Math 330 - Additional Material

Student edition with proofs

Michael Fochler
Department of Mathematics
Binghamton University

This document contains chapter 3 of the Math 330 lecture notes.

Last update: February 17, 2026

Contents

3 The Axiomatic Method

Introduction 3.1.

The purpose of this chapter is to familiarize the reader with the axiomatic method, often also called the "proof – theorem" method: How to go about proving a mathematic statement, such as the following:

If m and n both are odd integers then their product mn is odd.

The following is a somewhat simplified description of the axiomatic method. To prove a statement such as the one above one has the following to work with:

(a) Axioms: mathematical statements that are declared to be true and that may be used unquestioningly even though they cannot be proven.

(b) Definitions: declarations that allow you to reference a lengthy sentence or collection of sentences with a convenient short expression. As an example, see definition 3.1 below which allows you to use the words "semigroup" and "monoid" as a short for mathematical objects with certain properties. Thus a definition is not statements, i.e., something that is either true or false, and it makes no sense to ask for the proof of a definition.

(c) Propositions, theorems and lemmata: mathematical statements that may be used because they were previously proven.

Most of this document mainly addresses, besides the general mathematical "plumbing" which consists of sets and functions, topics from the realm of analysis, in particular, convergence and continuity. In contrast, this chapter introduces just enough topics from algebra to provide the foundation for the axiomatic definitions of the integers and the rational and real numbers, as can be found in chapters 1, 2, and 8 of [1] Beck/Geoghegan: The Art of Proof. □

3.1 Semigroups and Groups

//

Introduction 3.2. To be added later. □

Definition 3.1 (Semigroups and monoids)**.** ⋆

Given is a nonempty set S with a binary operation $\diamond$,

i.e. an "assignment rule" $(s,t) \mapsto s \diamond t$ which assigns to any two elements $s,t \in S$ a third element $u := s \diamond t \in S$. [1] The pair $(S, \diamond)$ is called a **semigroup** if the operation $\diamond$ satisfies

(3.1) **associativity:** $(s \diamond t) \diamond u = s \diamond (t \diamond u)$ for all $s,t,u \in S$.

A semigroup for which there exists in addition a **neutral element** with respect to the operation$(s,t) \mapsto s \diamond t$, i.e., some $e \in S$ such that

(3.2) $s \diamond e = e \diamond s = s$ for all $s \in S$

is called a **monoid**.

We can write S instead of $(S, \diamond)$ if it is clear which binary operation on S is represented by $\diamond$. □

Example 3.1.

(a) $(\mathbb{Z}, +)$ (the integers with addition) and $(\mathbb{Z}, \cdot)$ (the integers with multiplication) are monoids: Both $+$ and $\cdot$ are associative and addition has zero, multiplication has 1 as neutral element.
(b) The following also are monoids: $(\mathbb{N}, \cdot)$, $(\mathbb{Q}, +)$ and $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$.
(c) In case you have some knowledge about complex numbers: $(\mathbb{C}, +)$ and $(\mathbb{C}, \cdot)$ also are monoids.
(d) Beware: $(\mathbb{N}, +)$ is a semigroup but NOT a monoid since $0 \notin \mathbb{N}$; hence there is no neutral element under addition! □

Example 3.2.

If you do not know from linear algebra or ch.**??** on p.**??** about general vector spaces then skip this example.

If V is a vector space with addition $+$ and scalar multiplication $\cdot$ then $(V, +)$ is a monoid but $(V, \cdot)$ is not. (Why not?) □

The next example is so important that we state it as a proposition. You should review the (preliminary) definition of a function which was given in Definition **??** on p.**??** refresh your memory about function composition (chain rule in calculus!) to understand it.

Proposition 3.1.

Let A be a nonempty set and let $S := \{f : f \text{ is a function } A \to A\}$.

If this is too abstract for you, choose $A := \mathbb{R}$, the set of real numbers. Then the elements of S will be functions such as $f(x) = 3x^2$ and $g(x) = 7x + 5e^x$.

We define a binary operation $\circ$ on S as follows.

$$(f, g) \mapsto g \circ f$$

assigns to two functions $f, g : A \to A$ the function

$$g \circ f : A \to A; \qquad x \mapsto g \circ f(x) := g\big(f(x)\big).$$

$(S, \circ)$ is a monoid.

