

The Foundations of Real Analysis

A Fundamental Course with 347 Exercises
and Detailed Solutions

Richard Mikula



BrownWalker Press
Boca Raton

*The Foundations of Real Analysis:
A Fundamental Course with 347 Exercises and Detailed Solutions*

Copyright © 2015 Richard Mikula

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher.

BrownWalker Press
Boca Raton, Florida
USA • 2015

ISBN-10: 1-62734-565-5
ISBN-13: 978-1-62734-565-1

www.brownwalker.com

Cover design by Marija Milanovic

Macrovector used under license from Shutterstock.com

Publisher's Cataloging-in-Publication Data

Mikula, Richard, 1975-

The foundations of real analysis : a fundamental course with 347 exercises and detailed solutions / Richard Mikula.

pages cm

Includes bibliographical references and index.

ISBN: 978-1-62734-565-1 (pbk.)

1. Functions of real variables. 2. Mathematical analysis. 3. Transcendental functions—Textbooks. 4. Trigonometry—Textbooks. 5. Calculus—Textbooks. I. Title.

QA300 .M55 2015

515`.8—dc23

2015951048

Contents

1	The Set of Real Numbers	11
1.1	Introduction	11
1.2	Fields and the Set of Rational Numbers	11
1.2.1	Fields in the Algebraic Sense	11
1.2.2	The Rational Numbers and the Integers, a Rigorous Discussion	19
1.2.3	Homework Exercises	27
1.3	Further Properties of the Real Numbers	29
1.3.1	Positivity and Ordering on Fields	29
1.3.2	The Completeness Axiom of the Set of Real Numbers	31
1.3.3	Some Further Properties of the Set of Real Numbers	34
1.3.4	Homework Exercises	43
1.4	The Construction of the Real Numbers	46
1.4.1	Dedekind Cuts and the Construction of the Real Numbers	46
1.4.2	The Uniqueness of a Complete Ordered Field up to Isomorphism	56
1.5	The Complex Numbers	60
1.5.1	Homework Exercises	62
2	Elementary Point-Set Topology	65
2.1	Euclidean Spaces	65
2.1.1	Intervals in Euclidean Space	67
2.1.2	Balls or Disks in Euclidean Space	68
2.1.3	Convexity in Euclidean Space	69
2.2	Metric Spaces	70
2.3	Open Sets and Closed Sets	70
2.3.1	Open Sets	70

2.3.2	Closed Sets	71
2.3.3	Unions and Intersections of Open and Closed Sets	73
2.3.4	Homework Exercises	74
2.4	Compactness	76
2.4.1	Homework Exercises	84
2.5	Connectedness	84
2.6	The Cantor Set	85
2.6.1	Perfect Subsets of Euclidean Space	85
2.6.2	The Construction of the Cantor Set	86
2.6.3	Homework Exercises	87
3	Sequences and Series of Real Numbers	89
3.1	Limits of Sequences	89
3.1.1	Homework Exercises	92
3.1.2	Properties of Limits	92
3.1.3	Bounded Monotone Sequences	95
3.1.4	Homework Exercises	97
3.2	Subsequences	98
3.2.1	Homework Exercises	99
3.3	Limit Superior and Limit Inferior	100
3.3.1	Homework Exercises	101
3.4	Cauchy Sequences	103
3.4.1	Homework Exercises	105
3.5	Series	106
3.5.1	Geometric and Telescoping Series	109
3.5.2	Series of Non-negative Terms	111
3.5.3	The Root Test and the Ratio Test	114
3.5.4	Homework Exercises	118
3.5.5	The Number e	120
3.5.6	Alternating Series	122
3.5.7	Absolute and Conditional Convergence	125
3.5.8	The Algebra of Series	127
3.5.9	Rearrangements of Series	128
3.5.10	Power Series	133
3.5.11	Homework Exercises	136

4	Limits and Continuity	139
4.1	Limits of Functions	139
4.1.1	Properties of Limits	140
4.1.2	Homework Exercises	143
4.2	Continuous Functions	143
4.2.1	The Exponential and Logarithmic Functions	146
4.2.2	A Topological Characterization of Continuity	152
4.2.3	Continuity and Compactness	153
4.2.4	Continuity and Connectedness	154
4.2.5	Uniform Continuity	154
4.2.6	Discontinuities	156
4.2.7	Semicontinuity, \limsup and \liminf	157
4.3	Monotone Functions	158
4.4	Infinite Limits and Limits at Infinity	160
4.5	Homework Exercises	162
5	Differentiation	167
5.1	Definitions and Basic Differentiability Results	167
5.1.1	Derivatives of Some Functions	169
5.1.2	Approximation by Linear Functions	173
5.1.3	The Product and Quotient Rule	173
5.1.4	The Chain Rule	175
5.1.5	The Trigonometric Functions	177
5.1.6	Homework Exercises	190
5.2	Extrema for Functions	191
5.3	The Mean Value Theorem	192
5.3.1	The Inverse Function Theorem	194
5.3.2	The Continuity of Derivatives and the Intermediate Value Property	197
5.3.3	L'Hôpital's Rule	198
5.3.4	Homework Exercises	200
5.4	Higher Order Derivatives	201
5.4.1	Homework Exercises	201
5.5	Monotonicity, Concavity and Convexity	202
5.5.1	Some Monotonicity Results	202
5.5.2	The First and Second Derivative Tests	202
5.5.3	Concavity and Convexity	204
5.5.4	Homework Exercises	208

