$$

c) (Distributivity)
$$\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu.$$

d) (Properties of Exponents)

i. $\kappa^{\lambda+\mu} = \kappa^{\lambda}\kappa^{\mu}$,

ii. $(\kappa^{\lambda})^{\mu} = \kappa^{\lambda\mu}$,

iii. $(\kappa\lambda)^{\mu} = \kappa^{\mu}\lambda^{\mu}$.

On the other hand, the arithmetic of cardinal numbers can seem somewhat strange, as the next theorem shows.

Theorem D.3.3. *Let κ and λ be cardinal numbers, at least one of which is infinite. Then*
$$\kappa + \lambda = \kappa\lambda = \max\{\kappa, \lambda\}.$$

From exercise D.2.J we know there is a bijection from the power set $\mathcal{P}(S)$ of a set S and the set of all functions from S to $\{0, 1\}$. This leads to the following theorem.

Theorem D.3.4. *For any cardinal κ:*

a) If $|S| = \kappa$, then $|\mathcal{P}(S)| = 2^\kappa$.

b) $\kappa < 2^\kappa$.

Remark D.3.5. We have already observed that $|\mathbb{N}| = \aleph_0$, and that $\aleph_0$ is the smallest infinite cardinal; that is,

$$\kappa < \aleph_0 \;\Rightarrow\; \kappa \text{ is a natural number.}$$

It can also be shown that the set $\mathbb{R}$ can be put in bijection with the power set $\mathcal{P}(\mathbb{N})$. Therefore,

$$|\mathbb{R}| = 2^{\aleph_0}.$$

The set of all points on the real line is called the *continuum*, and the cardinal $2^{\aleph_0}$ is therefore called the *cardinality of the continuum*, usually denoted by $\mathfrak{c}$.

We are now in a position to define the aleph numbers, which enumerate the infinite cardinal numbers in increasing order.

Definition D.3.6. The sequence of *aleph numbers* $\{\aleph_\alpha\}$ is defined recursively as follows.

- $\aleph_0$ is the smallest infinite cardinal.
- Given a cardinal $\aleph_\alpha$, the cardinal $\aleph_{\alpha+1}$ is defined to be the smallest cardinal strictly larger than $\aleph_\alpha$.

Remark D.3.7. A natural question is whether there exist cardinal numbers strictly between $\aleph_0$ and $\mathfrak{c}$. The assertion that no such cardinal exists, that is, that $\mathfrak{c} = \aleph_1$, is known as the *Continuum Hypothesis*.

Theorem D.3.3 shows that cardinal addition and multiplication have a kind of *absorption* property, which makes it hard to produce larger cardinals from smaller ones. The next theorem demonstrates this more dramatically.

Theorem D.3.8. *a) Addition applied a countable number of times or multiplication applied a finite number of times to the cardinal number $\aleph_0$ does not yield anything more than $\aleph_0$. Specifically, for any nonzero $n \in \mathbb{N}$, we have*

$$\aleph_0 \cdot \aleph_0 = \aleph_0 \quad \textit{and} \quad \aleph_0^n = \aleph_0.$$

b) *Addition and multiplication applied a countable number of times to the cardinal number $2^{\aleph_0}$ does not yield more than $2^{\aleph_0}$. Specifically, we have*

$$\aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0} \quad \text{and} \quad \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0}.$$

Using this theorem, we can establish other relationships, such as

$$2^{\aleph_0} \leq (\aleph_0)^{\aleph_0} \leq \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0},$$

which, by theorem D.2.1 implies that

$$(\aleph_0)^{\aleph_0} = 2^{\aleph_0}.$$

Theorem D.3.9. *Let $\{A_k : k \in K\}$ be a family of sets, indexed by the set K with $|K| = \kappa$. Assume that $|A_k| \leq \lambda$ for all $k \in K$. Then*

$$\left| \bigcup_{k \in K} A_k \right| \leq \lambda\kappa.$$

Exercise D.3.A. Prove theorem D.3.9.

***Example* D.3.10.** The following examples illustrate some common sets and their cardinalities.

a) The following sets have cardinality $\aleph_0$:
   i. the set of rational numbers $\mathbb{Q}$;
   ii. the set of all finite subsets of $\mathbb{N}$;
   iii. the union of a countable family of countable sets;
   iv. the set $\mathbb{Z}^n$ of all ordered n-tuples of integers.

b) The following sets have cardinality $\mathfrak{c} = 2^{\aleph_0}$:
   i. the set of all points in $\mathbb{R}^n$;
   ii. the set of all infinite sequences of natural numbers;
   iii. the set of all infinite sequences of real numbers;
   iv. the set of all finite subsets of $\mathbb{R}$;
   v. the set of all irrational numbers.

Appendix E

The Real Numbers

To see a World in a Grain of Sand
And a Heaven in a Wild Flower
Hold Infinity in the palm of your hand
And Eternity in an hour.

— William Blake, *Auguries of Innocence*

E.1 Why do we need the real numbers?

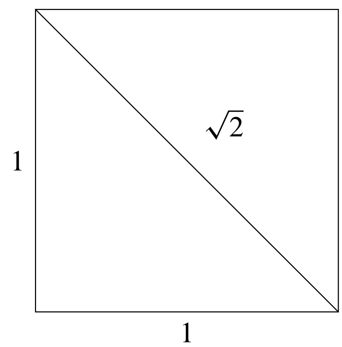


Figure E.1: A unit square and its diagonal.

It is not hard to find situations where numbers arise that are not rational. Since antiquity—think, for instance, of the Greeks in the fifth century B.C.—numbers such as $\sqrt{2}$ came to light. One discovers, for example, that a side and the diagonal of a square are *incommensurable*: there is no common unit length whose integer multiples measure both segments. Equivalently, the ratio of their lengths is not the ratio of two integers.

Indeed, suppose the ratio of the diagonal to the side were rational, say p/q with p and q integers with no common factor. The relation between the diagonal and the side forces both p and q to be divisible by 2, contradicting the assumption that p/q is in lowest terms.

A different way to exhibit irrational numbers is via decimal expansions. Using the division algorithm, one can show that the rational numbers are *exactly* those whose decimal expansion is eventually periodic. For if p/q is rational, then in the long division of p by q the remainder is always an integer between 0 and $q-1$. Hence, after finitely many steps, a remainder must repeat, and from that point on the digits repeat periodically. For example,

$$\frac{3}{7} = 0.\overline{428571}.$$

Conversely, any eventually periodic decimal expansion can be converted into a fraction (for instance, using a geometric series).

It is therefore easy to conceive of numbers whose decimal expansion is not periodic, and hence are not rational, for example,

$$0.101001000100001\ldots$$

Familiar constants such as

$$\pi = 3.14159265358979323846264338327950288419 7\ldots$$

and

$$e = 2.71828182845904523536028747135266249775 7\ldots$$

are also irrational. In contrast, for famous constants such as Euler's constant[1]

$$\gamma = 0.57721566490153286060651209008240243104 2\ldots,$$

it is not even known whether the number is rational.

Beyond their natural appearance, what other reasons can we give to justify the necessity of non-rational (irrational) numbers? If the reader recalls their calculus courses, one of the central results of calculus is Bolzano's[2] theorem (the Intermediate Value Theorem). If we were to restrict ourselves to the rational numbers as the ambient space, calculus would lose Bolzano's theorem and, with it, many of its most useful consequences. Indeed, consider the function $f\colon \mathbb{Q} \to \mathbb{Q}$, $f(x) = x^2 - 2$. Although f takes both positive and negative values, it never attains the value 0, and therefore does not satisfy Bolzano's theorem

[1]Leonhard Euler, 1707–1783.

[2]Bernard Placidus Johann Nepomuk Bolzano, 1781–1848.

when viewed as a function defined on $\mathbb{Q}$. (Later, the reader will have the opportunity to verify that f is continuous on its domain and hence satisfies the hypotheses of Bolzano's theorem when considered in the appropriate setting.)

This issue is not merely technical. The availability of irrational numbers is essential for solving equations and for establishing existence results, which play a fundamental role in mathematical economics and, in particular, in the general equilibrium theory developed in this text.

E.2 Another ordered field

In previous sections we discussed how the integers can be constructed from the natural numbers, and how the rational numbers arise from the integers. The real numbers can then be obtained from the rational numbers by adding a *completeness* (or *completion*) axiom to the axioms of field and order (see Definitions C.2.1 and C.2.4 for the rationals). Even before knowing precisely what the axiom of completeness is, the existence of the real numbers can be formulated formally as follows.

Theorem E.2.1. *There exists a unique ordered field satisfying the axiom of completeness and containing $\mathbb{Q}$ as a subfield. We denote this field by $\mathbb{R}$.*

The proof of this theorem can be carried out using the so-called *Dedekind cuts*[3] or, alternatively, by considering equivalence classes of objects known as *Cauchy sequences*[4] of rational numbers. We will not present the proof here, but the interested reader may consult Rudin (1976, ch. 1) for the construction via Dedekind cuts, or Bridges (1998, App. A) for the construction using Cauchy sequences. For the reader seeking an even more exhaustive treatment, Weiss (2015) provides a comprehensive survey enumerating a wide variety of alternative constructions of the real numbers.

Understanding the axiom of completeness is of fundamental importance for mathematical analysis; without exaggeration, one may say that this axiom is what makes the difference of analysis as its own mathematical field.

The axiom of completeness admits several equivalent formulations. In these notes we shall present two of them: the *supremum axiom* and the *nested intervals principle*, and later we will show their equivalence. We follow the classical route and begin, in the next section, with the supremum axiom.

[3] Julius Wilhelm Richard Dedekind, 1831–1916.
[4] Augustin Louis Cauchy, 1789–1857.

E.3 Completeness of the real numbers

In what follows we use the standard notation for intervals of real numbers. If $a, b \in \mathbb{R}$, then $(a, b) := \{x \in \mathbb{R} : a < x < b\}$, $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$, $[a, b) := \{x \in \mathbb{R} : a \leq x < b\}$, $(a, \infty) := \{x \in \mathbb{R} : a < x\}$, $(-\infty, b) := \{x \in \mathbb{R} : x < b\}$, and so on.

Definition E.3.1. Let $A \subseteq \mathbb{R}$, $A \neq \emptyset$. We say that $a_0 \in \mathbb{R}$ is a *maximum* of A if:

a) $a_0 \in A$,

b) $a_0 \geq a$ for every $a \in A$.

Similarly, we say that $a_0 \in \mathbb{R}$ is a *minimum* of A if:

a) $a_0 \in A$, and

b) $a_0 \leq a$ for every $a \in A$.

Note that, if a maximum or a minimum of a set exists, it is necessarily unique. Some examples are

$$\max\{2, 3, 5, 7\} = 7, \qquad \max\{[0, 1]\} = 1, \qquad \max(-\infty, 0) \text{ does not exist.}$$

Example E.3.2. The interval $A = \{x \in \mathbb{R} : 0 < x < 1\}$ has neither a minimum nor a maximum. Indeed, suppose that $a_0 = \max(A)$. Then $0 < a_0$ and $a_0 \geq a$ for all $a \in A$. Consider the number $(1 + a_0)/2$. Then

$$0 < a_0 < \frac{1 + a_0}{2} < 1.$$

Hence $(1 + a_0)/2 \in A$, which contradicts the assumption that $a_0 = \max(A)$. Therefore A has no maximum. An analogous argument shows that A has no minimum.

Definition E.3.3. Let $A \subseteq \mathbb{R}$, $A \neq \emptyset$. We say that $a_0 \in \mathbb{R}$ is an *upper bound* of A if $a_0 \geq a$ for every $a \in A$, and a *lower bound* of A if $a_0 \leq a$ for every $a \in A$.

If A has an upper bound, we say that A is *bounded above.* If A has a lower bound, we say that A is *bounded below.* The set A is *bounded* if it is bounded both above and below.

Note that, unlike a maximum or a minimum, an upper or lower bound of a set does *not necessarily* belong to the set. For instance, 1 is an upper bound of the interval $(0, 1)$, which, as we know, has no maximum. However, if a set does have a maximum, then this number is also an upper bound of the set.

Note also that if a number is an upper bound of a set, then any larger number is automatically an upper bound as well. Guided by a natural principle of optimality, it is therefore reasonable to ask for the *smallest* upper bound of a set that is bounded above. The answer to this question is precisely the content of the following axiom.

Axiom **E.3.4** (Supremum). Let $A \subseteq \mathbb{R}$, $A \neq \emptyset$. If A is bounded above, then A has a least upper bound. That is, there exists $a_0 \in \mathbb{R}$ such that:

a) $a_0 \geq a$ for every $a \in A$ (that is, a_0 is an upper bound), and

b) if $b \geq a$ for every $a \in A$, then $b \geq a_0$ (that is, a_0 is the least upper bound).

We call a_0 the *supremum* of A and denote it by $\sup(A)$.