PROOF:

We need to show that $\circ$ is associative and that S contains a neutral element.

We first prove associativity. For any three functions $f, g, h \in S$ and any $x \in A$ it follows from the definition of $\circ$ that

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

In other words, both the left–hand side $\big((h \circ g) \circ f\big)(x)$ and the right–hand side $\big(h \circ (g \circ f)\big)(x)$ are, for each argument $x \in A$, equal to $h(g(f(x)))$. This shows that those two functions coincide, and we have proven associativity.

We now prove the existence of a neutral element. Let $id_A : A \to A;\;\; x \mapsto x$ be the function which does nothing with its arguments. [2] We have

$$\big(id_A \circ f\big)(x) = id_A\big(f(x)\big) = f(x) = f\big(id_A(x)\big) = \;\big(f \circ id_A\big)(x)$$

for all $x \in A$. It follows that the three assignments $x \mapsto \big(id_A \circ f\big)(x)$, $x \mapsto \big(f \circ id_A\big)(x)$, and $x \mapsto f(x)$ coincide for all x, i.e., they all represent the same function $x \mapsto f(x)$. This proves (3.2) and hence the existence of a neutral element. ■

Theorem 3.1 (Uniqueness of the neutral element in monoids)**.**

Let $(S, \diamond)$ be a monoid and let $e, e' \in S$ such that both

$$s \diamond e \;= e \diamond s \;= s \tag{3.3}$$

$$s \diamond e' \;= e' \diamond s \;= s \tag{3.4}$$

for all $s \in S$. Then $e = e'$.

PROOF: We have

$$e \overset{(3.4)}{=} e' \diamond e \overset{(3.3)}{=} e'.$$

Here we applied (3.4) with $s = e$ and then (3.3) with $s = e'$. ■

Example 3.3.

Here is an example of a binary operation which is not associative. For integers m and n we define $m \diamond n \;:=\; |n - m|$, i.e., the distance between m and n. This operation is not associative for all $m, n \in \mathbb{Z}$. To prove that such is the case, we only need to find **one counterexample**, i.e., three specific integers m, n, k such that $(m \diamond n) \diamond k \neq m \diamond (n \diamond k)$. This kind of proof is called a **proof by counterexample**. We choose $m = 5$, $n = 3$, $k = 7$ and obtain

$$(5 \diamond 3) \diamond 7 \;= 2 \diamond 7 \;=\; 5, \quad \text{but } \; 5 \diamond (3 \diamond 7) \;=\; 5 \diamond 4 \;=\; 1.$$

It follows that $(\mathbb{Z}, \diamond)$ is not a semigroup. Note that 0 is not a neutral element for $(\mathbb{Z}, \diamond)$, because $n \diamond 0 = |n|$ does not equal n whenever $n < 0$.

What if we replace $\mathbb{Z}$ with the set $\mathbb{Z}_{\geq 0}$ of all nonnegative integers? The counterexample above shows that $(\mathbb{Z}_{\geq 0}, \diamond)$ is not a semigroup either. But in this case 0 is a neutral element for $(\mathbb{Z}_{\geq 0}, \diamond)$, because $n \diamond 0 = |n| = n$ for all $n \in \mathbb{Z}_{\geq 0}$. □

[2] id_A is called the **identity function** or just the **identity** on A.

Definition 3.2 (Groups and Abelian groups)**.**

Let $(G, \diamond)$ be a monoid with neutral element e which satisfies the following: For each $g \in G$ there exists some $g' \in G$ such that

$$g \diamond g' \;=\; g' \diamond g \;=\; e \quad \text{for all } g \in G. \tag{3.5}$$

We call such a g' an **inverse element**. of g, and we then call $(G, \diamond)$ a **group**.

Assume moreover that the operation $\diamond$ satisfies

$$\textbf{commutativity:} \quad g \diamond h \;= h \diamond g \quad \text{for all } g, h \in G. \tag{3.6}$$

Then G is called a **commutative group** or **abelian group**. We write G instead of $(G, \diamond)$ if it is clear which binary operation on G is represented by $\diamond$. □

Historical note: Abelian groups have been named after the Norwegian mathematician Niels Henrik Abel who lived in the first half of the 19th century and died at age 26.