5.6	Taylor's Theorem	208
5.6.1	Some Examples	210
5.6.2	Homework Exercises	211
5.7	Newton's Method	211
5.7.1	Homework Exercises	214
6	The Riemann Integral	217
6.1	Riemann Sums and the Riemann Integral	217
6.1.1	The Existence of Riemann Integrable Functions	219
6.1.2	Linearity and Comparative Properties of the Integral	220
6.1.3	A Cauchy Convergence Criterion for Integrability	222
6.1.4	Some Examples	224
6.1.5	Further Properties of Riemann Integrable Functions	226
6.1.6	Upper and Lower Sums and the Darboux Integral	232
6.1.7	A Sufficient Condition for Integrability	238
6.1.8	Additive Properties of the Riemann Integral	239
6.1.9	Homework Exercises	243
6.2	The Fundamental Theorem of Calculus	244
6.2.1	Integral Representation of Some Transcendental Functions	247
6.2.2	Homework Exercises	248
6.3	Functions of Bounded Variation	249
6.3.1	Homework Exercises	260
6.4	Rectifiable Curves and Arclength	260
6.4.1	Homework Exercises	263
6.5	Lebesgue's Integrability Criterion	264
6.5.1	Sets of Measure Zero	264
6.5.2	The Oscillation of a Function	265
6.5.3	Lebesgue's Criterion for Riemann Integrability	266
6.5.4	Homework Exercises	269
7	Sequences and Series of Functions	271
7.1	Point-wise Convergence	271
7.1.1	Homework Exercises	273
7.2	Uniform Convergence	274
7.2.1	Uniform Convergence and Continuity	276
7.2.2	Uniform Convergence and Integration	278
7.2.3	Uniform Convergence and Differentiation	279

7.2.4	Homework Exercises	281
7.3	Series of Functions	283
7.3.1	Uniform Convergence of Power Series	284
7.3.2	Homework Exercises	287
7.4	Equicontinuity	287
7.4.1	Properties of Convergent Sequences of Functions	287
7.4.2	The Ascoli-Arzelà Theorem and Compactness	290
7.4.3	Homework Exercises	292
7.5	Uniform Approximation by Polynomials	293
7.5.1	The Weierstrass Approximation Theorem	294
8	Functions of Several Real Variables	297
8.1	The Algebra and Topology of \mathbb{R}^n	297
8.1.1	\mathbb{R}^n as a Normed Linear Space	298
8.1.2	Homework Exercises	305
8.2	Linear Transformations and Affine Functions	306
8.2.1	Linear Transformations on Vector Spaces	306
8.2.2	Homework Exercises	311
8.2.3	Affine Functions	311
8.3	Differentiation	312
8.3.1	The Chain Rule	315
8.3.2	The Gradient and Directional Derivatives	316
8.3.3	Taylor's Theorem, the Second Derivative and Extreme Values	320
8.3.4	Homework Exercises	325
8.4	The Inverse Function and Implicit Function Theorems	327
8.4.1	The Contraction Mapping Principle	327
8.4.2	The Inverse Function Theorem	328
8.4.3	The Implicit Function Theorem	333
8.4.4	Homework Exercises	338
9	The Lebesgue Integral	339
9.1	Lebesgue Outer Measure and Measurable Sets	339
9.1.1	The Lebesgue Outer Measure	339
9.1.2	The Lebesgue Measure	342
9.1.3	Homework Exercises	352
9.2	Lebesgue Measurable Functions	353
9.2.1	Sequences of Measurable Functions	355