If A is the empty set, it is convenient to define $\sup(A) = -\infty$ (thinking of the fact that every real number is an upper bound of the empty set). An operational version of the supremum axiom is given below and is illustrated in figure E.1

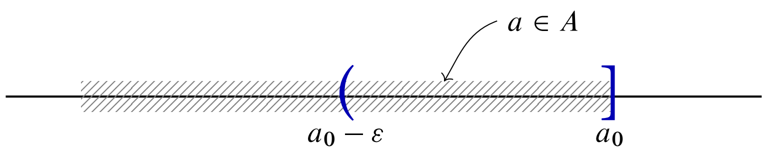


Figure E.1: Graphical illustration of theorem E.3.5

Theorem E.3.5. *Let $A \subseteq \mathbb{R}$, $A \neq \emptyset$. If A is bounded above, then for $a_0 \in \mathbb{R}$ the following statements are equivalent:*

a) $a_0 = \sup(A)$.

b) a_0 *is an upper bound of A and, for every $\varepsilon > 0$, there exists $a = a(\varepsilon) \in A$ such that*

$$a_0 - \varepsilon < a \leq a_0.$$

That is,

$$A \cap (a_0 - \varepsilon, a_0] \neq \emptyset$$

for every $\varepsilon > 0$.

Proof. a) $\Rightarrow$ b) Suppose first that $a_0 = \sup(A)$. By definition, a_0 is an upper bound of A. Let $\varepsilon > 0$. Since $a_0 - \varepsilon < a_0$, the number $a_0 - \varepsilon$ cannot be an upper bound of A. Hence there exists $a \in A$ such that

$$a_0 - \varepsilon < a \leq a_0.$$

b) $\Rightarrow$ a) For the converse implication, suppose that a_0 is not the least upper bound of A. Then there exists $b < a_0$ such that b is an upper bound of A. Let $\varepsilon = a_0 - b > 0$. By hypothesis, there exists $a \in A$ such that

$$a_0 - \varepsilon < a \leq a_0,$$

that is, $b < a \leq a_0$, which is impossible since b is an upper bound of A. Therefore a_0 is the least upper bound of A, and hence $a_0 = \sup(A)$. /ᐠ｡ꞈ｡ᐟ\

Example **E.3.6**. If $A \subseteq \mathbb{R}$ is finite and nonempty, then $\sup(A) = \max(A)$. More generally, if $\max(A) \in A$, then $\sup(A) = \max(A)$.

Example **E.3.7**. Let $A, B \subseteq \mathbb{R}$ be nonempty and bounded above. Define $A+B := \{a + b : a \in A,\ b \in B\}$. Then $\sup(A + B) = \sup(A) + \sup(B)$.

First observe that $A + B \neq \emptyset$ and that $A + B$ is bounded above by $\sup(A) + \sup(B)$, hence $\sup(A + B) \leq \sup(A) + \sup(B)$. Let $\varepsilon > 0$. We will show that there exists $a + b \in A + B$ such that

$$\sup(A) + \sup(B) - \varepsilon < a + b \leq \sup(A) + \sup(B).$$

Using Theorem E.3.5 with $\varepsilon/2$, choose $a \in A$ such that $\sup(A) - \frac{\varepsilon}{2} < a \leq \sup(A)$, and $b \in B$ such that $\sup(B) - \frac{\varepsilon}{2} < b \leq \sup(B)$. Adding the inequalities term by term yields $\sup(A) + \sup(B) - \varepsilon < a + b \leq \sup(A) + \sup(B)$. Therefore $\sup(A + B) = \sup(A) + \sup(B)$.

Example **E.3.8** (Iterated supremum principle). Let A, B be nonempty sets and let $h\colon A \times B \to \mathbb{R}$ be a bounded function; that is, there exists $M > 0$ such that $|h(x, y)| < M \quad$ for all $(x, y) \in A \times B$. Then

$$\sup\{h(x, y) : (x, y) \in A \times B\} = \sup\{g(x) : x \in A\} = \sup\{f(y) : y \in B\},$$

where $g(x) = \sup\{h(x, y) : y \in B\}$ and $f(y) = \sup\{h(x, y) : x \in A\}$.

Proof. Let $\alpha = \sup\{h(x, y) : (x, y) \in A \times B\}$. We show that $\sup\{g(x) : x \in A\} = \alpha$. Clearly, $\sup\{g(x) : x \in A\} \leq \alpha$, since for any fixed $x' \in A$,

$$g(x') = \sup\{h(x', y) : y \in B\} \leq \sup\{h(x, y) : (x, y) \in A \times B\} = \alpha,$$

which exhibits α as an upper bound of $\{g(x) : x \in A\}$.

Suppose, by contradiction, that $\sup\{g(x) : x \in A\} < \alpha$. Since $\alpha = \sup\{h(x, y) : (x, y) \in A \times B\}$, there exists $(x_0, y_0) \in A \times B$ such that

$$\sup\{g(x) : x \in A\} < h(x_0, y_0) \leq \alpha.$$

But since $g(x_0) = \sup\{h(x_0, y) : y \in B\}$, it follows that $h(x_0, y_0) \leq g(x_0)$. Hence

$$h(x_0, y_0) \leq g(x_0) \leq \sup\{g(x) : x \in A\} < h(x_0, y_0),$$

which is impossible. Therefore $\sup\{g(x) : x \in A\} = \alpha$.

An analogous argument shows that $\alpha = \sup\{f(y) : y \in B\}$.

Note that, in order to verify that a given number is the supremum of a set, Theorem E.3.5 requires finding elements of the set that are arbitrarily close to the candidate supremum (thinking, as always, of ε as being small). The next section is devoted to an important property of the real numbers that allows, among other things, the construction of arbitrarily small numbers starting from the natural numbers.

Parallel to the notion of the supremum of a set as its least upper bound, if a set is bounded below it should possess a *greatest lower bound*. This indeed exists and is known as the *infimum* of the set. Its existence can be deduced from the supremum axiom as follows.

Proposition E.3.9. *Let $A \subseteq \mathbb{R}$, $A \neq \emptyset$. If A is bounded below, then A has a unique greatest lower bound, denoted by* $\inf(A)$. *In other words, there exists $c \in \mathbb{R}$ such that c is a lower bound of A and for every $\varepsilon > 0$ there exists $a \in A$ such that*

$$c \leq a < c + \varepsilon.$$

Proof. Consider the set $-A := \{-a : a \in A\}$. Clearly $-A$ is bounded above. Let $b = \sup(-A)$. We claim that $c := -b$ is the greatest lower bound of A. Indeed, since $b \geq -a$ for every $a \in A$, it follows that $a \geq -b$ for every $a \in A$, and hence $-b$ is a lower bound of A. Now let $\varepsilon > 0$. Since $b = \sup(-A)$, there exists $-a \in -A$ such that $b - \varepsilon < -a \leq b$, from which it follows that $-b < a \leq -b + \varepsilon$, as desired.

Note that the previous proposition, in particular, implies that

$$\inf(A) = -\sup(-A).$$

Exercise E.3.A. Let $B \subseteq \mathbb{R}$ be bounded above. Prove:

a) If $\alpha = \sup(B)$ and $\alpha \in B$, then $\alpha = \max(B)$.

b) If $A \subseteq B$, then A is bounded above and $\sup(A) \leq \sup(B)$.

Exercise E.3.B. Let $A = (0, 1)$. Prove:

a) $\{a \in \mathbb{R} : a \text{ is an upper bound of } A\} = [1, \infty)$.

b) $\{b \in \mathbb{R} : b \text{ is a lower bound of } A\} = (-\infty, 0]$.

c) $\sup(A) = 1$.

d) $\inf(A) = 0$.

Exercise E.3.C. Let $A \subseteq \mathbb{R}$ be bounded above. Prove that $\beta = \sup(A)$ if and only if

$$\{a \in \mathbb{R} : a \text{ is an upper bound of } A\} = [\beta, \infty).$$

Exercise E.3.D. Prove that if S is a nonempty bounded subset of $\mathbb{R}$ and $a < 0$, then

$$\sup(a \cdot S) = a \inf(S)$$

and

$$\inf(a \cdot S) = a \sup(S).$$

Exercise E.3.E. Find the supremum and the infimum of the following sets. If they do not exist, indicate so and justify your answer.

a) $(0, 1) \setminus \mathbb{Q}$.

b) $\{x + 1/x \in \mathbb{R} : x > 0\}$.

c) $\left\{\frac{x}{x+y} \in \mathbb{R} : x, y > 0\right\}$.

d) $\left\{\frac{1}{x} - \frac{1}{y} \in \mathbb{R} : x, y \geq 1\right\}$.

e) $\{x \in \mathbb{R} : x^2 < x + 1\}$.

Exercise E.3.F. In the following items, A and B are bounded subsets of positive real numbers. Prove:

a) If $A + 1 := \{a + 1 : a \in A\}$, then $\sup(A + 1) = \sup(A) + 1$.

b) If $A \cdot B := \{ab : a \in A,\ b \in B\}$, then $\sup(A \cdot B) = \sup(A)\sup(B)$.

c) If $A^{-1} := \{1/a : a \in A\}$, then $\sup(A^{-1}) = 1/\inf(A)$.

Exercise E.3.G. Let $f, g\colon A \subseteq \mathbb{R} \to \mathbb{R}$ be bounded functions; that is, $|f(x)|, |g(x)| \leq M$ for some $M > 0$ and for every $x \in A$. Consider the numbers

a) $\alpha = \inf\{f(x) : x \in A\} + \inf\{g(x) : x \in A\}$,

b) $\beta = \inf\{f(x) + g(x) : x \in A\}$,

c) $\gamma = \inf\{f(x) : x \in A\} + \sup\{g(x) : x \in A\}$,

d) $\delta = \sup\{f(x) + g(x) : x \in A\}$,

e) $\varepsilon = \sup\{f(x) : x \in A\} + \sup\{g(x) : x \in A\}$.

Prove that $\alpha \leq \beta \leq \gamma \leq \delta \leq \varepsilon$ and give examples where the inequalities above are strict.

Exercise E.3.H.🐾 (Min–max principle.) Let A, B be nonempty sets and let $u\colon A \times B \to \mathbb{R}$ be a bounded function; that is, there exists $M > 0$ such that $|u(a, b)| \leq M$ for all $(a, b) \in A \times B$. Prove the min–max principle:

$$\sup_{a \in A} \left(\inf_{b \in B} u(a, b) \right) \leq \inf_{b \in B} \left(\sup_{a \in A} u(a, b) \right).$$

Exhibit examples where the inequality is strict.

Remark **E.3.10**. The min–max principle admits a natural interpretation in terms of a two-player zero-sum game. Player I chooses an action $a \in A$, Player II chooses an action $b \in B$, and the payoff to Player I is given by $u(a, b)$, with Player II receiving $-u(a, b)$. Denote

$$\begin{aligned} \underline{v} &= \sup_{a \in A} \inf_{b \in B} u(a, b) \\ \overline{v} &= \inf_{a \in A} \sup_{b \in B} u(a, b) \end{aligned}$$

The value $\underline{v}$ is called the *maximin value* of the game, and $\overline{v}$ is called the *minmax value.* Player I can guarantee that he will get at least $\underline{v}$, and Player II can guarantee that she will pay no more than $\overline{v}$. The inequality in the min–max principle states that, in general, these two values need not coincide, reflecting the possible absence of a saddle point in pure strategies. The *Minimax Theorem* of von Neumann[5], from 1928, identifies conditions under which the min-max inequality holds with equality. When it does, the zero-sum game is said to have a *value.*

[5] John von Neumann, 1903–1957,

Exercise E.3.I. Let $A \subseteq (0, \infty)$. Prove that A is not bounded above if and only if $\inf(A^{-1}) = 0$.

Exercise E.3.J. Let A be a set that is bounded above and satisfies $\inf(A) > 0$. Define

$$B = \left\{ \frac{x}{y} \in \mathbb{R} : x, y \in A \right\}.$$

Prove that

$$\sup(B) = \frac{\sup(A)}{\inf(A)}, \qquad \inf(B) = \frac{\inf(A)}{\sup(A)}.$$

Exercise E.3.K. Let $A \subseteq (0, \infty)$ be a set that is not bounded above. Define

$$B = \left\{ \frac{x}{1 + x^2} \in \mathbb{R} : x \in A \right\}.$$

a) Prove that

$$B = \left\{ \frac{x}{1 + x^2} \in \mathbb{R} : x \in A^{-1} \right\}.$$

b) Prove that $\inf(B) = 0$.

We finish this section by defining the extended real number system.

***Definition* E.3.11.** The *extended real number system* consists of the real number system, $\mathbb{R}$, to which we add two symbols, $+\infty$ and $-\infty$, i.e.,

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}.$$

The order is extended by declaring

$$-\infty < x < +\infty \quad \text{for every } x \in \mathbb{R}.$$

The following arithmetic rules are satisfied:

a) If $x \in \mathbb{R}$, then

$$x + \infty = +\infty, \qquad x + (-\infty) = -\infty, \qquad \frac{x}{+\infty} = \frac{x}{-\infty} = 0.$$

b) If $x > 0$, then

$$x \cdot (+\infty) = +\infty, \qquad x \cdot (-\infty) = -\infty.$$

c) If $x < 0$, then

$$x \cdot (+\infty) = -\infty, \qquad x \cdot (-\infty) = +\infty.$$

Arithmetic expressions involving indeterminate forms such as

$$+\infty - \infty, \qquad 0 \cdot (\pm\infty), \qquad \frac{\infty}{\infty}$$

are left undefined.

Definition **E.3.12**. Let $E \subseteq \overline{\mathbb{R}}$. If E is not bounded above in $\mathbb{R}$, that is, if for every real number y there exists $x \in E$ such that $x > y$, then we define

$$\sup E := +\infty.$$

Similarly, if E is not bounded below in $\mathbb{R}$, that is, if for every real number y there exists $x \in E$ such that $x < y$, then we define

$$\inf E := -\infty.$$

Remark **E.3.13**. In the extended real number system, every subset of $\overline{\mathbb{R}}$ has a supremum and an infimum. This is the principal reason for adjoining the symbols $+\infty$ and $-\infty$.