Groups $(G, \diamond)$ are characterized as follows.

(a)	If $g, h \in G$ then $g \diamond h \in G$	**binary operation**
(b)	If $g, h, k \in G$ then $(g \diamond h) \diamond k \;=\; g \diamond (h \diamond k)$	**associativity**
(c)	There exists $e \in G$ such that $g \diamond e \;=\; e \diamond g \;=\; g$ for all $g \in G$	**neutral element**
(d)	For each $g \in G$ there exists $g' \in G$ such that $g \diamond g' \;=\; g' \diamond g \;=\; e$	**inverse element**

G is a **commutative group (abelian group)** if, in addition,

(e)	$g \diamond h \;=\; h \diamond g$ for all $g, h \in G$	**commutativity**

Theorem 3.2 (Uniqueness of the inverse in groups)**.**

Let $(G, \diamond)$ be a group and let $g \in G$. Assume that there exists besides g' another $g'' \in G$ which satisfies (3.5). Then $g'' = g'$.

PROOF: We have

$$g'' \overset{(3.2)}{=} e \diamond g'' \overset{(3.5)}{=} (g' \diamond g) \diamond g'' \overset{\text{assoc}}{=} g' \diamond (g \diamond g'') \overset{(3.5)}{=} g' \diamond e \overset{(3.2)}{=} g'$$

and this proves uniqueness.

Epilogue: We have taken care in this proof to give for every step a reference. ■

Definition 3.3 (inverse element g^{-1})**.**

It is customary to write g^{-1} for the unique element of G that is associated with the given $g \in G$ by means of (3.5). We call g^{-1} the inverse element of g rather than an inverse element of g. □

Example 3.4.

(a) $(\mathbb{R}_{\neq 0}, \cdot)$ (the nonzero real numbers with multiplication) is a commutative group: Multiplication is both associative and commutative, and the number 1 is the neutral element. Let $x \in \mathbb{R}$ not be zero. Then $x^{-1} = \frac{1}{x}$ satisfies $x \cdot x^{-1} = x^{-1} \cdot x = 1$, i.e., (3.5). The notation g^{-1} for the inverse of g comes from this example.

(b) $(\mathbb{Z}, +)$ (the integers with addition) is an abelian group: We have already seen that $(\mathbb{Z}, +)$ is a monoid.

The inverse element to $k \in \mathbb{Z}$ with respect to addition is $-k$ because $k + (-k) = (-k) + k = 0$ for all $k \in \mathbb{Z}$. Note that it would be very confusing to write k^{-1} rather than $-k$ for the inverse element under addition.

This group is abelian because $m + k = k + m$ for all $k, m \in \mathbb{Z}$.

(c) $(\mathbb{Z}_{\neq 0}, \cdot)$ (the nonzero integers with multiplication) is **not** a group: Let $k = 5$. Then $k \in \mathbb{Z}_{\neq 0}$. but $1/5$, the only number m such that $5 \cdot m = m \cdot 5 = 1$ is not an integer and hence does not belong to $\mathbb{Z}_{\neq 0}$. □

Proposition 3.2.

Let $(G, \diamond)$ be a group with neutral element e. Let $g, h \in G$. Then

$$\left(g^{-1}\right)^{-1} = g, \tag{3.7}$$

$$(h \diamond g)^{-1} = g^{-1} \diamond h^{-1}. \tag{3.8}$$

PROOF of (3.7): By definition of the inverse g^{-1}, we have

$$g \diamond g^{-1} = g^{-1} \diamond g = e.$$

These two equations not only show that g^{-1} is an inverse of g, but also that g is an inverse of g^{-1}. It follows from thm.3.2 that g is the unique inverse $\left(g^{-1}\right)^{-1}$ of g^{-1}. We have shown (3.7).