9.2.2	Homework Exercises	360
9.3	The Riemann and Lebesgue Integrals	362
9.3.1	The Riemann Integral in \mathbb{R}^n	362
9.3.2	The Lebesgue Integral of Non-Negative Functions in \mathbb{R}^n	373
9.3.3	Lebesgue Integral for a Measurable Function of Any Sign	382
9.3.4	Homework Exercises	389
9.4	Iterated Integration and Fubini's Theorem	392
9.4.1	Convolutions	397
9.4.2	Homework Exercises	398
A	Preliminary Materials	401
A.1	Sets and Related Notation	401
A.2	Notation in Symbolic Logic	402
A.3	The Basics in Symbolic Logic	402
A.4	Quantified Sentences in Symbolic Logic	405
A.4.1	Negations of Quantified Sentences	407
A.5	Equivalence Relations	408
A.6	The Natural Numbers and Induction	409
A.6.1	The Well-Ordering Principle	411
A.6.2	Inductive Sets	412
A.6.3	How the Principle of Mathematical Induction is Used in Proofs	413
A.6.4	The Principle of Complete Induction	413
B	Homework Solutions	415
B.1	Homework Solutions 1.2.3	415
B.2	Homework Solutions 1.3.4	418
B.3	Homework Solutions 1.5.1	421
B.4	Homework Solutions 2.3.4	422
B.5	Homework Solutions 2.4.1	425
B.6	Homework Solutions 2.6.3	426
B.7	Homework Solutions 3.1.1	426
B.8	Homework Solutions 3.1.4	427
B.9	Homework Solutions 3.2.1	429
B.10	Homework Solutions 3.3.1	430
B.11	Homework Solutions 3.4.1	434
B.12	Homework Solutions 3.5.4	435
B.13	Homework Solutions 3.5.11	437

B.14 Homework Solutions 4.1.2	439
B.15 Homework Solutions 4.5	440
B.16 Homework Solutions 5.1.6	447
B.17 Homework Solutions 5.3.4	448
B.18 Homework Solutions 5.4.1	449
B.19 Homework Solutions 5.5.4	450
B.20 Homework Solutions 5.6.2	451
B.21 Homework Solutions 5.7.1	453
B.22 Homework Solutions 6.1.9	453
B.23 Homework Solutions 6.2.2	457
B.24 Homework Solutions 6.3.1	459
B.25 Homework Solutions 6.4.1	461
B.26 Homework Solutions 6.5.4	462
B.27 Homework Solutions 7.1.1	463
B.28 Homework Solutions 7.2.4	464
B.29 Homework Solutions 7.3.2	468
B.30 Homework Solutions 7.4.3	469
B.31 Homework Solutions 8.1.2	471
B.32 Homework Solutions 8.2.2	474
B.33 Homework Solutions 8.3.4	476
B.34 Homework Solutions 8.4.4	480
B.35 Homework Solutions 9.1.3	482
B.36 Homework Solutions 9.2.2	485
B.37 Homework Solutions 9.3.4	489
B.38 Homework Solutions 9.4.2	494

Chapter 1

The Set of Real Numbers

1.1 Introduction

Real Analysis must begin with the set of real numbers \mathbb{R} , along with the two binary operations addition $+$ and multiplication \cdot , which makes $(\mathbb{R}, +, \cdot)$ a field in the algebraic sense. In fact $(\mathbb{R}, +, \cdot)$ can be called the only *complete, ordered field*, with "only" being up to algebraic isomorphism of rings.

It is the completeness property of \mathbb{R} that is essential to calculus, and many of its results. Note that $(\mathbb{Q}, +, \cdot)$ is an ordered field, where \mathbb{Q} being the set of rational numbers $\{\frac{m}{n} : m, n \text{ integers, and } n \neq 0\}$. However \mathbb{Q} is not complete. To see this, take for instance terms in the sequence

$$1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, \dots$$

that is the sequence of terms $\{a_n\}_{n=0}^{\infty}$ which have the decimal expansion for $\sqrt{2}$ out to the $(10)^{-n}$ th place. Clearly all the terms in this sequence are rational, however, if the sequence converges, it must converge to $\sqrt{2} \notin \mathbb{Q}$. Thus \mathbb{Q} is not complete.

1.2 Fields and the Set of Rational Numbers

1.2.1 Fields in the Algebraic Sense

Let \mathbb{F} be a set that has the following binary relations $+$: $\mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$ and \cdot : $\mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$, called addition and multiplication respectively. We will assume

that the triple $(\mathbb{F}, +, \cdot)$ satisfies the following list of properties:

For any $x, y, z \in \mathbb{F}$

1. **Commutativity of Addition:**

$$x + y = y + x$$

2. **Associativity of Addition:**

$$x + (y + z) = (x + y) + z$$

3. **Existence of Zero:** There is an element $0 \in \mathbb{F}$, called **zero**, which satisfies

$$0 + x = x$$

for all $x \in \mathbb{F}$.

4. **Additive Inverse:** For each $x \in \mathbb{F}$ there is a $-x \in \mathbb{F}$ so that

$$x + (-x) = 0.$$

5. **Commutativity of Multiplication:**

$$x \cdot y = y \cdot x$$

6. **Associativity of Multiplication:**

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

7. **Existence of Unity¹:** There is an element $1 \in \mathbb{F}$, called **one**, so that

$$1 \cdot x = x$$

for all $x \in \mathbb{F}$.

8. **Multiplicative Inverse:** For each non-zero $x \in \mathbb{F}$ there is a $x^{-1} \in \mathbb{F}$ so that

$$x \cdot x^{-1} = 1$$

¹Unity in a ring refers to 1.