E.4 The Archimedean property of $\mathbb{R}$

Theorem E.4.1 (Archimedean property). *If $x \in \mathbb{R}$, then there exists $n \in \mathbb{N}$ such that $n > x$.*[6]

Proof. Suppose, by contradiction, that $n \leq x$ for every $n \in \mathbb{N}$; that is, $\mathbb{N}$ is bounded above. Let $\alpha = \sup(\mathbb{N})$. Then, for $\varepsilon = 1$, there exists $n_0 \in \mathbb{N}$ such that

$$\alpha - 1 < n_0 \leq \alpha.$$

Adding 1 to each side of the inequality yields $\alpha < n_0 + 1$. Since $n_0 + 1 \in \mathbb{N}$, the inequality above shows that α is not an upper bound of $\mathbb{N}$, contradicting the definition of α. ^. .^)9

Although we used the supremum axiom to derive the Archimedean property, it is worth noting that there exist ordered fields that satisfy the Archimedean property but not the supremum axiom; for instance, the field of rational numbers. Observe that the Archimedean property merely asserts that $\mathbb{N}$, viewed as a subset of $\mathbb{R}$, is not bounded above. This fact, together with several results established in previous sections, implies the following corollary.

[6] Archimedes of Syracuse, 287–212 BCE

Corollary E.4.2. *Let $S \subseteq \mathbb{N}$ be a nonempty set. Then the following statements are equivalent:*

a) *S is an infinite set.*

b) *S is not bounded above.*

c) $\inf(S^{-1}) = 0$.

Exercise E.4.A.🐾 Prove corollary E.4.2

We now present some reformulations of the Archimedean property that will be of great use. The first item of Corollary E.4.3 is the formulation historically known as the Archimedean property (a sufficiently large sum of segments of arbitrarily small length exceeds the length of a given segment). The most useful version of the Archimedean property is the second item of Corollary E.4.3.

Corollary E.4.3. *If x, y are positive real numbers, then:*

a) *there exists $n \in \mathbb{N}$ such that $y < nx$,*

b) *there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n}x < y$,*

c) *there exists $n \in \mathbb{N}$ such that $n - 1 \leq x < n$.*

Proof. By the Archimedean property, there exists $n \in \mathbb{N}$ such that $\frac{y}{x} < n$. Hence $y < nx$.

Again by the Archimedean property, there exists $n \in \mathbb{N}$ such that $0 < \frac{x}{y} < n$. Thus $0 < \frac{1}{n}x < y$.

Next, by the Archimedean property, choose $m \in \mathbb{N}$ such that $x < m$. Then the set $E = \{k \in \mathbb{N} : x < k\}$ is nonempty. By the well-ordering principle C.1.6, the set E has a least element; denote it by n. Since n is the least element of E, we have $n - 1 \notin E$, hence $n - 1 \leq x$, and therefore $n - 1 \leq x < n$, as desired. /ᐠ｡ꞈ｡ᐟ\

Exercise E.4.B.🐾 Prove that each of the items in corollary E.4.3 is equivalent to the Archimedean property as stated in theorem E.4.1.

Some properties of the real numbers illustrating the usefulness of the Archimedean property are given below.

Example **E.4.4.** If $A = (0, 1)$, then $\sup(A) = 1$. Clearly, 1 is an upper bound of A. Let $\varepsilon > 0$. By the Archimedean property (Corollary E.4.3), there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < \varepsilon$. We may assume $n > 1$, and then $a = 1 - \frac{1}{n}$ satisfies $1 - \varepsilon < 1 - \frac{1}{n} < 1$, so $a \in (0, 1)$, as required.

Proposition E.4.5 (Density of $\mathbb{Q}$ on $\mathbb{R}$). *If $x, y \in \mathbb{R}$ with $0 < x < y$, then there exists $r \in \mathbb{Q}$ such that $x < r < y$.*

Proof. Let $x, y \in \mathbb{R}$ with $0 < x < y$. By the Archimedean property, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < y - x$. We seek $m \in \mathbb{N}$ such that $x < \frac{m}{n} < y$. Again by the Archimedean property, there exists $k \in \mathbb{N}$ such that $nx < k$. Define $A = \{k \in \mathbb{N} : nx < k\}$. Then $A \neq \emptyset$, and by the well-ordering principle it has a least element, denote it by m. Hence

$$nx < m, \quad \text{or equivalently} \quad x < \frac{m}{n}.$$

It remains to show that $\frac{m}{n} < y$. Suppose, to the contrary, that $y \leq \frac{m}{n}$. Then

$$\frac{1}{n} < y - x \leq \frac{m}{n} - \frac{m-1}{n} = \frac{1}{n},$$

since $\frac{m-1}{n} < x < \frac{m}{n}$ and m is the least element of A. This is a contradiction. Therefore $\frac{m}{n} < y$, and hence $x < \frac{m}{n} < y$, as required. ^. .^)9

Remark **E.4.6**. The preceding result is known as the *density of the rational numbers in the real numbers*. In fact, it is equivalent to the following statement: if $a < b$, then $(a, b) \cap \mathbb{Q} \neq \emptyset$.

Exercise E.4.C. State and prove a proposition equivalent to Proposition E.4.5 when the given real numbers are not necessarily positive.

As a consequence of the supremum axiom and the Archimedean property, we can now prove the existence of the number $\sqrt{2}$.

Proposition E.4.7. *There exists $x \in \mathbb{R}$ such that $x^2 = 2$.*

Proof. Let

$$A = \{x \in \mathbb{R} : x^2 < 2 \text{ and } x > 0\}.$$

The set A is nonempty since $1 \in A$. Moreover, A is bounded above because $x \leq 2$ for every $x \in A$. Indeed, if $x > 2$ for some $x \in A$, then $x^2 > 4$, which is impossible. By the supremum axiom, there exists $x_0 = \sup(A)$. We will show that $x_0^2 = 2$. By trichotomy, it suffices to show that the cases $x_0^2 < 2$ and $x_0^2 > 2$ are impossible.

Suppose first that $x_0^2 < 2$. The idea is to show that this strict inequality allows a small perturbation: we will find a number slightly larger than x_0 that still belongs to A, which is impossible if x_0 is the supremum of A. Choose $n \in \mathbb{N}$ such that

$$x_0^2 \left(1 + \frac{3}{n}\right) < 2.$$

(Such an n exists by the Archimedean property.) We claim that $x_0\left(1+\frac{1}{n}\right) \in A$. Indeed,

$$\left(x_0\left(1+\frac{1}{n}\right)\right)^2 = x_0^2\left(1+\frac{2}{n}+\frac{1}{n^2}\right) < x_0^2\left(1+\frac{2}{n}+\frac{1}{n}\right) = x_0^2\left(1+\frac{3}{n}\right) < 2.$$

This yields a contradiction, since $x_0\left(1+\frac{1}{n}\right) \in A$ and $x_0\left(1+\frac{1}{n}\right) > x_0 = \sup(A)$. Hence x_0^2 cannot be less than 2.

Now suppose that $x_0^2 > 2$. Choose $n \in \mathbb{N}$ such that

$$x_0^2\left(1-\frac{2}{n}\right) > 2.$$

(Again, such an n exists by the Archimedean property.) Observe that

$$\left(x_0\left(1-\frac{1}{n}\right)\right)^2 = x_0^2\left(1-\frac{1}{n}\right)^2 = x_0^2\left(1-\frac{2}{n}+\frac{1}{n^2}\right) > x_0^2\left(1-\frac{2}{n}\right) > 2.$$

Since $x_0\left(1-\frac{1}{n}\right) < x_0 = \sup(A)$, there exists $\tilde{x} \in A$ such that

$$x_0\left(1-\frac{1}{n}\right) < \tilde{x} \leq x_0.$$

Then

$$2 < \left(x_0\left(1-\frac{1}{n}\right)\right)^2 < \tilde{x}^2 \leq x_0^2 < 2,$$

which is a contradiction. Therefore x_0^2 cannot be greater than 2.

We conclude that $x_0^2 = 2$. Hence $\sqrt{2}$ exists. /ᐢ。ᐞ。ᐢ\

***Joke* E.4.8.** We have therefore exhibited an irrational number. After some effort, at least one such beast has been secured. Cheers to us!

Let us show next that irrational numbers are ubiquitous. We begin by stating the following elementary arithmetic lemma.

Lemma E.4.9. *Let $r \in \mathbb{Q}$ and let $\xi, \zeta \in \mathbb{R} \setminus \mathbb{Q}$. Then:*

a) If $r \neq 0$, then $r\xi \in \mathbb{R} \setminus \mathbb{Q}$.

b) $r + \xi \in \mathbb{R} \setminus \mathbb{Q}$.

c) The product $\xi \cdot \zeta$ may be rational or irrational.

d) The sum $\xi + \zeta$ may be rational or irrational.

Exercise E.4.D. Prove lemma E.4.9

Proposition E.4.10 (Density of $\mathbb{R} \setminus \mathbb{Q}$ in $\mathbb{R}$). *The set $\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$; that is, for all $x, y \in \mathbb{R}$ with $x < y$, there exists $\xi \in \mathbb{R} \setminus \mathbb{Q}$ such that $x < \xi < y$.*

Proof. Consider the interval $(\sqrt{2}x, \sqrt{2}y)$. Since the rational numbers are dense in $\mathbb{R}$, there exists $r \in \mathbb{Q}$ such that $\sqrt{2}x < r < \sqrt{2}y$. Then $x < \frac{r}{\sqrt{2}} < y$. If $r \neq 0$, then $\frac{r}{\sqrt{2}}$ is irrational, and we have found the desired number. If $r = 0$, then there exists $s \in \mathbb{Q}$ such that $0 < s < \sqrt{2}y$. Hence $\sqrt{2}x < s < \sqrt{2}y$, which implies $x < \frac{s}{\sqrt{2}} < y$, and since $\frac{s}{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$, the conclusion follows. ^. .^)9

Exercise E.4.E. Prove that for every $x > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{2^n} < x$.

Exercise E.4.F. Prove the following:

a) $\inf\left\{\frac{1}{n} - \frac{1}{m} \in \mathbb{R} : n, m \in \mathbb{N}\right\} = -1$.

b) $\sup\left\{\frac{1}{n} - \frac{1}{m} \in \mathbb{R} : n, m \in \mathbb{N}\right\} = 1$.

c) $\inf\left\{\frac{m}{m+n} \in \mathbb{R} : m, n \in \mathbb{N}\right\} = 0$.

d) $\inf\left\{\frac{1}{n!} \in \mathbb{R} : n \in \mathbb{N}\right\} = 0$.

Exercise E.4.G. Let $c < 0$. For each $n \in \mathbb{N}$, let $u_n \in \mathbb{R}$ satisfy $0 \leq u_n < \frac{c}{2^n}$. Prove that $\inf\{u_n : n \in \mathbb{N}\} = 0$.

Exercise E.4.H. Prove that $\inf\left\{\frac{2^n}{n!} \in \mathbb{R} : n \in \mathbb{N}\right\} = 0$.

E.5 Nested intervals principle

One of the great theorems of calculus, Bolzano's theorem (the Intermediate Value Theorem), states that if a continuous function $f\colon [a, b] \to \mathbb{R}$ takes two values of opposite sign, then there exists $c \in [a, b]$ such that $f(c) = 0$. What the theorem does not say is where the point c is located.

To approximate c, one proceeds by trial and error, constructing a sequence of nested intervals

$$[a, b] \supset [a_1, b_1] \supset [a_2, b_2] \supset [a_3, b_3] \supset \cdots$$

in such a way that the value of f at the endpoints of each interval has opposite sign,

$$f(a_n)\,f(b_n) < 0.$$

The process can be continued until the limit of our patience—or the precision of the computer—allows, yielding a good approximation of the value of c. The guarantee provided by the *nested intervals principle* is that, if we could continue the construction indefinitely, then there would be a point common to all these intervals; that is,

$$\bigcap_{n=1}^{\infty}[a_n, b_n] \neq \emptyset.$$

Although this may appear obvious, the nested intervals principle[7] is rather subtle: not every intersection of nested intervals is nonempty. For example:

Example **E.5.1**. Let $I_n = (0, 1/n]$, $n \in \mathbb{N}$. Then

$$\bigcap_{n\in\mathbb{N}} I_n = \{x \in \mathbb{R} : 0 < x \leq 1/n \text{ for all } n \in \mathbb{N}\} = \emptyset.$$

The principle is also false if the intervals are not bounded, for instance, if $I_n = [n, \infty)$ then $\bigcap_{n\in\mathbb{N}} I_n = \emptyset$. This points to the fact that the intervals must then be closed and bounded intervals.

Theorem E.5.2 (Principle of Nested Intervals). *Let $I_n = [a_n, b_n]$, $n \in \mathbb{N}$, be a sequence of closed and bounded intervals in $\mathbb{R}$ such that*

$$[a_{n+1}, b_{n+1}] \subseteq [a_n, b_n] \quad \textit{for all } n \in \mathbb{N}.$$

Then

$$\bigcap_{n\in\mathbb{N}} I_n \neq \emptyset.$$

Proof. First, we show that for each $m \in \mathbb{N}$, the number b_m is an upper bound for the set of left endpoints $\{a_n : n \in \mathbb{N}\}$. Let $n \in \mathbb{N}$. If $n \leq m$, then $b_m \geq a_m \geq a_n$, and if $n > m$, then $b_m \geq b_n \geq a_n$. Hence $b_m \geq a_n$ for all $n \in \mathbb{N}$.