PROOF of (3.8): We have

$$\begin{aligned}(g^{-1} \diamond h^{-1}) \diamond (h \diamond g) &\overset{(3.1)}{=} g^{-1} \diamond \left(h^{-1} \diamond (h \diamond g)\right) \\ &\overset{(3.1)}{=} g^{-1} \diamond \left((h^{-1} \diamond h) \diamond g\right) \overset{(3.5)}{=} g^{-1} \diamond (e \diamond g) \overset{(3.2)}{=} g^{-1} \diamond g \overset{(3.5)}{=} e.\end{aligned}$$

We substitute h^{-1} for g and g^{-1} for h in the above chain of equations, and we obtain $\left((h^{-1})^{-1} \diamond (g^{-1})^{-1}\right) \diamond (g^{-1} \diamond h^{-1}) = e$. We apply (3.7) and it follows that $(h \diamond g) \diamond (g^{-1} \diamond h^{-1}) = e$. It follows that $g^{-1} \diamond h^{-1}$ is an inverse of $h \diamond g$. We have shown (3.8).

Note that it follows from prop.3.2 that $g^{-1} \diamond h^{-1}$ is the unique inverse $(h \diamond g)^{-1}$ of $h \diamond g$. ■

Proposition 3.3. ⋆

Let $(G, \diamond)$ be a group. Let $g, h \in G$. Then

$$h \diamond g^{-1} = (g \diamond h^{-1})^{-1}. \tag{3.9}$$

FIRST PROOF – doing it the hard way from scratch:

Proof strategy: Let e denote the neutral element G as usual. If we write $x := h \diamond g^{-1}$ and $y := g \diamond h^{-1}$ then our assertion is that $x = y^{-1}$. According to the definition of inverses we thus must prove that $x \diamond y = e$ and $y \diamond x = e$, i.e., we must prove that

$$(h \diamond g^{-1}) \diamond (g \diamond h^{-1}) = e \ (\star) \qquad \text{and} \qquad (g \diamond h^{-1}) \diamond (h \diamond g^{-1}) = e \ (\star\star).$$

PROOF of $(\star)$:

$$\begin{array}{lll} (h \diamond g^{-1}) \diamond (g \diamond h^{-1}) & = \big[(h \diamond g^{-1}) \diamond g\big] \diamond h^{-1} & \text{(associativity)} \\ & = \big[h \diamond (g^{-1} \diamond g)\big] \diamond h^{-1} & \text{(associativity)} \\ & = (h \diamond e) \diamond h^{-1} & \text{(def. inverse)} \\ & = h \diamond h^{-1} & \text{(def. neutral element)} \\ & = e & \text{(def. inverse)} \end{array}$$

The proof of $(\star\star)$ is left as exercise 3.5 (see p.93). ■

Proposition 3.4 (B/G prop.1.9 and B/G prop.8.10)**.**

Let $g, h, h' \in (G, \diamond)$. If $g \diamond h = g \diamond h'$ then $h = h'$.

PROOF: It follows that the assumption that $g^{-1} \diamond (g \diamond h) = g^{-1} \diamond (g \diamond h')$.

Thus, by associativity, $(g^{-1} \diamond g) \diamond h = (g^{-1} \diamond g) \diamond h'$.

It follows from (3.5) in the definition of the group inverse that $g^{-1} \diamond g = e$, thus $e \diamond h = e \diamond h'$.

Since the neutral element acts as a "no–op" we finally obtain $h = h'$. ■

Example 3.5. Let $S := \{f : f \text{ is a function } \mathbb{R} \to \mathbb{R}\}$ with the operation $(f, g) \mapsto g \circ f$ defined as $g \circ f(x) = g(f(x))$. We have seen in prop.3.1 that $(S, \circ)$ is a monoid. We now show that $(S, \circ)$ is not a group.

Proof strategy: According to Definition 3.2, S is a group if and only if each function $f : \mathbb{R} \to \mathbb{R}$ possesses an inverse element $f^{-1} : \mathbb{R} \to \mathbb{R}$ which satisfies (3.5). Because the neutral element of S is the function $id_{\mathbb{R}} : x \mapsto x$, this inverse f^{-1} must satisfy

$$f \circ f^{-1} = f^{-1} \circ f = id_{\mathbb{R}}, \quad \text{i.e.,} \quad f\big(f^{-1}(x)\big) = f^{-1}\big(f(x)\big) = x \text{ for all } x \in \mathbb{R}.$$

Accordingly, to prove that S is not a group, it suffices to produce just one counterexample $f \in S$ for which an inverse f^{-1} does not exist.

Some functions will have an inverse. For example $f(x) = x - 7$ has inverse $f^{-1}(x) = x + 7$.