9. **Distributive Property:** $+$ and \cdot are related by

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

Needless to say $1, 0 \in \mathbb{F}$ may not be the $1, 0$ in the set of real numbers.

Such an ordered triple $(\mathbb{F}, +, \cdot)$ is called a **field**.

The Set of Natural Numbers

There is an important set of numbers called the **natural numbers**², denoted by \mathbb{N} , and which satisfies the property that $1 \in \mathbb{N}$, and if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$. Moreover, there does not exist an $m \in \mathbb{N}$ so that $m + 1 = 1$. Here of course \mathbb{N} has two binary operations $+$, \cdot .³ Moreover, the set of natural numbers is closed under $+$ and \cdot and satisfies the following list of properties for any $k, m, n \in \mathbb{N}$:

1. **Associativity:**

$$k + (m + n) = (k + m) + n, \quad k \cdot (m \cdot n) = (k \cdot m) \cdot n$$

2. **Commutativity:**

$$k + m = m + k, \quad k \cdot m = m \cdot k$$

3. **Existence of a Unity:** There is an element $1 \in \mathbb{N}$, called **one**, so that

$$1 \cdot k = k$$

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

²The natural numbers \mathbb{N} can actually be characterized by the following five axioms: A1: $1 \in \mathbb{N}$. A2: $\forall x \in \mathbb{N}$ there exists a unique $(x + 1) \in \mathbb{N}$, called the successor of x . A3: $\forall x \in \mathbb{N}$, $x + 1 \neq 1$. That is 1 is not the successor of any natural number. A4: If $x + 1 = y + 1$, then $x = y$. A5 (the axiom of induction): Suppose $A \subseteq \mathbb{N}$ satisfies: $1 \in A$; $x \in A$ implies $(x + 1) \in A$. Then $A = \mathbb{N}$. For a complete construction of the properties of \mathbb{N} see for instance [7].

³Although we are using the same notation for $+$, \cdot for both our field \mathbb{F} and \mathbb{N} , as well as for the element $1 \in \mathbb{F}$ and $1 \in \mathbb{N}$, they are unrelated in general.

4. **Cancellation Property:**

$$k + m = k + n \Rightarrow m = n$$

$$k \cdot m = k \cdot n \Rightarrow m = n$$

5. **The Distributive Property:**

$$k \cdot (m + n) = (k \cdot m) + (k \cdot n)$$

6. For a given pair of natural numbers m, n one and only one of the following holds:

- $m = n$,
- $m = n + k$ for some $k \in \mathbb{N}$,
- $n = m + k$ for some $k \in \mathbb{N}$.

This in turn allows us to define an ordering on \mathbb{N} . The following are **order properties**:

- (a) $m < n$ if and only if there exists $j \in \mathbb{N}$ so that $n = m + j$.
- (b) $m \leq n$ if and only if $m < n$ or $m = n$.
- (c) $k < m$ and $m < n$ implies $k < n$.
- (d) $m \leq n$ and $n \leq m$ implies $m = n$.
- (e) $m < n$ implies $m + k < n + k$ and $k \cdot m < k \cdot n$.

Moreover, we also have the following axiom for the set \mathbb{N} of natural numbers:

The Axiom of Induction: Let $S \subseteq \mathbb{N}$. Suppose S satisfies

1. $1 \in S$.
2. $n \in S$ implies $n + 1 \in S$.

Then $S = \mathbb{N}$.

From this characterization of \mathbb{N} in terms of the above properties, we see that $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.

The Set of Integers

From the set of natural numbers we may define the set of **integers**, denoted by⁴ \mathbb{Z} , that has the same binary operations $+$, \cdot and is closed under these operations.⁵ \mathbb{Z} contains \mathbb{N} as a subset, and also contains an element 0 so that $m + 0 = m$ for all $m \in \mathbb{Z}$. Moreover, for any $m \in \mathbb{Z}$ we have $m = 0$, $m \in \mathbb{N}$ or $-m \in \mathbb{N}$, where $m + (-m) = 0$. Thus we see that $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$. \mathbb{Z} satisfies all the field axioms except the axiom which says that every non-zero element x has a multiplicative inverse x^{-1} . Moreover, the set of integers also satisfies the **cancellation property**⁶, and so \mathbb{Z} cannot have any zero divisors, that is

$$x \cdot y = 0 \quad \Rightarrow \quad x = 0, \quad \text{or} \quad y = 0.$$

Moreover, on \mathbb{Z} we may define an ordering via the relation $<$, where $m < n$ if and only if $n + (-m) \in \mathbb{N}$.

The Set of Rational Numbers

From the set of integers, we may construct set set of **rational numbers**, denoted by \mathbb{Q} , which are defined by

$$\mathbb{Q} := \{a \cdot b^{-1} : a, b \in \mathbb{Z}, b \neq 0\}. \quad (1.1)$$

We may think of this as the algebraic extension of the integral domain \mathbb{Z} to a field of fractions. In a later section we shall give a rigorous construction of \mathbb{Q} from \mathbb{Z} , as well as a rigorous construction of \mathbb{Z} from \mathbb{N} .