Therefore, the supremum $\alpha := \sup\{a_n : n \in \mathbb{N}\}$ exists and satisfies $\alpha \leq b_m$ for every $m \in \mathbb{N}$. In particular, the set of right endpoints $\{b_m : m \in \mathbb{N}\}$ is bounded below by α. Hence $\beta := \inf\{b_m : m \in \mathbb{N}\}$ exists and satisfies $\beta \geq \alpha$.

[7] This result is often referred to as *Cantor's Intersection Theorem.* In these notes, we adopt a more precise terminology: we reserve that name for the general version formulated in metric spaces (see Chapter 1) and refer to the present, real-line case as the *nested intervals principle.*

We claim that

$$[\alpha, \beta] \subseteq \bigcap_{n=1}^{\infty} I_n.$$

Indeed, let $x \in [\alpha, \beta]$ and let $n \in \mathbb{N}$. Since $a_n \leq \alpha \leq x \leq \beta \leq b_n$, it follows that $x \in [a_n, b_n] = I_n$. Hence $x \in \bigcap_{n \in \mathbb{N}} I_n$, which proves the claim and completes the proof. ^. .^)9

Remark E.5.3. From the proof we see that the intersection is not only nonempty: it may consist of a single point (when $\alpha = \beta$) or of an uncountable set, i.e., an interval.

Remark E.5.4. The proof of the principle of nested intervals relies on the axiom of completeness (the supremum axiom) for the real numbers. Conversely, it is not difficult to show that the supremum axiom can be derived from the principle of nested intervals together with the Archimedean property.

Exercise E.5.A. Prove that, in the principle of nested intervals E.5.2, the intersection of the intervals consists of a single point if and only if $\inf\{b_n - a_n : n \in \mathbb{N}\} = 0$, that is, if and only if the lengths of the intervals converge to zero.

Exercise E.5.B. Let $0 < a_1 < b_1$ be two distinct positive numbers. Define recursively $b_{n+1} = \frac{1}{2}(a_n + b_n)$ and $a_{n+1} = \sqrt{a_n b_n}$. Prove the following:

a) $0 < a_n < b_n$ for all $n \in \mathbb{N}$.

b) If $I_n = [a_n, b_n]$, then (I_n) is a sequence of nested intervals, that is, $I_{n+1} \subseteq I_n$.

c) $b_n - a_n < (b_1 - a_1)/2^{n-1}$ for all $n \in \mathbb{N}$.

d) The intersection $\bigcap_{n=1}^{\infty} I_n$ consists of a single point.

Exercise E.5.C. We now give another proof of the existence of a real number $x_0 \in \mathbb{R}$ such that $x_0^2 = 2$. Let $g\colon (0, \infty) \to \mathbb{R}$ be defined by

$$g(x) = \frac{2x + 2}{x + 2}.$$

Let $a_1 = 1$ and $b_1 = 2$, and define recursively $a_{n+1} = g(a_n), b_{n+1} = g(b_n)$. Prove the following:

a) If $0 < x < y$, then $0 < g(x) < g(y)$. Conclude that $0 < a_n < b_n$ for all $n \in \mathbb{N}$.

b) $[a_{n+1}, b_{n+1}] = g([a_n, b_n])$.

c) $a_n^2 < 2$ and $a_n < a_{n+1}$. (*Suggestion*: prove by induction.)

d) $b_n^2 > 2$ and $b_{n+1} < b_n$. Conclude that $[a_n, b_n]$ is a sequence of nested intervals.

e) $b_n - a_n < 3/2^n$ for all $n \in \mathbb{N}$.

f) The intersection of the intervals consists of a single point, that is,

$$\bigcap_{n=1}^{\infty} [a_n, b_n] = \{x_0\}.$$

g) The point x_0 satisfies $g(x_0) = x_0$. Conclude that $x_0^2 = 2$.

Exercise E.5.D. Let $I_n = [a_n, b_n]$, $n \in \mathbb{N}$, be a sequence of closed and bounded intervals in $\mathbb{R}$ such that $[a_{n+1}, b_{n+1}] \subseteq [a_n, b_n]$ for all $n \in \mathbb{N}$. Let $\alpha = \sup\{a_n : n \in \mathbb{N}\}$ and $\beta = \inf\{b_n : n \in \mathbb{N}\}$. In the proof of the nested intervals principle E.5.2, the inclusion

$$[\alpha, \beta] \subseteq \bigcap_{n=1}^{\infty} I_n$$

was established. Prove the equality $[\alpha, \beta] = \bigcap_{n=1}^{\infty} I_n$. (Suggestion: consider Theorem E.3.5.)

Exercise E.5.E. Use the principle of nested intervals E.5.2 to show that the interval $[0, 1]$ is uncountable. *Suggestion:* Suppose that $[0, 1]$ is countable. Then there exists a function $f : \mathbb{N} \to [0, 1]$. Let $x_n := f(n)$. First choose an interval of length $1/3$ that does not contain x_1. Next, choose an interval contained in the previous one, of length $1/9$, that does not contain x_2. Continue inductively.

Exercise E.5.F. Prove that if $0 < \varepsilon < 1$, then $(1 + \varepsilon)^n \leq 1 + 3^n \varepsilon$ for all $n \in \mathbb{N}$.

Exercise E.5.G. (n-th Roots.) Let $a > 0$ be a real number and let $n \in \mathbb{N}$. Prove that there exists $x_0 \in \mathbb{R}$ such that $x_0^n = a$, called the *n-th root of a*. *Suggestion:* See Exercise E.5.F. Consider the set $A = \{x \in \mathbb{R} : x > 0,\ x^n < a\}$, and show that $x_0 = \sup(A)$ exists. Proceed as in the proof of Proposition E.4.7, ruling out the cases $x_0^n < a$ and $x_0^n > a$ by considering

$$y = x_0(1 + \varepsilon), \qquad 0 < \varepsilon < \frac{a - x_0^n}{3^n x_0^n} \quad \text{if } x_0^n < a,$$

and
$$y = \frac{x_0}{1+\varepsilon}, \qquad 0 < \varepsilon < \min\left\{1, \frac{x_0^n - a}{3^n a}\right\} \quad \text{if } x_0^n > a.$$

Exercise E.5.H. Prove that if $0 < t < 1$, then $t^n < t$ for all $n \in \mathbb{N}$, and that if $t \geq 1$, then $t^n \geq t$ for all $n \in \mathbb{N}$. Prove that $0 < a < b$ if and only if $a^{1/n} < b^{1/n}$.

Exercise E.5.I. (Rules of exponents.) Let $a \in \mathbb{R} \setminus \{0\}$. Define $a^0 = 1$, $a^1 = a$, and inductively $a^{n+1} = a \cdot a^n, n \in \mathbb{N}$. Prove by induction the following rules of exponents:

a) $a^n a^m = a^{n+m}$ for $a \in \mathbb{R}, n, m \in \mathbb{N}$.

b) $a^n b^n = (ab)^n$ for $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$.

c) $(a^n)^m = a^{nm}$ for $a \in \mathbb{R}, n, m \in \mathbb{N}$.

Exercise E.5.J. Let $n \in \mathbb{Z}$ and $a \in \mathbb{R} \setminus \{0\}$. Define
$$a^n = \begin{cases} a^n, & n \geq 0, \\ \dfrac{1}{a^{-n}}, & n < 0. \end{cases}$$

State and prove the exponent rules analogous to those of Exercise E.5.I for integer exponents.

Exercise E.5.K. Let $a > 0$ be a real number and let $n \in \mathbb{N}$. Denote the n-th root of a by $a^{1/n}$ (see Exercise E.5.G) and define, for $r = p/q \in \mathbb{Q}$, $a^r = (a^{1/q})^p$. State and prove the exponent rules analogous to those of Exercise E.5.I for rational exponents. Discuss possible extensions to real exponents that are not necessarily positive.

Exercise E.5.L.🐾 Let $a > 0$ be a real number and let $r \in \mathbb{R}$. Define
$$a^r = \sup\{a^q : q \in \mathbb{Q},\ q \leq r\}.$$

Prove that a^r is well defined (that is, the supremum exists) and state and prove the exponent rules analogous to those of Exercise E.5.I for real exponents.

Appendix F

Vector Spaces

The fact that the commodity space has the structure of a real vector space is a basic reason for the success of mathematization of Economic Theory.

Gerard Debreu, *Nobel Memorial Lecture*

F.1 Vector Spaces

We begin with the definition of the principal object of study in this appendix.

***Definition* F.1.1** (Vector space). Let F be a field, whose elements are referred to as *scalars.* A *vector space* over F is a nonempty set V, whose elements are referred to as *vectors*, together with two operations. The first operation, called *addition* and denoted by $+$, assigns to each pair (u, v) of vectors in V a vector $u + v$ in V. The second operation, called *scalar multiplication* and denoted by juxtaposition, assigns to each pair $(r, u) \in \mathsf{F} \times V$ a vector ru in V. Furthermore, the following properties must be satisfied:

a) For all $u, v, w \in V$,
$$u + (v + w) = (u + v) + w.$$
(associativity of addition)

b) For all $u, v \in V$,
$$u + v = v + u.$$
(commutativity of addition)

c) There exists an element $0 \in V$ such that
$$u + 0 = 0 + u = u \quad \text{for all } u \in V.$$
(existence of a zero vector)

d) For each $u \in V$ there exists an element $-u \in V$ such that

$$u + (-u) = (-u) + u = 0.$$

(existence of additive inverses)

(V5) For all $a, b \in \mathsf{F}$ and all $u, v \in V$,

$$\begin{aligned} a(u+v) &= au + av, \\ (a+b)u &= au + bu, \\ (ab)u &= a(bu), \\ 1u &= u. \end{aligned}$$

(properties of scalar multiplication)

Remark **F.1.2**. A vector space over a field F is sometimes called an F-*space*. A vector space over $\mathbb{R}$ is called a *real vector space*, and a vector space over the field of complex numbers is called a *complex vector space*. Unless stated otherwise, all vector spaces considered in this text are real vector spaces.

Definition **F.1.3** (Linear combination). Let V be a vector space over F, and let $S \subseteq V$ be a nonempty subset. A *linear combination* of vectors in S is an expression of the form

$$a_1 v_1 + \cdots + a_n v_n,$$

where $v_1, \ldots, v_n \in S$ and $a_1, \ldots, a_n \in \mathsf{F}$. The scalars $a_1, \ldots, a_n$ are called the *coefficients* of the linear combination. The linear combination is said to be *trivial* if $a_i = 0$ for all $i = 1, \ldots, n$, and *nontrivial* otherwise.

Below are a few examples of vector spaces.

Example **F.1.4**. Let F be a field. The set F^{F} of all functions from F to F is a vector space over F, under the operations of ordinary addition and scalar multiplication of functions, defined by

$$(f+g)(x) = f(x) + g(x)$$

and

$$(af)(x) = af(x).$$

Example **F.1.5**. The set $\mathcal{M}_{m,n}(\mathsf{F})$ of all $m \times n$ matrices with entries in a field F is a vector space over F, under the operations of matrix addition and scalar multiplication.

***Example* F.1.6.** The set F^n of all ordered n-tuples whose components lie in a field F is a vector space over F, with addition and scalar multiplication defined component-wise:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

and

$$c(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n).$$

When convenient, we will also write the elements of F^n in column form.

***Example* F.1.7.** Many sequence spaces are vector spaces. The set $\mathsf{F}^{\mathbb{N}}$ of all infinite sequences with members from a field F is a vector space under the component-wise operations

$$(s_n) + (t_n) = (s_n + t_n)$$

and

$$a(s_n) = (as_n).$$

Exercise F.1.A. Let (V, F) be a vector space. Prove that for every $v \in V$,

$$-(-v) = v.$$

Exercise F.1.B. Explain why the empty set cannot be a vector space. Identify precisely which axiom in the definition of a vector space fails.

Exercise F.1.C. Show that in the definition of a vector space, the additive inverse axiom can be replaced by the condition

$$0v = 0 \quad \text{for all } v \in V,$$

where 0 on the left denotes the scalar zero in F and 0 on the right denotes the zero vector.

Exercise F.1.D. Let (V, F) be a vector space. Prove that for every $v \in V$,

$$(-1)v = -v.$$

Exercise F.1.E. Let (V, F) be a vector space and let $u, v \in V$. Show that if

$$u + v = u,$$

then $v = 0$.

Exercise F.1.F. Let (V, F) be a vector space and $v \in V$. Suppose that

$$av = bv$$

for some $a, b \in \mathsf{F}$. Show that if $v \neq 0$, then $a = b$.

Exercise F.1.G. Let (V, F) be a vector space and let $S \subseteq V$. Show that the set of all linear combinations of vectors in S is closed under addition and scalar multiplication.

Exercise F.1.H. Let (V, F) be a vector space and let S be a set. Denote by V^S the set of all functions from S to V. Define addition and scalar multiplication on V^S by

$$(f+g)(s) = f(s) + g(s) \quad \text{and} \quad (af)(s) = af(s),$$

for all $f, g \in V^S$, all $a \in \mathsf{F}$, and all $s \in S$. Show that V^S is a vector space over F.

F.2 Subspaces

Most algebraic structures contain substructures, and vector spaces are no exception.