Recall from calculus that if f has an inverse then f must pass the "horizontal line test": Any parallel to the x–axis may intersect the graph of f (see Definition **??** (preliminary definition of a function) on p.**??**) in at most one point. [3] We We must find a function which does not have an inverse. Here are three.

$f(x) = x^2$: The horizontal line $y = 4$ intersects the graph of f in $(-2, 4)$ and also in $(2, 4)$.
$f(x) = 21$: The horizontal line $y = 21$ intersects the graph of f in $(x, 21)$ for each $x \in \mathbb{R}$.
$f(x) = \sin(x)$: The horizontal line $y = 0$ intersects the graph of f in $(n\pi, 0)$ for each $n \in \mathbb{Z}$. □

Proposition 3.5.

Let G be the set of all polynomials of degree 1. In other words,

$$G \;=\; \{f : \mathbb{R} \to \mathbb{R} : f(x) = ax + b \text{ for some } a, b \in \mathbb{R} \text{ where } a \neq 0\}$$

This is the set of functions whose graph is a straight line in the x, y–plane, which is parallel neither to the x–axis, nor to the y–axis. As in example 3.5, let $(f, g) \mapsto g \circ f$ be defined as $g \circ f(x) = g(f(x))$. Then $(G, \circ)$ is a group.

PROOF:

First, we prove that $\circ$ is a binary operation on G, i.e., if $f, g \in G$ then $g \circ f \in G$ (see the beginning of Definition 3.1 (semigroups and monoids) on p.53). In other words, we will show that the composition of two straight line functions is a straight line function.

So let $f(x) := a_1x + b_1$ and $g(x) := a_2x + b_2$ for suitable $a_1, b_1, a_2, b_2 \in \mathbb{R}$ where moreover $a_1, a_2 \neq 0$. Let $x \in \mathbb{R}$. Then

$$g \circ f(x) \;= g(a_1x + b_1) \;=\; a_2(a_1x + b_1) + b_2 \;=\; (a_1a_2)x + (a_2b_1 + b_2).$$

Hence $g \circ f$ is of the form $x \mapsto ax + b$ with $a = a_1a_2 \in \mathbb{R}_{\neq 0}$ and $b = a_2b_1 + b_2 \in \mathbb{R}$. We have proved that $\circ$ is a binary operation on G.

It follows from from prop.3.1 that $(G, \circ)$ is a monoid. We only have to note that $id_{\mathbb{R}} \in G$ because, if $a = 1$ and $b = 0$, then $id_{\mathbb{R}}(x) = x = ax + b$.

To prove that this monoid is a group, we must prove thefollowing. If $f \in G$, then there exists $g \in G$ such that $g(f(x)) = f(g(x)) = x$, for all $x \in \mathbb{R}$.

We have learned in calculus that, if $y = f(x)$, we must "solve for x" to obtain the inverse function. Let $f(x) = ax + b$ $(a \neq 0)$. Then

$$y \;=\; ax + b \;\Rightarrow ax \;=\; y - b \;\Rightarrow\; x \;=\; \tfrac{1}{a}y + \tfrac{-b}{a}.$$

Let $g(x) := \frac{1}{a}x - \frac{b}{a}$. Then $g \in G$. To prove that $g = f^{-1}$, we must show that

$$g\big(f(x)\big) \;= g\big(f(x)\big) \;=\; x \text{ for all } x \in \mathbb{R}.$$

[3] Actually, our definition of inverse function demands that any parallel to the x–axis must intersect the graph of f in exactly one point. (see rem. **??** (horizontal and vertical line tests) on p.**??**).

We have

$$g\big(f(x)\big) \;=\; g(ax+b) \;=\; \tfrac{1}{a}(ax+b)-\tfrac{b}{a} \;=\; (x+\tfrac{b}{a})-\tfrac{b}{a} \;=\; x;$$
$$f\big(g(x)\big) \;=\; f(\tfrac{1}{a}x+\tfrac{-b}{a}) \;=\; a(\tfrac{1}{a}x-\tfrac{b}{a})+b \;=\; (x-b)+b \;=\; x.$$

Hence $g=f^{-1}$. We have shown that every element f of the monoid $(G,\circ)$ possesses an inverse and it follows that $(G,\circ)$ is a group. ■

The next definition is familiar to you if you have taken a linear algebra course.