Notational Conventions for Fields

The following is a list of standard notational conventions:

1. We often write xy instead of $x \cdot y$.
2. We define **subtraction** by

$$x - y := x + (-y).$$

⁴ \mathbb{Z} for the German *Zahl*, which means number.

⁵In a later section we shall give a rigorous argument for the construction of \mathbb{Z} from \mathbb{N} .

⁶ $a \cdot b = a \cdot c$ and $a \neq 0$ implies $b = c$

3. We often write $\frac{1}{x}$ instead of x^{-1} .
4. We define **division** by

$$x \div y \text{ or } \frac{x}{y} := x \cdot y^{-1}$$

for $x \in \mathbb{F}$, and $y \neq 0$ in \mathbb{F} .

5. We define **powers** of a element x by $x^1 := x$, $x^2 := x \cdot x$, $x^3 := x \cdot x^2 = x \cdot x \cdot x$ and for n a positive integer

$$x^{n+1} := x \cdot x^n.$$

For n a positive integer, we define x^{-n} as $(x^{-1})^n$ or equivalently $(x^n)^{-1}$. Since both ways to define this will agree with one another.

6. We define **multiples** of an element x by $1x := x$, $2x := x + x$, $3x := x + 2x = x + x + x$, and for a positive integer n by

$$(n + 1)x = x + nx.$$

Moreover, because of the distributive property, we have

$$n \cdot x = nx.$$

That is,

$$\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}}.$$

Note as well

$$\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} \cdot x$$

where here $1 \in \mathbb{F}$.

7. Order of Operations:

- (a) Operations in parentheses are performed first, working with the inner most first. In the innermost parentheses, or in the absence of parentheses, follow the remaining steps.
- (b) Powers are computed first, going from left to right.

- (c) Multiplication and division are performed next (with equal weight) going from left to right.
- (d) Addition and subtraction are performed after all multiplications and divisions have been performed. Addition and subtraction (which hold equal weight) are performed from left to right.

Thus, we see that we may write the distributive property as

$$x(y + z) = xy + xz.$$

Some Consequences of the Field Axioms

The following result shows that additive and multiplicative inverses for a fixed element x are unique, and the elements 1 and 0 are unique in a field \mathbb{F} .

Proposition 1.2.1 *The elements 0 and 1 of a field are unique. Moreover, for a given element $x \in \mathbb{F}$, the additive inverse $-x$ is unique, and for $x \neq 0$ the multiplicative inverse x^{-1} is unique.*

Proof: Suppose that there are two elements $0_1, 0_2 \in \mathbb{F}$ such that $0_1 + x = x$ and $0_2 + x = x$ for any $x \in \mathbb{F}$. Then $0_1 + 0_2 = 0_2$ by using $x = 0_2$, and $0_1 + 0_2 = 0_1$ by using $x = 0_1$. Thus, $0_1 = 0_2$. Next, we suppose there are two elements $1_1, 1_2 \in \mathbb{F}$ such that $1_1 \cdot x = x$ and $1_2 \cdot x = x$. Then $1_1 \cdot 1_2 = 1_2$ by using $x = 1_2$ and on the other hand $1_1 \cdot 1_2 = 1_1$ by using $x = 1_1$. Thus, $1_1 = 1_2$.

Now, given $x \in \mathbb{F}$, suppose there are two elements $y, z \in \mathbb{F}$ so that $x + y = 0$ and $x + z = 0$. Then, by associativity we have

$$y = y + 0 = y + (x + z) = (y + x) + z = 0 + z = z.$$

Given $x \neq 0$, suppose there are two elements $y, z \in \mathbb{F}$ so that $xy = 1$ and $xz = 1$. Then, by associativity we have

$$y = y \cdot 1 = y(xz) = (yx)z = 1 \cdot z = z.$$

□

Since additive and multiplicative inverses are unique,

$$-(-x) = x, \quad \frac{1}{\frac{1}{x}} = (x^{-1})^{-1} = x \quad (1.2)$$

Another important result to note is the **cancellation property**:

Proposition 1.2.2 *If $x + y = x + z$, then $y = z$. Moreover, if $x \neq 0$ and $xy = xz$, then $y = z$.*

Proof: If $x + y = x + z$, by adding $-x$ to both sides we get

$$\begin{aligned} y &= 0 + y = (-x + x) + y = -x + (x + y) \\ &= -x + (x + z) = (-x + x) + z = 0 + z = z. \end{aligned}$$

Moreover, if $x \neq 0$ and $xy = xz$, by multiplying both sides by x^{-1} we get

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = 1 \cdot z = z.$$

□

The next result relates $(-1) \cdot x$ to $-x$ and also gives us the property $0 \cdot x = 0$, neither of which are axioms of our field \mathbb{F} .