Definition F.2.1. A *subspace* of a vector space V is a subset $S \subseteq V$ that is itself a vector space under the operations obtained by restricting the operations of V to S. We say that S is a *proper subspace* of V if $S \subsetneq V$, i.e., $S \subseteq V$, and $S \neq V$. The *zero subspace* of V is $\{0\}$.

Since many of the properties of addition and scalar multiplication hold *a fortiori* for any nonempty subset $S \subseteq V$, it is often sufficient to verify that S is closed under the operations of V in order to establish that S is a subspace.

Theorem F.2.2 (Subspace Criterion). *A nonempty subset $S \subset V$ of a vector space V is a subspace of V if and only if S is closed under addition and scalar multiplication. Equivalently, S is a subspace of V if and only if it is closed under linear combinations; that is,*

$$a, b \in \mathsf{F},\ u, v \in S \implies au + bv \in S.$$

Exercise F.2.A. For each of the following subsets of $\mathbb{R}^3$, determine whether it is a subspace of $\mathbb{R}^3$:

a) $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + 2x_2 + 3x_3 = 0\}$,

b) $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + 2x_2 + 3x_3 = 4\}$,

c) $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 x_2 x_3 = 0\}$,

d) $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 = 5x_3\}$.

Example **F.2.3** (Subspaces). We present here a few examples of subspaces.

a) If $b \in \mathsf{F}$, then the set

$$\{(x_1, x_2, x_3, x_4) \in \mathsf{F}^4 \mid x_3 = 5x_4 + b\}$$

is a subspace of F^4 if and only if $b = 0$.

b) The set of continuous real-valued functions on the interval $[0, 1]$ is a subspace of $\mathbb{R}^{[0,1]}$.

c) The set of differentiable real-valued functions on $\mathbb{R}$ is a subspace of $\mathbb{R}^{\mathbb{R}}$.

d) The set of differentiable real-valued functions on the interval $(0, 3)$ such that $f'(2) = b$ is a subspace of $\mathbb{R}^{(0,3)}$ if and only if $b = 0$.

e) The set of all real sequences $(x_n)_{n \in \mathbb{N}}$ such that

$$\lim_{n \to \infty} x_n = 0$$

is a subspace of $\mathbb{R}^{\mathbb{N}}$.

Exercise F.2.B. Verify all assertions about subspaces stated in Example F.2.3.

Exercise F.2.C. Show that the set of differentiable real-valued functions on $(-4, 4)$ such that

$$f'(-1) = 3f'(2)$$

is a subspace of $\mathbb{R}^{(-4,4)}$.

Exercise F.2.D. Suppose $b \in \mathbb{R}$. Show that the set of continuous real-valued functions on $[0, 1]$ such that

$$\int_0^1 f = b$$

is a subspace of $\mathbb{R}^{[0,1]}$ if and only if $b = 0$.

Exercise F.2.E. Give an example of a nonempty subset U of $\mathbb{R}^2$ that is closed under scalar multiplication but is not a subspace of $\mathbb{R}^2$.

Exercise F.2.F. Give an example of a nonempty subset U of $\mathbb{R}^2$ that is closed under addition and taking additive inverses but is not a subspace of $\mathbb{R}^2$.

Exercise F.2.G. Let V_1 and V_2 be subspaces of a vector space V. Prove that the intersection $V_1 \cap V_2$ is a subspace of V.

Exercise F.2.H. Prove that the intersection of an arbitrary collection of subspaces of a vector space V is a subspace of V.

Theorem F.2.4. *Let V be a nontrivial vector space over an infinite field F. Then V is not the union of finitely many proper subspaces.*

Proof. Suppose, toward a contradiction, that

$$V = S_1 \cup \cdots \cup S_n,$$

where each S_i is a proper subspace of V. Without loss of generality, assume that

$$S_1 \not\subseteq S_2 \cup \cdots \cup S_n.$$

Choose $w \in S_1 \setminus (S_2 \cup \cdots \cup S_n)$, and choose $v \in V \setminus S_1$. Consider the set

$$A = \{rw + v : r \in \mathsf{F}\},$$

which is the affine line through v in the direction of w.

We claim that each subspace S_i contains at most one element of A. This contradicts the fact that A is infinite and that $V = S_1 \cup \cdots \cup S_n$.

Indeed, suppose first that $rw + v \in S_1$ for some $r \neq 0$. Then $v = (rw + v) - rw \in S_1$, which contradicts the choice of v.

Next, suppose that for some $i \geq 2$ there exist $r_1 \neq r_2$ such that $r_1 w + v \in S_i$ and $r_2 w + v \in S_i$. Then

$$(r_1 w + v) - (r_2 w + v) = (r_1 - r_2)w \in S_i,$$

and since F is a field and $r_1 - r_2 \neq 0$, it follows that $w \in S_i$, contradicting the choice of w.

Therefore each S_i contains at most one element of A, which is impossible. This completes the proof. /ᐢ˳ᐢ\

An important construction is the sum of subspaces.

Definition **F.2.5** (Sum of subspaces). Let S and T be subspaces of a vector space V. The *sum* $S + T$ is defined by

$$S + T := \{ u + v : u \in S,\ v \in T \}.$$

More generally, if $\{S_i\}_{i \in K}$ is a collection of subspaces of V, their sum is the set

$$\sum_{i \in K} S_i := \left\{ s_1 + \cdots + s_n \;\middle|\; s_j \in S_{i_j} \text{ for some } i_j \in K,\ n \in \mathbb{N} \right\}.$$

Remark **F.2.6**. The sum $S + T$ coincides with the Minkowski sum (see definition 1.7.8) of the subsets S and T. When S and T are subspaces, this sum is again a subspace of V.

Remark **F.2.7**. Definition F.2.5 is important because it allows us to construct the *smallest* subspace of V containing the subspaces S and T. Formally, if we partially order the set of all subspaces from V by set inclusion, then the sum $S + T$ is the least upper bound of S and T.

Exercise F.2.I. Suppose

$$U = \{(x, -x, 2x) \in \mathbb{R}^3 \mid x \in \mathbb{R}\} \quad \text{and} \quad W = \{(x, x, 2x) \in \mathbb{R}^3 \mid x \in \mathbb{R}\}.$$

Describe $U + W$ using symbols, and also give a description of $U + W$ that does not involve symbols.

Exercise F.2.J. Let U be a subspace of a vector space V. What is $U + U$?

Exercise F.2.K. Let U and W be subspaces of a vector space V. Is the operation of addition on subspaces commutative? In other words, is it always true that

$$U + W = W + U?$$

Exercise F.2.L. Let V_1, V_2, V_3 be subspaces of a vector space V. Is the operation of addition on subspaces associative? In other words, is it always true that

$$(V_1 + V_2) + V_3 = V_1 + (V_2 + V_3)?$$

Exercise F.2.M. Does the operation of addition on the subspaces of a vector space V have an additive identity? If so, identify it. Which subspaces, if any, have additive inverses?

Exercise F.2.N. Prove or give a counterexample: if V_1, V_2, U are subspaces of a vector space V such that

$$V_1 + U = V_2 + U,$$

then $V_1 = V_2$.

F.3 Direct Sums

We will now define two important constructions, which will allow us to construct new vector spaces from old ones.

Definition **F.3.1** (External direct sum). Let $(V_1, \dots, V_n)$ be vector spaces over a field F. The *external direct sum* of $V_1, \dots, V_n$, denoted by

$$V_1 \boxplus \cdots \boxplus V_n,$$

is the vector space whose elements are ordered n-tuples

$$V_1 \boxplus \cdots \boxplus V_n = \{(v_1, \dots, v_n) \mid v_i \in V_i \text{ for } i = 1, \dots, n\},$$

with addition and scalar multiplication defined componentwise by

$$(u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n),$$

and

$$a(v_1, \dots, v_n) = (av_1, \dots, av_n),$$

for all $a \in \mathsf{F}$.

Example **F.3.2**. The vector space F^n is the external direct sum of n copies of F:

$$\mathsf{F}^n = \mathsf{F} \boxplus \cdots \boxplus \mathsf{F},$$

where there are n summands on the right-hand side.

The preceding construction can be reformulated in functional terms. An ordered n-tuple $(v_1, \dots, v_n)$ may be identified with a function

$$f : \{1, \dots, n\} \to \bigcup_{i=1}^{n} V_i$$

such that $f(i) \in V_i$ for each i.

Definition **F.3.3** (Direct product). Let $\mathcal{F} = \{V_i \mid i \in K\}$ be a family of vector spaces over a field F. The *direct product* of the family $\mathcal{F}$ is the vector space

$$\bigtimes_{i \in K} V_i = \left\{ f : K \to \bigcup_{i \in K} V_i \;\middle|\; f(i) \in V_i \text{ for all } i \in K \right\},$$

with addition and scalar multiplication defined pointwise by

$$(f + g)(i) = f(i) + g(i), \qquad (af)(i) = af(i),$$

for all $f, g \in \bigtimes_{i \in K} V_i$, all $a \in \mathsf{F}$, and all $i \in K$.

Remark **F.3.4.** The direct product from definition F.3.3 is exactly the same construction we used to define the *cartesian product* in definition B.2.12. The only difference is that we are now adding the vector space structure.

Below we present a different version of the direct sum construction.

Definition **F.3.5** (Internal direct sum). Let V be a vector space, and let

$$\mathcal{F} = \{S_i \mid i \in I\}$$

be a family of subspaces of V. We say that V is the *(internal) direct sum* of the family $\mathcal{F}$, and write

$$V = \bigoplus \mathcal{F} \quad \text{or} \quad V = \bigoplus_{i \in I} S_i,$$

if the following conditions hold:

a) *(Join of the family)* V is the sum of the family $\mathcal{F}$, that is,

$$V = \sum_{i \in I} S_i.$$

b) *(Independence of the family)* For each $i \in I$,

$$S_i \cap \left(\sum_{j \in I,\, j \neq i} S_j \right) = \{0\}.$$

In this case, each subspace S_i is called a *direct summand* of V. If $\mathcal{F} = \{S_1, \ldots, S_n\}$ is a finite family, the direct sum is often written

$$V = S_1 \oplus \cdots \oplus S_n.$$

Finally, if $V = S \oplus T$, then T is called a *complement* of S in V.

Remark **F.3.6.** Note that condition b) in definition F.3.5 is stronger than saying simply that the members of $\mathcal{F}$ are pairwise disjoint.

Remark **F.3.7.** We need to be cautious here: If S and T are subspaces of V, then the sum $S + T$ exists. However, if we say that the direct sum $S \oplus T$ exists, then it implies that $S \cap T = \{0\}$. Thus, while the sum of two subspaces always exists, the *direct* sum of two subspaces does not always exist.

Remark **F.3.8.** It turns out that the constructions we just defined in definitions F.3.1 and F.3.5 are essentially equivalent.[1] For this reason, the term "direct sum" is often used without qualification.

[1] Isomorphic.

The following is an important theorem, but we postpone its proof until we discuss the notion of a basis.

Theorem F.3.9. *Any subpsace of a vector space has a complement, that is, if S is a subspace of V, then there exists a subspace T for which $V = S \oplus T$.*

***Remark* F.3.10**. Let S and T be subspaces of a vector space V. A vector $v \in V$ is said to be expressible as a sum of vectors from the distinct subspaces S and T if there exist $s \in S$ and $t \in T$ such that $v = s + t$.

If $x, y \in S \cap T$, then the vector $v = x + y$ admits such a representation: indeed, $v = x + y$ with $x \in S$ and $y \in T$. Thus, even though x and y both lie in the same subspace, the decomposition $v = x + y$ may still be viewed as a sum of vectors drawn from distinct subspaces.

The direct sum condition $S \cap T = \{0\}$ rules out such ambiguities and ensures that every vector in $S + T$ has a unique representation as a sum of vectors from S and T.

Theorem F.3.11 (Equivalent characterizations of a direct sum). *Let*

$$\mathcal{F} = \{S_i \mid i \in I\}$$

be a family of distinct subspaces of a vector space V. The following statements are equivalent:

a) (Independence of the family) *For each $i \in I$,*

$$S_i \cap \left(\sum_{j \neq i} S_j \right) = \{0\}.$$

b) (Uniqueness of expression for 0) *The zero vector* 0 *cannot be written as a sum of nonzero vectors from distinct subspaces of $\mathcal{F}$.*

c) (Uniqueness of expression) *Every nonzero vector $v \in \sum_{i \in I} S_i$ has a unique expression, up to the order of the terms, of the form*

$$v = s_1 + \cdots + s_n,$$

where each s_k is a nonzero vector belonging to a distinct subspace in $\mathcal{F}$.

Consequently, the sum

$$V = \sum_{i \in I} S_i$$

is a direct sum if and only if any of the conditions (a)–(c) hold.