Definition 3.4 (Linear functions on $\mathbb{R}$)**.**

⋆

A function $f:\mathbb{R}\to\mathbb{R}$ is a **linear function on** $\mathbb{R}$ if the following is true for all $x,y,\lambda\in\mathbb{R}$:

(3.10) $f(x+y) = f(x)+f(y)$ **(additivity)**,

(3.11) $f(\lambda x) = \lambda f(x)$ **(homogeneity)**. □

The symbol λ (prounced lambda) that occurs in the definition above is the greek version of the letter l. Note that Chapter **??** (Greek Letters) on p.**??** contains a list of the most commonly used Greek letters.

You will learn later about the general definition of a linear function. See Definition **??** (linear mappings) on p.**??**.

Theorem 3.3.

Let $f:\mathbb{R}\to\mathbb{R}$. Then f is linear if and only if there exists $a\in\mathbb{R}$ such that $f(x)=ax$ for all $x\in\mathbb{R}$.

PROOF:

Proof strategy: The proof of a statement of the form "P is true if and only if Q is true" consists of two parts. We must prove that **a)** if P is true then Q is true and also **b)** if Q is true then P is true. In the context of this theorem we have

P: f is linear,

Q: there exists $a\in\mathbb{R}$ such that $f(x)=ax$ for all $x\in\mathbb{R}$.

a) Proof that if f is linear then there exists $a\in\mathbb{R}$ such that $f(x)=ax$ for all $x\in\mathbb{R}$:

(3.12) $$f(1) \;=\; f\Big(\frac{y-x}{y-x}\Big) \overset{(3.11)}{=} \frac{f(y-x)}{y-x} \overset{(3.10)}{=} \frac{f(y)-f(x)}{y-x} \quad \text{for all } y\neq x.$$

It follows that f represents a straight line in the plane with slope $m=f(1)$.

Next we observe that $f(0) \;=\; f(2\cdot 0) \overset{(3.11)}{=} 2f(0)$, hence $f(0)=0$.

We substitute $y = 0$ in (3.12) and obtain $f(1) = \frac{-f(x)}{-x}$. It follows with $a := f(1)$ that indeed $f(x) = a \cdot x$ for some $a \in \mathbb{R}$.

b) Proof that if there exists $a \in \mathbb{R}$ such that $f(x) = ax$ for all $x \in \mathbb{R}$ then f is linear:

We show the validity of 3.10 and 3.11 by brute force. Let $x, y, \lambda \in \mathbb{R}$. Then

$$\begin{aligned} f(x+y) &= a(x+y) = ax + ay = f(x) + f(y), \\ f(\lambda x) &= a(\lambda x) = \lambda(ax) = \lambda f(x). \end{aligned}$$

This proves both additivity and homogeneity and hence the linearity of f. ■

Let $(G, \diamond)$ be a group and $H \subseteq G$. Note that if $h, h' \in H$ then $h, h' \in G$ and hence $h \diamond h'$ exists as an element of G, but there is no guarantee that $h \diamond h' \in H$. For example, let $(G, \diamond)$ be the group $(\mathbb{R}, +)$ of all real numbers with addition as its binary operation, and let $H := [-1, 1] = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$. Then $\frac{1}{2}$ and $\frac{3}{4}$ belong to H, but $\frac{1}{2} + \frac{3}{4} \notin H$. Subsets H of G which are "closed" with respect to $\diamond$, i.e., $h \diamond h' \in H$ whenever $h, h' \in H$, deserve a special name.

Definition 3.5 (Subgroup)**.**

★ Let $(G, \diamond)$ be a group and $H \subseteq G$.

We call $(H, \diamond)$ a **subgroup** of G if the following is true:

(3.13) H is not empty,

(3.14) if $h, h' \in H$ then $h \diamond h' \in H$,

(3.15) if $h \in H$ then its inverse element h^{-1} (in G!) belongs to H.

We also write H for $(H, \diamond)$, if there is no confusion about the nature of "$\diamond$". □

Proposition 3.6.

Subgroups are groups.