Proposition 1.2.3 *For any $x \in \mathbb{F}$ we have $(-1) \cdot x = -x$ and $0 \cdot x = 0$. Moreover, $(-1)^2 = 1$.*

Proof: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$ and thus by the cancellation property we have

$$0 \cdot x = 0.$$

To show $(-1) \cdot x = -x$ we will show $(-1) \cdot x$ is the additive inverse $-x$, and thus by uniqueness of inverses, we get the result. To see this, note

$$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1 + 1) \cdot x = 0 \cdot x = 0.$$

For the last result, we will show $(-1)^2$ is the additive inverse of -1 .

$$-1 + (-1)^2 = (-1) \cdot 1 + (-1)^2 = (-1) \cdot (1 + (-1)) = (-1) \cdot 0 = 0.$$

□

A consequence of the above proposition is that for any $x, y \in \mathbb{F}$ we have

$$(-x) \cdot y = -(x \cdot y) = x \cdot (-y) \quad (1.3)$$

To see this, we use the property $-x = (-1) \cdot x$, and thus

$$(-x) \cdot y = ((-1) \cdot x) \cdot y = (-1) \cdot (x \cdot y) = -(x \cdot y).$$

To see the other equality, we use commutativity, and reverse the roles of x and y .

Moreover, we also have

$$(-x) \cdot (-y) = x \cdot y,$$

since

$$(-x) \cdot (-y) = (-1)^2 \cdot x \cdot y.$$

The next result tells us that there are no zero divisors in a field.

Proposition 1.2.4 *Suppose that $x \cdot y = 0$, then either $x = 0$ or $y = 0$.*

Proof: Suppose $x \cdot y = 0$ and $x \neq 0$. Then multiplying $x \cdot y = 0$ by $\frac{1}{x}$ we get

$$0 = \frac{1}{x} \cdot 0 = \frac{1}{x} \cdot (x \cdot y) = \left(\frac{1}{x} \cdot x\right) \cdot y = 1 \cdot y = y.$$

□

1.2.2 The Rational Numbers and the Integers, a Rigorous Discussion

In this section we will discuss the construction of the set of integers from the set of natural numbers, and then a construction of the set of rational numbers from the set of integers. We will think of the set of rational numbers as an algebraic extension of the set of integers (as an integral domain) to a field.

The Construction of the Integers from the Natural Numbers

Consider the set $\mathbb{N} \times \mathbb{N}$. On this set we define a relation⁷ R by

$$(a, b) \sim_R (c, d) \iff a + d = b + c. \quad (1.4)$$

We claim that R is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. Clearly $(a, b) \sim_R (a, b)$ since $a + b = b + a$, and thus R is reflexive. Likewise, if $(a, b) \sim_R (c, d)$, then $a + d = b + c$. By commutativity of addition on \mathbb{N} , we know that $c + b = d + a$, and so $(c, d) \sim_R (a, b)$. Hence R is a symmetric relation on $\mathbb{N} \times \mathbb{N}$. Next, we suppose that $(a, b) \sim_R (c, d)$ and $(c, d) \sim_R (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Adding f to the first equation $a + d = b + c$ we get $a + d + f = b + c + f$, and then using the second equation $c + f = d + e$ we get $b + c + f = b + d + e$, and so $a + d + f = b + d + e$. By the cancellation property of \mathbb{N} , we may conclude that $a + f = b + e$, and so $(a, b) \sim_R (e, f)$. Thus we see that R is a transitive relation on $\mathbb{N} \times \mathbb{N}$. This allows us to define \mathcal{Z} to be the set of equivalence classes defined by this relation on $\mathbb{N} \times \mathbb{N}$. Let $[a, b]$ denote the equivalence class of $(a, b) \in \mathbb{N} \times \mathbb{N}$ with respect to this equivalence relation R .

On \mathcal{Z} we define an operation $+$ by $[a, b] + [c, d] := [a + c, b + d]$. Likewise, we define an operation \cdot by $[a, b] \cdot [c, d] := [ac + bd, ad + bc]$. Now it is our job to show that on \mathcal{Z} the operations $+$ and \cdot as defined are well-defined. Moreover, \mathcal{Z} is closed with respect to $+$ and \cdot . On \mathcal{Z} , $+$ is commutative and associative, \cdot is commutative and associative, and $+$ and \cdot satisfy a distributive property.