Proof. *(a)* $\Rightarrow$ *(b).* Suppose that *(b)* fails. Then there exist nonzero vectors $s_{j_1}, \ldots, s_{j_n}$ belonging to distinct subspaces $S_{j_1}, \ldots, S_{j_n}$ in $\mathcal{F}$ such that

$$0 = s_{j_1} + \cdots + s_{j_n}.$$

Necessarily $n > 1$. Rewriting the above equality gives

$$-s_{j_1} = s_{j_2} + \cdots + s_{j_n}.$$

The right-hand side belongs to $\sum_{k \neq j_1} S_k$, while the left-hand side belongs to S_{j_1}. Since $s_{j_1} \neq 0$, this contradicts condition *(a).* Hence *(a)* implies *(b).*
(b) $\Rightarrow$ *(c).* Assume *(b)* holds. Suppose that a nonzero vector v admits two expressions

$$v = s_1 + \cdots + s_n \quad \text{and} \quad v = t_1 + \cdots + t_m,$$

where all terms are nonzero, the vectors s_i belong to distinct subspaces of $\mathcal{F}$, and similarly for the t_j. Subtracting the two expressions yields

$$0 = s_1 + \cdots + s_n - t_1 - \cdots - t_m.$$

By collecting terms belonging to the same subspaces, we may rewrite this as

$$0 = (s_{i_1} - t_{i_1}) + \cdots + (s_{i_k} - t_{i_k}) + s_{i_{k+1}} + \cdots + s_{i_n} - t_{i_{k+1}} - \cdots - t_{i_m},$$

where each summand is either zero or a nonzero vector from a distinct subspace. By condition *(b)*, all summands must be zero. Therefore $n = m = k$ and, after reordering terms if necessary,

$$s_i = t_i \quad \text{for all } i = 1, \ldots, n.$$

This proves *(c).*
(c) $\Rightarrow$ *(a).* Suppose that *(c)* holds, and assume for contradiction that *(a)* fails. Then there exists an index i and a nonzero vector

$$v \in S_i \cap \left(\sum_{j \neq i} S_j \right).$$

Thus v admits two expressions:

$$v = s_i \quad \text{with } s_i \in S_i \setminus \{0\},$$

and

$$v = s_{j_1} + \cdots + s_{j_n},$$

where each s_{j_k} is a nonzero vector in S_{j_k} and $j_k \neq i$. These two expressions represent v as sums of nonzero vectors from distinct subspaces, contradicting the uniqueness asserted in *(c).* Hence *(c)* implies *(a).* ^. .^)9

***Example* F.3.12.** Let $\mathcal{M}_n(\mathbb{R})$ denote the vector space of all $n \times n$ real matrices. For any matrix $A \in \mathcal{M}_n(\mathbb{R})$, define

$$B = \frac{1}{2}(A + A^t) \quad \text{and} \quad C = \frac{1}{2}(A - A^t),$$

where A^t denotes the transpose of A. Then

$$A = B + C.$$

The matrix B is symmetric and the matrix C is skew-symmetric.[2] Let Sym denote the subspace of symmetric matrices in $\mathcal{M}_n(\mathbb{R})$, and let $\mathsf{SkewSym}$ denote the subspace of skew-symmetric matrices. Thus,

$$\mathcal{M}_n(\mathbb{R}) = \mathsf{Sym} + \mathsf{SkewSym}.$$

Moreover, if $U \in \mathsf{Sym} \cap \mathsf{SkewSym}$, then $U^t = U$ and $U^t = -U$, which implies $U = -U$ and hence $U = 0$. Therefore,

$$\mathcal{M}_n(\mathbb{R}) = \mathsf{Sym} \oplus \mathsf{SkewSym}.$$

***Remark* F.3.13.** The decomposition in Example F.3.12 of $\mathcal{M}_n(\mathbb{R})$ relies on an algebraic property of the field $\mathbb{R}$ that is shared by some, but not all, fields. Consequently, additional care is required when considering $\mathcal{M}_n(\mathsf{F})$ for an arbitrary field F.

Exercise F.3.A. Let

$$U = \{(x, x, y, y) \in \mathsf{F}^4 \mid x, y \in \mathsf{F}\}.$$

Find a subspace W of F^4 such that $\mathsf{F}^4 = U \oplus W$.

Exercise F.3.B. Let

$$U = \{(x, y, x + y, x - y, 2x) \in \mathsf{F}^5 \mid x, y \in \mathsf{F}\}.$$

Find a subspace W of F^5 such that $\mathsf{F}^5 = U \oplus W$.

Exercise F.3.C. Let

$$U = \{(x, y, x + y, x - y, 2x) \in \mathsf{F}^5 \mid x, y \in \mathsf{F}\}.$$

[2] $C^t = -C$.

Find three subspaces W_1, W_2, W_3 of F^5, none of which is $\{0\}$, such that $\mathsf{F}^5 = U \oplus W_1 \oplus W_2 \oplus W_3$.

Exercise F.3.D. Prove or give a counterexample: If V_1, V_2, U are subspaces of a vector space V such that

$$V = V_1 \oplus U \quad \text{and} \quad V = V_2 \oplus U,$$

then $V_1 = V_2$.

F.4 Spanning Sets and Linear Independence

We say that a set of vectors *spans* a vector space if every vector can be written as a linear combination of some of the vectors in that set, i.e., the span of such a set of vectors is the set of all linear combinations that can be formed with them. Below is the formal definition.

Definition **F.4.1**. Let V be a vector space over a field F, and let $S \subseteq V$ be a nonempty set. The *subspace spanned* (or *subspace generated*) by S is the set of all linear combinations of vectors from S, namely

$$\langle S\rangle = \operatorname{span}(S) = \{r_1 v_1 + \cdots + r_n v_n : n \in \mathbb{N},\ r_i \in \mathsf{F}, v_i \in S\}.$$

When $S = \{v_1, \ldots, v_n\}$ is a finite set, we use equivalently the notation $\langle v_1, \ldots, v_n\rangle$ or $\operatorname{span}(v_1, \ldots, v_n)$. A set $S \subseteq V$ is said to *span* V, or to *generate* V, if $V = \operatorname{span}(S)$.

Remark **F.4.2**. Any superset of a spanning set is also a spanning set. Note also that all vector spaces have spanning sets, since V spans itself.

We next discuss a fundamental concept in linear algebra.

Definition **F.4.3**. Let V be a vector space over a field F. A nonempty set $S \subseteq V$ is said to be *linearly independent* if for every finite collection of distinct vectors $s_1, \ldots, s_n \in S$,

$$\sum_{i=1}^{n} \alpha_i s_i = 0, \qquad \alpha_i \in \mathsf{F},$$

implies that $\alpha_i = 0$ for all $i = 1, \ldots, n$. If this condition is not satisfied, the set S is said to be *linearly dependent.*

Note that it is immediate from definition F.4.3 that a linearly independent set of vectors cannot contain the zero vector since $1 \cdot 0 = 0$ violates the condition of the definition.

Remark **F.4.4.** An equivalent way to phrase the definition of linear independence is the following. A set S is linearly independent if the zero vector admits a *unique* representation as a linear combination of vectors from S. More precisely, although the zero vector can always be written as

$$0 = 0s_1 + \cdots + 0s_n,$$

linear independence ensures that it cannot be written in any other way as a linear combination of vectors in S.

Remark **F.4.5.** If $s_1 \neq 0$, the identity

$$0 = s_1 + (-s_1)$$

should be interpreted as involving the two distinct vectors s_1 and $-s_1$, rather than as a nontrivial linear combination of a single vector. Consequently, if a set S is linearly independent, it cannot contain both s_1 and $-s_1$.

Definition **F.4.6.** Let V be a vector space over a field F and let $S \subseteq V$ be a nonempty set. A nonzero vector $v \in V$ is said to be an *essentially unique linear combination* of the vectors in S if, up to reordering of terms, there is exactly one way to write

$$v = a_1 s_1 + \cdots + a_n s_n,$$

where the vectors $s_1, \ldots, s_n$ are distinct elements of S and the coefficients $a_i \in \mathsf{F}$ are nonzero.

More explicitly, a nonzero vector v is an essentially unique linear combination of vectors in S if $v \in \operatorname{span}(S)$ and whenever

$$v = a_1 s_1 + \cdots + a_n s_n \quad \text{and} \quad v = b_1 t_1 + \cdots + b_m t_m,$$

with the vectors s_i and t_j distinct and all coefficients nonzero, then $m = n$ and, after a reindexing if necessary,

$$a_i = b_i \quad \text{and} \quad s_i = t_i \qquad \text{for all } i = 1, \ldots, n.$$

The next theorem establishes different characterizations of linear independence.

Theorem F.4.7. *Let V be a vector space over a field F, and let $S \subseteq V$ be a nonempty set with $S \neq \{0\}$. The following statements are equivalent:*

a) S is linearly independent.

b) Every nonzero vector $v \in \operatorname{span}(S)$ admits an essentially unique representation as a linear combination of vectors in S.

c) No vector in S can be written as a linear combination of other vectors in S.

Proof. Assume that *(a)* holds and suppose that

$$0 \neq v = a_1 s_1 + \cdots + a_n s_n = b_1 t_1 + \cdots + b_m t_m,$$

where the vectors $s_1, \ldots, s_n$ are distinct, the vectors $t_1, \ldots, t_m$ are distinct, and all coefficients are nonzero. Subtracting the two expressions and grouping together equal vectors, we obtain

$$\begin{aligned} 0 = {} & (a_{i_1} - b_{i_1}) s_{i_1} + \cdots + (a_{i_k} - b_{i_k}) s_{i_k} \\ & + a_{i_{k+1}} s_{i_{k+1}} + \cdots + a_{i_n} s_{i_n} \\ & - b_{i_{k+1}} t_{i_{k+1}} - \cdots - b_{i_m} t_{i_m}. \end{aligned}$$

Since S is linearly independent, all coefficients must be zero. It follows that $n = m = k$, that $a_{i_u} = b_{i_u}$, and that $s_{i_u} = t_{i_u}$ for all $u = 1, \ldots, k$. Thus, *(a)* implies *(b)*.

Assume next that *(b)* holds and suppose that $s \in S$ can be written as

$$s = a_1 s_1 + \cdots + a_n s_n,$$

where each $s_i \in S$ is distinct from s. Collecting like terms and removing all terms with zero coefficient yields a nontrivial representation of s, which contradicts the essential uniqueness asserted in *(b)*. Hence, *(b)* implies *(c)*.

Finally, assume that *(c)* holds and suppose that

$$a_1 s_1 + \cdots + a_n s_n = 0,$$

where the vectors $s_1, \ldots, s_n$ are distinct and $a_1 \neq 0$. Then $n > 1$ and we may solve for s_1 as

$$s_1 = -\frac{1}{a_1}\big(a_2 s_2 + \cdots + a_n s_n\big),$$

which expresses s_1 as a linear combination of other vectors in S, contradicting *(c)*. Therefore, *(c)* implies *(a)*. ^. .^)9

Appendix G

Real Normed Vector Spaces

> Humans cannot create anything out of nothingness.
> Humans cannot accomplish anything without holding onto something.
>
> Kaworu Nagisa, *Evangelion 3.33*, Hideaki Anno

G.1 Normed Vector Spaces

When X is a vector space (which we will assume is a vector space over the field F of real numbers throughout this chapter), the useful metrics are those that in some way "respect" the vector space structure. For example, we would like the distance between vectors in X not to change when we translate these vectors by a fixed vector (these are called *invariant metrics*). We would also expect that when multiplying a vector by a scalar, the magnitude of the new vector varies according to the scalar factor in the same proportion. The notion of *norm* is the one that defines the most important metric in vector spaces. See Section 1.1 for the discussion on metric spaces.

Definition **G.1.1** (Norm). Let X be a vector space over $\mathbb{R}$. A norm on X is a function $\|\cdot\| : X \to \mathbb{R}$ that satisfies:

a) $\|x\| \geq 0$ for every $x \in X$. *(positive definiteness)*

b) $\|x\| = 0$ if and only if $x = 0$.

c) $\|\alpha x\| = |\alpha|\|x\|$ for every $x \in X$ and every $\alpha \in \mathbb{R}$. *(absolute homogeneity)*

d) $\|x + y\| \leq \|x\| + \|y\|$ for every $x, y \in X$. *(triangle inequality)*

The pair $(X, \|\cdot\|)$ is called a *normed space.*

In the next proposition we will see that every normed vector space $(X, \|\cdot\|)$ is a metric space. Since having a vector space structure is necessary in order to be a normed space, there exist metric spaces that are not normed spaces.

Proposition G.1.2. *Let $(X, \|\cdot\|)$ be a normed space. Then the following defines a distance on the set X:*

$$d(x, y) = \|x - y\|.$$

Proof. The only part that is not trivial is the proof of the triangle inequality. Let $x, y, z \in X$. Then

$$d(x, y) = \|x - y\| = \|(x - z) + (z - y)\| \leq \|x - z\| + \|z - y\| = d(x, z) + d(z, y).$$

The rest follows from the other properties of the norm.

Example **G.1.3.** In $\mathbb{R}$, the absolute value $|(|\cdot)$ is a norm. Thus, $(\mathbb{R}, |(|\cdot))$ is a normed space.

Exercise G.1.A. Let $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be given by $d(a, b) = |(|a - b)$. Verify that $|\cdot|$ satisfies the triangle inequality.

Example **G.1.4** (The taxicab norm). Also known as the *Hamming distance* or the *Shannon distance* due to its use in cryptography, the taxicab norm or ℓ^1-norm in $\mathbb{R}^n$ is defined by

$$\|(x_1, x_2, \ldots, x_n)\|_1 = \sum_{i=1}^{n} |x_i|.$$

That $\|\cdot\|_1$ is a norm follows directly from the fact that the absolute value is a norm.

Example **G.1.5** (The supremum norm). The supremum norm in $\mathbb{R}^n$ is defined as

$$\|(x_1, x_2, \ldots, x_n)\|_\infty = \max\{|x_1|, |x_2|, \ldots, |x_n|\}.$$

It is left as an exercise for the reader to prove that $\|\cdot\|_\infty$ is a norm.

Example **G.1.6** (The usual Euclidean norm). The usual Euclidean norm in $\mathbb{R}^n$, $\|\cdot\|_2$, as we will prove later, is also a norm. Recall that this norm is defined by

$$\|(x_1, x_2, \ldots, x_n)\|_2 = \left(\sum_{i=1}^{n} |x_i|^2\right)^{1/2}.$$

Example **G.1.7.** Let us consider an example that calculates each of the norms we have just defined in the Euclidean space $\mathbb{R}^2$.

$$\begin{aligned}
\|(5, -12)\|_2 &= 13, \\
\|(5, -12)\|_1 &= |5| + |-12| = 17, \\
\|(5, -12)\|_\infty &= \max\{|5|, |-12|\} = 12.
\end{aligned}$$

***Example* G.1.8** (The p-norms). The natural generalization of the Euclidean norm in $\mathbb{R}^n$ is the so-called p-norm. If $1 \le p < \infty$ is a real number, then

$$\|(x_1, x_2, \ldots, x_n)\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$$

is a norm in $\mathbb{R}^n$. Observe that the particular case $p = 2$ corresponds to the usual Euclidean norm. As with the norms defined above, proving the triangle inequality for $\|\cdot\|_p$, that is,

$$\|x + y\|_p \le \|x\|_p + \|y\|_p,$$

is not trivial. The triangle inequality is also known as *Minkowski's inequality*[1]. To prove this inequality, the following lemmas will be used.

Lemma G.1.9 (Young's inequality[2]). *If a, b are positive real numbers and p, q are conjugate exponents, that is, $p, q \ge 1$ and*

$$\frac{1}{p} + \frac{1}{q} = 1,$$

then

$$ab \le \frac{a^p}{p} + \frac{b^q}{q}.$$

Proof. Previously, the power of a positive real number t raised to the exponent α was defined as

$$t^\alpha = \sup\{t^q : q \in \mathbb{Q},\ q \le \alpha\}.$$

Let $t \ge 1$ and $0 < \alpha < 1$. Consider a rational number $m/n \in \mathbb{Q}$ with $m/n \le \alpha$ and $m < n$. Define $z = m(t-1)$. Clearly $z > -m$ and by Exercise C.1.G it follows that

$$\left(1 + \frac{z}{m}\right)^m \le \left(1 + \frac{z}{n}\right)^n.$$

This implies that

$$t^m \le \left(1 + \frac{m}{n}(t-1)\right)^n,$$

and therefore

$$t^{m/n} \le 1 + \frac{m}{n}(t-1) \le 1 + \alpha(t-1).$$

[1] Hermann Minkowski, 1864-1909.
[2] William Henry Young, 1863–1942.

Taking the supremum, one obtains the inequality

$$t^{\alpha} \leq \alpha t + (1-\alpha). \tag{G.1.10}$$

Now consider two positive numbers a, b and two conjugate exponents p, q, that is, $p, q \geq 1$ and $1/p + 1/q = 1$.

If $a^p \geq b^q$ then define $t = a^p/b^q \geq 1$ and $\alpha = 1/p$. Inequality (G.1.10) implies that

$$t^{1/p} \leq \frac{t}{p} + \frac{1}{q},$$

and therefore,

$$\frac{a}{b^{q/p}} \leq \frac{1}{p}\frac{a^p}{b^q} + \frac{1}{q}.$$

Observe that

$$\frac{b^q}{b^{q/p}} = b^{q-q/p} = b.$$

Multiplying the previous inequality by b^q, one obtains

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}.$$

The proof in the case $a^p < b^q$ is carried out in a similar way, using $t = b^q/a^p$ and $\alpha = 1/q$.

***Remark* G.1.11.** The notion of conjugate exponent can be extended to numbers $p, q \in [1, \infty]$, since by convention, the conjugate of $p = 1$ is $q = \infty$.

Lemma G.1.12 (Hölder's[3] inequality). *Let p and q be conjugate exponents and let $x = (x_1, \dots, x_n)$, and $y = (y_1, \dots, y_n)$ be vectors in $\mathbb{R}^n$. Then*

$$\sum_{i=1}^{n} |x_i y_i| \leq \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p} \left(\sum_{i=1}^{n} |y_i|^q\right)^{1/q}.$$

If $p = 1$ and $q = \infty$, the inequality becomes

$$\sum_{i=1}^{n} |x_i y_i| \leq \max\{|y_1|, \dots, |y_n|\} \left(\sum_{i=1}^{n} |x_i|\right).$$

[3] Otto Ludwig Hölder, 1859-1937.

Proof. We prove Hölder's inequality for the case $1 < p, q < \infty$. The case $p = 1$, $q = \infty$ is left to the reader. First observe that the inequality is true if either $x = 0$ or $y = 0$. Suppose therefore that $x \neq 0 \neq y$. For each $j \in \{1, 2, \ldots, n\}$, define

$$a_j = \frac{|x_j|}{\|x\|_p}, \qquad b_j = \frac{|y_j|}{\|y\|_q}.$$

By Young's inequality we have

$$a_j b_j \leq \frac{a_j^p}{p} + \frac{b_j^q}{q},$$

for every $j = 1, 2, \ldots, n$. Therefore,

$$\sum_{j=1}^{n} a_j b_j \leq \frac{1}{p} \sum_{j=1}^{n} a_j^p + \frac{1}{q} \sum_{j=1}^{n} b_j^q.$$

From this it follows that

$$\frac{1}{\|x\|_p \|y\|_q} \sum_{j=1}^{n} |x_j y_j| \leq \frac{1}{p} \sum_{j=1}^{n} \frac{|x_j|^p}{\|x\|_p^p} + \frac{1}{q} \sum_{j=1}^{n} \frac{|y_j|^q}{\|y\|_q^q}.$$

That is,

$$= \frac{1}{p} \frac{1}{\|x\|_p^p} \sum_{j=1}^{n} |x_j|^p + \frac{1}{q} \frac{1}{\|y\|_q^q} \sum_{j=1}^{n} |y_j|^q$$

$$= \frac{1}{p} \frac{\|x\|_p^p}{\|x\|_p^p} + \frac{1}{q} \frac{\|y\|_q^q}{\|y\|_q^q} = \frac{1}{p} + \frac{1}{q} = 1.$$

Therefore,

$$\sum_{j=1}^{n} |x_j y_j| \leq \|x\|_p \|y\|_q,$$

as was to be shown. /˚‸˚\

Let us now verify the triangle inequality for the p-norm.

Lemma G.1.13. *Let $p > 1$. Then*

$$\|x + y\|_p \leq \|x\|_p + \|y\|_p,$$

for every $x, y \in \mathbb{R}^n$.

Proof. Let $x, y \in \mathbb{R}^n$, let $p > 1$, and let q be the conjugate exponent of p. Once we have Hölder's inequality, the trick that leads to Minkowski's inequality is purely arithmetic. Indeed,

$$\begin{aligned}
\|x+y\|_p^p &= \sum_{i=1}^n |x_i + y_i|^p = \sum_{i=1}^n |x_i + y_i|^{p-1}|x_i + y_i| \\
&\le \sum_{i=1}^n |x_i + y_i|^{p-1}(|x_i| + |y_i|) \\
&= \sum_{i=1}^n |x_i + y_i|^{p-1}|x_i| + \sum_{i=1}^n |x_i + y_i|^{p-1}|y_i| \\
&\le \left(\sum_{i=1}^n |x_i + y_i|^{(p-1)q}\right)^{1/q} \left(\sum_{i=1}^n |x_i|^p\right)^{1/p} \\
&\quad + \left(\sum_{i=1}^n |x_i + y_i|^{(p-1)q}\right)^{1/q} \left(\sum_{i=1}^n |y_i|^p\right)^{1/p} \\
&= \left(\sum_{i=1}^n |x_i + y_i|^{(p-1)q}\right)^{1/q} \left(\|x\|_p + \|y\|_p\right) \\
&= \left(\sum_{i=1}^n |x_i + y_i|^{p}\right)^{1/q} \left(\|x\|_p + \|y\|_p\right) \\
&= \|x+y\|_p^{p/q} \left(\|x\|_p + \|y\|_p\right),
\end{aligned}$$

where the second inequality comes from applying Hölder's inequality to each sum, and the next to last equality comes from noticing that $(p-1)q = p$.

Therefore,

$$\|x+y\|_p^{p-p/q} \le \|x\|_p + \|y\|_p.$$

Note that

$$p - \frac{p}{q} = p\left(1 - \frac{1}{q}\right) = \frac{p}{p} = 1.$$

Hence,

$$\|x+y\|_p \le \|x\|_p + \|y\|_p,$$

which is what we wanted to prove. /ᐠ｡ꞈ｡ᐟ\

Exercise G.1.B. Prove Hölder's inequality for the case $p = 1$ and $q = \infty$. Use it to verity that $\|\cdot\|_1$ and $\|\cdot\|_\infty$ are norms.

If the reader wonders why the values $0 < p < 1$ are excluded in the p-norms, the reason is that if $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n$ are vectors in $\mathbb{R}^n$, then the expression

$$\left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$$

is not a norm in $\mathbb{R}^n$. However,

$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i|^p$$

is a metric in $\mathbb{R}^n$.

Exercise G.1.C. Let $(X, \|\cdot\|)$ be a normed space. Let $T : X \to X$ be a linear and injective function. Prove that the following defines a norm on X: $\|x\|_T = \|Tx\|$.

Exercise G.1.D. Let $\bar{\omega} := (\omega_1, \omega_2, \dots, \omega_n)$ be fixed positive scalars. Prove that

$$\|(x_1, x_2, \dots, x_n)\|_{\bar{\omega}} = \left(\sum_{j=1}^{n} \omega_j x_j^2\right)^{1/2}$$

is a norm in $\mathbb{R}^n$.

G.2 Spaces with Inner Product

The reader may recall that the usual Euclidean norm is a very special type of norm, since it is induced by an *inner product.* We will now study the notion of an inner product and the norm it induces.

Definition G.2.1. Let X be a vector space over $\mathbb{R}$. An inner product (or dot product) on X is a function

$$\langle \cdot, \cdot \rangle : X \times X \to \mathbb{R}$$

such that:

a) $\langle x, x \rangle \geq 0$ for every $x \in X$, and $\langle x, x \rangle = 0$ if and only if $x = 0$. *(positive definiteness)*

b) $\langle \alpha x + y, z \rangle = \alpha \langle x, z \rangle + \langle y, z \rangle$ for all $x, y, z \in X$. and all $\alpha \in \mathbb{R}$. *(linearity in the first argument)*

c) $\langle x, y\rangle = \langle y, x\rangle$ for all $x, y \in X$. *(symmetry)*

The pair $(X, \langle \cdot\,, \cdot\rangle)$ is called an *inner product space.*

Remark **G.2.2.** For real vector spaces, notice that symmetry and linearity in the first argument imply bilinearity of the inner product.

In inner product spaces one can reproduce the geometric principles known from Euclidean spaces $\mathbb{R}^n$, because in principle the notion of angle is defined from the dot product, and one certainly obtains a notion of distance, as we will see in Proposition G.2.5.

Example **G.2.3.** In $\mathbb{R}^n$, $\langle (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)\rangle = \sum_{i=1}^n x_i y_i$ is an inner product.

Example **G.2.4.** An $n \times n$ matrix A is positive if for every $x \in \mathbb{R}^n$ with $x \neq 0$,

$$x^T Ax > 0.$$

If A is positive definite, then the following defines an inner product on $\mathbb{R}^n$:

$$\langle x, y\rangle = x^T Ay.$$

In fact, it can also be shown that all inner products on $\mathbb{R}^n$ are of this form; that is, they arise from a positive definite matrix.

Proposition G.2.5. *Let $(X, \langle\cdot, \cdot\rangle)$ be an inner product space. Then the function from X into $\mathbb{R}$ given by*

$$x \longmapsto \sqrt{\langle x, x\rangle}$$

is a norm. It is called the norm induced by the inner product.

Remark **G.2.6.** There are norms that are *not* induced by an inner product. I invite the reader to discover a geometric condition that is necessary and sufficient for a norm to be induced by an inner product.

Exercise G.2.A. If $(X, \langle\cdot, \cdot\rangle)$ is an inner product space, prove that

$$\|x + y\|^2 + \|x - y\|^2 = 2\big(\|x\|^2 + \|y\|^2\big),$$

and

$$4\,\langle x, y\rangle = \|x + y\|^2 - \|x - y\|^2.$$

The first identity is called the *parallelogram identity* and the second the *polarization identity.* Interpret geometrically the parallelogram identity. Find a norm that does *not* satisfy the parallelogram identity.

The proof of proposition G.2.5 is easy until we try to show that the norm satisfies the triangle inequality. In order to prove it, we will need the following results.