First we address the well-defined nature of our definitions of $+$ and \cdot . Suppose $[a, b] = [a', b']$, and $[c, d] = [c', d']$. In other words, $(a, b) \sim_R (a', b')$ and $(c, d) \sim_R (c', d')$. We claim that $[a, b] + [c, d] = [a', b'] + [c', d']$ and $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$. In order to see this, we first observe that for any $n \in \mathbb{N}$ we have that $[a, b] = [a + n, b + n]$, since $a + (b + n) = b + (a + n)$. Now,

$$\begin{aligned} [a, b] + [c, d] &= [a + c, b + d] \\ &= [a + c + a' + c', b + d + a' + c'] \\ &= [a + c + a' + c', a' + b + c' + d] \end{aligned}$$

⁷Our motivation is (a, b) should be thought of as $a - b$, since we may obtain \mathbb{Z} from \mathbb{N} by taking all possible differences of two natural numbers.

$$\begin{aligned}
&= [a + c + a' + c', a + c + b' + d'] \\
&= [a' + c', b' + d'] \\
&= [a', b'] + [c', d'].
\end{aligned}$$

Likewise,

$$\begin{aligned}
[a, b] \cdot [c, d] &= [ac + bd, ad + bc] \\
&= [ac + bd + ac' + bd', ac' + ad + bd' + bc] \\
&= [ac + bd + ac' + bd', a(c' + d) + b(d' + c)] \\
&= [ac + bd + ac' + bd', a(c + d') + b(d + c')] \\
&= [ac + bd + ac' + bd', ac + bd + c'b + d'a] \\
&= [ac' + bd', c'b + d'a] \\
&= [ac' + bd' + a'c' + b'd', c'a' + c'b + d'b' + d'a] \\
&= [ac' + bd' + a'c' + b'd', c'(a' + b) + d'(b' + a)] \\
&= [ac' + bd' + a'c' + b'd', c'(a + b') + d'(b + a')] \\
&= [ac' + bd' + a'c' + b'd', ac' + bd' + a'd' + b'c'] \\
&= [a'c' + b'd', a'd' + b'c'] \\
&= [a', b'] \cdot [c', d'].
\end{aligned}$$

We leave it as an exercise to the reader to show the associativity and commutativity of both $+$ and \cdot as defined on \mathcal{Z} .

Next, we address the distributive property, which relates the operations $+$ and \cdot .

$$\begin{aligned}
[a, b] \cdot ([c, d] + [e, f]) &= [a, b] \cdot [c + e, d + f] \\
&= [a(c + e) + b(d + f), a(d + f) + b(c + e)] \\
&= [(ac + bd) + (ae + bf), (ad + bc) + (af + be)] \\
&= [ac + bd, ad + bc] + [ae + bf, af + be] \\
&= ([a, b] \cdot [c, d]) + ([a, b] \cdot [e, f]).
\end{aligned}$$

Next, we will show how to embed \mathbb{N} into \mathcal{Z} , and we will do this via the identification of \mathbb{N} with the elements of \mathcal{Z} in the subset $\mathcal{P} := \{[m, n] : m > n\}$. First, we claim that $[m, n] \in \mathcal{P}$ has a representation of the form $[n + k, n]$.

This is clear from the fact that $m > n$ in \mathbb{N} means that $m = n + k$ for some $k \in \mathbb{N}$. We claim that \mathcal{P} is isomorphic to \mathbb{N} relative to the operations $+$, \cdot as defined on each set. Since we can think of elements of \mathcal{P} as elements of the form $[n+k, n]$, we define the mapping $k \mapsto [n+k, n]$, where $n \in \mathbb{N}$ is any fixed natural number. Since $[k+m, m] = [k+n, n]$ for all $m, n \in \mathbb{N}$, what we are defining is well-defined and the mapping $k \mapsto [n+k, n]$ is thus independent of the natural number n . This is an isomorphism of rings since $[k+m, m] = [j+n, n]$ if and only if $k = j$. Likewise, $[k+n, n] + [j+m, m] = [k+j+m+n, m+n]$ and $[k+n, n] \cdot [j+m, m] = [(k+n)(j+m) + nm, (k+n)m + n(j+m)] = [jk+l, l]$ where $l = nj + km + 2nm$.

We define the zero of \mathcal{Z} to be the element $[m, m]$, where $m \in \mathbb{N}$ is any fixed integer. Clearly $[j, k] + [m, m] = [j+k, k+m] = [j, k]$, $[j, k] \cdot [m, m] = [jm+km, jm+km] = [m, m]$. We define the negative of an element $[j, k]$ to be $[k, j]$ since $[j, k] + [k, j] = [j+k, k+j] = [m, m]$. From this we see that we can identify the collection of negatives of elements of \mathcal{P} with the collection of elements of the form $[j, j+k]$, and such an element can be thought of as the negative of the natural number k . Through this, we identify the collection of integers, commonly denoted by \mathbb{Z} with the integral domain \mathcal{Z} .

The Construction of the Rational Numbers from the Integers

In the future we will write a rational number in the form $\frac{m}{n}$ where $m, n \in \mathbb{Z}$ and $n \neq 0$. We will define this collection from $\mathbb{Z} \times \mathbb{Z}$ by defining binary operations $+$, \cdot from those on \mathbb{Z} .