Lemma G.2.7 (Pythagoras' Theorem). *Let $x, y \in X$. Then $\langle x, y \rangle = 0$ if and only if*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Proof. By definition of $\|\cdot\|$ and the properties of the inner product, we have

$$\|x + y\|^2 = \langle x + y, x + y \rangle = \langle x, x \rangle + 2\langle x, y \rangle + \langle y, y \rangle.$$

Therefore, $\|x + y\|^2 = \|x\|^2 + \|y\|^2 \quad$ if and only if $\quad \langle x, y \rangle = 0.$ ^. .^)9

Definition **G.2.8**. Let X be a vector space with inner product over $\mathbb{R}$ and let $x, y \in X$. Suppose that $y \neq 0$. The projection of x onto y is defined by

$$\operatorname{proj}_y(x) = \left(\frac{\langle x, y \rangle}{\|y\|^2} \right) y.$$

Proposition G.2.9. *Let X be a vector space with inner product over $\mathbb{R}$ and let $x, y \in X$. Suppose that $y \neq 0$. Then the projection of x onto y is the unique element $\operatorname{proj}_y(x) \in X$ such that*

$$\left\langle x - \operatorname{proj}_y(x)\,,\ y \right\rangle = 0.$$

Lemma G.2.10 (Cauchy–Buniakovsky–Schwarz inequality). [4][5][6] *Let X be a vector space with inner product over $\mathbb{R}$ and let $x, y \in X$. Then*

$$|\langle x, y \rangle| \leq \|x\| \|y\|.$$

Equality holds if and only if $x = \lambda y$ or $y = \lambda x$ for some $\lambda \in \mathbb{R}$.

Proof. Let $x, y \in X$. If either x or y is zero, the result is clear. Suppose that neither of them is zero and denote by $\operatorname{proj}_y(x)$ the projection of x onto y. We know that

$$\left\langle x - \operatorname{proj}_y(x)\,,\ y \right\rangle = 0,$$

hence by Pythagoras' theorem we have

$$\begin{aligned} \|x\|^2 = \left\| x - \operatorname{proj}_y(x) + \operatorname{proj}_y(x) \right\|^2 &= \left\| x - \operatorname{proj}_y(x) \right\|^2 + \left\| \operatorname{proj}_y(x) \right\|^2 \\ &\geq \left\| \operatorname{proj}_y(x) \right\|^2 = \frac{\langle x, y \rangle^2}{\|y\|^4} \|y\|^2. \end{aligned}$$

[4] Augustin Louis Cauchy, 1789-1857.
[5] Viktor Yakovlevich Buniakovsky, 1804-1889.
[6] Hermann Amandus Schwarz, 1843-1921.

Therefore, $\|x\|^2\|y\|^2 \geq \langle x, y\rangle^2$, that is, $\|x\|\|y\| \geq |\langle x, y\rangle|$.

Moreover, $\|x\|\|y\| = |\langle x, y\rangle|$ if and only if $\left\|x - \operatorname{proj}_y(x)\right\| = 0$, or equivalently,

$$x = \operatorname{proj}_y(x) = \frac{\langle x, y\rangle}{\|y\|^2}\, y,$$

that is, $x = \lambda y$ with $\lambda = \frac{\langle x,y\rangle}{\|y\|^2}$. /ᐠ｡ꞈ｡ᐟ\

We can now give a proof of the triangle inequality in proposition G.2.5.

Proof (Prop. G.2.5). Let $x, y \in X$. By the CBS inequality G.2.10 we have that

$$\|x - y\|^2 = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2,$$

therefore, $\|x + y\| \leq \|x\| + \|y\|$. ^. .^)9

Exercise G.2.B. Consider $(\mathbb{R}^n, \langle\cdot,\cdot\rangle)$ (here $\langle\cdot,\cdot\rangle$ is the usual inner product). Prove that for every $x \in \mathbb{R}^n$,

$$\|x\|_p = \sup\left\{\langle x, y\rangle : y \in \mathbb{R}^n,\ \|y\|_q \leq 1\right\},$$

where $\frac{1}{p} + \frac{1}{q} = 1$.

Exercise G.2.C. True (give a proof) or false (give a counterexample): In $\mathbb{R}^2$ there exists an inner product such that the associated norm is

$$\|(x, y)\| = |x| + |y|.$$

Exercise G.2.D. True (give a proof) or false (give a counterexample): If $(X, \|\cdot\|)$ is a normed vector space, then

$$\|x + y\| = \|x\| + \|y\| \quad \text{if and only if} \quad x = \lambda y$$

for some $\lambda \in \mathbb{R}$.

Exercise G.2.E. Consider the norm defined in exercise G.1.D. Find an inner product on $\mathbb{R}^n$ whose induced norm is $\|\cdot\|_{\bar{\omega}}$.

Appendix H

Binary Relations

> "Seeing together things that are scattered about everywhere and collecting them into one kind, so that by defining each thing we can make clear the subject of any instruction we wish to give."
>
> PLATO, *Phaedrus* 265d

This appendix provides a glossary of binary relations and their properties, along with key definitions related to preference relations and utility functions.

H.1 Basic Definitions

Definition **H.1.1** (Relation). A *relation* between members of X and Y can be thought of as a subset of $X \times Y$.

Definition **H.1.2** (Binary Relation). A *binary relation* on X is a relation over $X \times X$. For a binary relation R on X, we have that $R \subset X \times X$.

Remark **H.1.3** (Notation). For a binary relation R on X, we usually write xRy rather than $(x, y) \in R$. We read this as "x is R-related to y."

In the next definition, all statements should be interpreted with the proper universal quantifier: "for every x, y, z" etc. The symbol $\neg$ indicates negation, and a compound expression xRy and yRz may be abbreviated as $xRyRz$.

Definition **H.1.4** (Properties of Binary Relations). A binary relation R on a set X is:

- *reflexive* if xRx for all $x \in X$.
- *irreflexive* if $\neg(xRx)$ for all $x \in X$.
- *symmetric* if xRy implies yRx for all $x, y \in X$.
- *asymmetric* if xRy implies $\neg(yRx)$ for all $x, y \in X$.

- *antisymmetric* if xRy with $x \neq y$ implies $\neg(yRx)$ for all $x, y \in X$.
- *transitive* if xRy and yRz imply xRz for all $x, y, z \in X$.
- *complete* if either xRy or yRx or both, for all $x, y \in X$.
- *an equivalence relation* if it is reflexive, symmetric, and transitive.
- *the symmetric part* of the relation S if $xRy \Leftrightarrow (xSy \text{ and } ySx)$.
- *the asymmetric part* of the relation S if $xRy \Leftrightarrow (xSy \text{ and } \neg ySx)$.

Remark **H.1.5**. Note the following:

- Symmetry does not imply reflexivity.
- An asymmetric relation is irreflexive.
- An antisymmetric relation may or may not be reflexive.
- A complete relation is reflexive.

H.2 Preference Relations

Definition **H.2.1** (Preference Relation). A *preference relation* on the set X is a complete and transitive binary relation on X.

Remark **H.2.2** (Interpretation of Preference Relations). We model the decision maker's (DM's) tastes via preference relations. The idea is as follows: imagine that we present to the DM a questionnaire with the following format. For all $x, y \in X$ (not necessarily distinct), we ask: "Is x at least as preferred as y?" The DM must check exactly one of the following two boxes: Yes or No.

In order for the responses to constitute a preference relation, we require that:

a) The answer to at least one of the questions $R(x, y)$ and $R(y, x)$ must be Yes. In particular, the question $R(x, x)$ must always be answered Yes.

b) For every $x, y, z \in X$, if the answer to $R(x, y)$ is Yes and the answer to $R(y, z)$ is also Yes, then the answer to $R(x, z)$ must be Yes.

Note that under these conditions, R is indeed complete and transitive, and thus a preference relation.

H.2.1 Notation for Preference Relations

Definition **H.2.3** (Weak Preference). We use the symbol $\succsim$ to denote the answers to each question $R(x, y)$ from the preference questionnaire. We write $x \succsim y$ and read this as "x is at least as preferred as y."

Definition **H.2.4** (Indifference). The symmetric part of $\succsim$ is denoted by $\sim$. If $x \sim y$ we read this as "x is indifferent to y."

Definition **H.2.5** (Strict Preference). The asymmetric part of $\succsim$ is denoted by $\succ$. If $x \succ y$ we read this as "x is strictly preferred to y."

H.2.2 Utility Functions

While preference relations provide a primitive way to describe the DM's preferences, we can also represent preferences via a utility function. Taking the preference relation as primitive, if there exists some utility function that represents the preferences, we say that the utility function *represents* the preference relation.

Definition **H.2.6** (Utility Function). For any set X and preference relation $\succsim$ on X, the function $u : X \to \mathbb{R}$ *represents* $\succsim$ if

$$x \succsim y \text{ if and only if } u(x) \geq u(y).$$

We say that u is a *utility function* for $\succsim$.

Definition **H.2.7** (Minimal and Maximal Alternatives). For any set X and preference relation $\succsim$ on X, the alternative $x \in X$ is:

- *minimal with respect to* $\succsim$ *in* X if $y \succsim x$ for all $y \in X$, and
- *maximal with respect to* $\succsim$ *in* X if $x \succsim y$ for all $y \in X$.

Lemma H.2.8 (Existence of Minimal and Maximal Alternatives). *Let X be a nonempty set and let $\succsim$ be a preference relation on X. At least one member of X is minimal with respect to $\succsim$ in X and at least one member is maximal.*

Proposition H.2.9 (Representing a Preference Relation by a Utility Function). *Every preference relation on a finite set can be represented by a utility function.*

Bibliography

Abreu, Dilip, David Pearce, and Ennio Stacchetti (1990). "Toward a Theory of Discounted Repeated Games with Imperfect Monitoring". In: *Econometrica* 58.5, pp. 1041–1063.

Aigner, Martin and Günter M. Ziegler (1998). *Proofs from THE BOOK*. Berlin: Springer-Verlag.

Aliprantis, Charalambos D. and Kim C. Border (2006). *Infinite Dimensional Analysis: A Hitchhiker's Guide*. 3rd ed. Berlin: Springer. DOI: 10.1007/3-540-29587-9.

Arrow, Kenneth J. and Gérard Debreu (1954). "Existence of an Equilibrium for a Competitive Economy". In: *Econometrica* 22.3, pp. 265–290.

Aumann, Robert J. (1964). "Markets with a Continuum of Traders". In: *Econometrica* 32.1/2, pp. 39–50.

– (1966). "Existence of Competitive Equilibria in Markets with a Continuum of Traders". In: *Econometrica* 34.1, pp. 1–17.

Birkhoff, Garrett and Saunders Mac Lane (1997). *A Survey of Modern Algebra*. 5th. Natick, MA: A K Peters.

Border, Kim C. (1985). *Fixed Point Theorems with Applications to Economics and Game Theory*. Cambridge: Cambridge University Press.

Bridges, Douglas S. (1998). *Foundations of Real and Abstract Analysis*. Vol. 174. Graduate Texts in Mathematics. New York: Springer-Verlag.

Cantor, Georg (1955). *Contributions to the Founding of the Theory of Transfinite Numbers*. New York: Dover Publications.

Cournot, Antoine Augustin (1838). *Recherches sur les principes mathématiques de la théorie des richesses*. Paris: L. Hachette.

Debreu, Gérard (1959). *Theory of Value: An Axiomatic Analysis of Economic Equilibrium*. Cowles Foundation Monograph 17. New Haven, CT: Yale University Press.

Debreu, Gérard and Herbert Scarf (1963). "A Limit Theorem on the Core of an Economy". In: *International Economic Review* 4.3, pp. 235–246.

Edgeworth, Francis Ysidro (1881). *Mathematical Psychics: An Essay on the Application of Mathematics to the Moral Sciences*. London: C. Kegan Paul.

Fraenkel, Abraham A. (1966). *Set Theory and Logic*. Reading, MA: Addison-Wesley.

Fudenberg, Drew and Jean Tirole (1991). *Game Theory.* Cambridge, MA: The MIT Press.

Green, Jerry R. and Walter P. Heller (1981). "Mathematical Analysis and Convexity with Applications to Economics". In: *Handbook of Mathematical Economics.* Ed. by Kenneth J. Arrow and Michael D. Intriligator. Vol. 1. Amsterdam: North-Holland, pp. 15–52.

Mas-Colell, Andreu, Michael D. Whinston, and Jerry R. Green (1995). *Microeconomic Theory.* New York, NY: Oxford University Press.

McKenzie, Lionel W. (1959). "On the Existence of General Equilibrium for a Competitive Market". In: *Econometrica* 27.1, pp. 54–71.

Munkres, James R. (2000). *Topology.* 2nd. Upper Saddle River, NJ: Prentice Hall.

Nash, John (1951). "Non-Cooperative Games". In: *Annals of Mathematics.* Second Series 54.2, pp. 286–295.

Nash, John F. (1950). "Equilibrium Points in n-Person Games". In: *Proceedings of the National Academy of Sciences* 36.1, pp. 48–49.

Neumann, John von and Oskar Morgenstern (1944). *Theory of Games and Economic Behavior.* Princeton, NJ: Princeton University Press.

Pareto, Vilfredo (1906). *Manuale di economia politica.* Milan: Società Editrice Libraria.

– (1896–1897). *Cours d'économie politique.* Vol. 1–2. Two volumes. Lausanne: F. Rouge.

Rudin, Walter (1976). *Principles of Mathematical Analysis.* 3rd. New York: McGraw-Hill.

Smith, Adam (1776). *An Inquiry into the Nature and Causes of the Wealth of Nations.* London: W. Strahan and T. Cadell.

Walras, Léon (1874). *Éléments d'économie politique pure, ou théorie de la richesse sociale.* Lausanne: L. Corbaz.

Weiss, Ittay (2015). "Survey Article: The real numbers–a survey of constructions". In: *Rocky Mountain Journal of Mathematics* 45.3, pp. 737–762. DOI: 10.1216/RMJ-2015-45-3-737.