Let

$$Q = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}.$$

We need to identify ordered pairs that would give the same value of $\frac{a}{b}$, where we think of (a, b) as $\frac{a}{b}$ or ab^{-1} . To do this, we define an equivalence relation \sim on Q , which is given by

$$(a, b) \sim (c, d) \iff ad = bc.$$

Clearly $(a, b) \sim (a, b)$ since $ab = ba$. Thus \sim is reflexive.

$$(a, b) \sim (c, d) \iff ad = bc \iff da = cb \iff (c, d) \sim (a, b).$$

Thus we see \sim is symmetric. Moreover, if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then we know $ad = cb$ and $cf = de$. Now,

$$ad = cb \Rightarrow adf = cbf$$

and

$$cf = de \Rightarrow cfb = deb.$$

Since \mathbb{Z} is commutative we know

$$adf = deb,$$

or simply

$$(af)d = (be)d.$$

Since $d \neq 0$, by the cancellation property we may conclude that

$$af = be,$$

and thus

$$(a, b) \sim (e, f).$$

Hence we have shown \sim is transitive.

We have established \sim is an equivalence relation on Q , and hence we may view Q as a disjoint union of equivalence classes. Let $[a, b]$ denote the equivalence class of (a, b) . Let \mathcal{Q} be the set of equivalence classes. On this set we define $+$, \cdot by:

$$[a, b] + [c, d] = [ad + bc, bd]$$

and

$$[a, b] \cdot [c, d] = [ac, bd].$$

To understand these definitions, simply remember the formulae:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

However, before we proceed any further, we must make certain these definitions of $+$, \cdot on \mathcal{Q} are well-defined. That is if $[a, b] = [r, s]$ and $[c, d] = [t, u]$, then

$$[ad + bc, bd] = [a, b] + [c, d]$$

$$= [r, s] + [t, u] = [ru + st, su]$$

and

$$[ac, bd] = [a, b] \cdot [c, d] = [r, s] \cdot [t, u] = [rt, su].$$

That is we actually need to show

$$[ad + bc, bd] = [ru + st, su]$$

and

$$[ac, bd] = [rt, su]$$

whenever $(a, b) \sim (r, s)$ and $(c, d) \sim (t, u)$.

Taking the condition $as = br$ and multiplying both sides by cu gives

$$ascu = brcu.$$

However, $cu = dt$ and thus

$$ascu = bdrt,$$

which implies

$$[ac, bd] = [rt, su].$$

Taking the condition $as = br$ and multiplying both sides by du gives

$$adsu = brdu.$$

Taking the condition $cu = dt$, and multiplying both sides by bs gives us

$$bc su = dtbs.$$

Adding these together gives

$$(ad + bc)su = (ru + st)bd,$$

and thus

$$[ad + bc, bd] = [ru + st, su].$$

Thus we see that the binary operations $+$, \cdot on \mathcal{Q} are well-defined. It is left as an exercise to check that addition and multiplication are associative and commutative, and the distributive property holds.

In \mathcal{Q} the element $[0, 1]$ is the zero element, and the element $[1, 1]$ is the unity. The negative of $[a, b]$ is $[-a, b]$ and the multiplicative inverse of a non-zero element $[a, b]$ is $[b, a]$. Thus we see that \mathcal{Q} is a field. Moreover, we can identify \mathbb{Z} with the subset $\{[a, 1] : a \in \mathbb{Z}\}$ and it is clear that we may view \mathcal{Q} as an extension of \mathbb{Z} , since

$$[a, 1] + [b, 1] = [a + b, 1]$$

and

$$[a, 1] \cdot [b, 1] = [ab, 1].$$

Moreover, any non-zero $a \in \mathbb{Z}$ has $[a, 1]$ as an invertible element in \mathcal{Q} .

This field $(\mathcal{Q}, +, \cdot)$ is what we usually called the field of rational numbers $(\mathbb{Q}, +, \cdot)$. We instead use familiar the notation $\frac{a}{b}$ for $[a, b]$.

Order on the Set of Rational Numbers

We may define an ordering on the set of integers, which extends to the set of rational numbers as follows: The **positive** integers are the natural numbers, and the **negative** integers are the integers whose additive inverses are positive. The intersection between these two collections is empty. We say that an integer is **non-negative** if it is positive or zero, and **non-positive** if it is negative or zero.

Note that from its definition, and the property that $-n = (-1) \cdot n$ holds for any $n \in \mathbb{Z}$, as well as $(-1)^2 = 1$, we get that the set of positive integers are closed under \cdot , a positive times a negative is negative, and a negative times a negative is a positive.

We extend the notions of positivity and negativity to set of the rational numbers. We say that a rational number $\frac{m}{n}$ is positive if m, n are either both positive or both negative. A rational number $\frac{m}{n}$ is negative if one of $\{m, n\}$ is positive, and the other is negative. From these definitions, the properties of the set of positive rational numbers and negative rational numbers satisfy: the positive rational numbers are closed under \cdot , a positive times a negative is negative, and a negative times a negative is a positive.