PROOF:

Let $(G, \diamond)$ be a group and let H be a subgroup of G. We must prove that $(H, \diamond)$ is a monoid (H is not empty, $\diamond$ is a binary operation on the subset H of G, H has a neutral element e_H, and H satisfies associativity) and that each $h \in H$ possesses $h' \in H$ such that $h \diamond h' = h' \diamond h = e_H$

(a) H is nonempty: This follows from (3.13).

(b) $\diamond$ is a binary operation on H: We must show that if $h, h' \in H$ then $h \diamond h' \in H$ (not just that $h \diamond h' \in G$). But this follows from (3.14).

(c) Existence of a neutral element: Let e be the neutral element of G. H is not empty, hence there exists $h_0 \in H$. h_0 has an inverse h_0^{-1} in the group G which belongs, according to (3.15), to H. It follows from (3.14) that $e = h_0 \diamond h_0^{-1} \in H$.

$g \diamond e = e \diamond g = e$ holds for any $g \in G$ and hence, in particular, for each $g \in H$. This proves that e is a neutral element of H.

(d) We next prove associativity. Let $h_1, h_2, h_3 \in H$. We apply (3.14) four times to obtain

$$h_1 \diamond h_2 \in H,\ (h_1 \diamond h_2) \diamond h_3 \in H,\ h_2 \diamond h_3 \in H,\ \ h_1 \diamond (h_2 \diamond h_3) \in H.$$

It further follows from the associativity of $\diamond$ in G that $(h_1 \diamond h_2) \diamond h_3 \ = \ h_1 \diamond (h_2 \diamond h_3)$. We thus have proven associativity of $\diamond$ in H.

(e) We finally prove that if $h \in H$ then its inverse in G, h^{-1}, is also the inverse of h in H. That follows from the fact that, by (3.15), $h^{-1} \in H$, the neutral element e of G is also the neutral element of H, and

$$h \diamond h^{-1} \ = \ h^{-1} \diamond h \ = \ e. \ \blacksquare$$

Example 3.6.

- **(a)** $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, because the sum of two integers is an integer and the additive inverse of an integer is an integer.
- **(b)** $(\mathbb{Q}_{\neq 0}, \cdot)$ is a subgroup of $(\mathbb{R}_{\neq 0}, \cdot)$, because the product of two nonzero fractions is a nonzero fraction and the multiplicative inverse of two nonzero fractions is a nonzero fraction.
- **(c)** Let $H := \{x \in \mathbb{R} : 0 < |x| < 1\}$. Then $(H, \cdot)$ is **not** a subgroup of $(\mathbb{R}_{\neq 0}, \cdot)$ (since $1 \notin H$, but also since $0.5^{-1} = -2 \notin H$).
- **(d)** Then $(\mathbb{Z}_{\neq 0}, \cdot)$ is not a subgroup of $(\mathbb{R}_{\neq 0}, \cdot)$ because $\frac{1}{2}$, the multiplicative inverse of $2 \in \mathbb{Z}$, is not an integer.
- **(e)** Let $H := [1, 2]$. Then $(H, \cdot)$ is not a subgroup of $(\mathbb{R}_{\neq 0}, \cdot)$, and $(H, +)$ is not a subgroup of $(\mathbb{R}, +)$.

Proposition 3.7.

Let $(G, \circ)$ be the set of all polynomials of degree 1 with function composition, i.e.,

$$G \ = \ \{\, \mathbb{R} \xrightarrow{f} \mathbb{R} : \ f(x) = ax + b, \text{ for some } a, b \in \mathbb{R} \text{ such that } a \neq 0 \},$$

$$g \circ f : \ x \mapsto g \circ f(x) \ = \ g(f(x)).$$

Further, let

$$H \ := \ \{\, \mathbb{R} \xrightarrow{f} \mathbb{R} : \ f(x) = ax, \text{ for some nonzero } a \in \mathbb{R} \}.$$

Then $(H, \circ)$ is a subgroup of $(G, \circ)$.

PROOF:

It was established in prop.3.5 that $(G, \circ)$ is a group. H is a subset of G because elements of H are those functions $x \mapsto ax + b$ of G for which $b = 0$. To prove that H is a subgroup of G we must show that if $h, h' \in H$ then $h \circ h' \in H$ and that the inverse function h^{-1} in G actually belongs to H.

So let $h(x) := ax$ and $h'(x) := a'x$ ($a, a' \in \mathbb{R}$ and $a, a' \neq 0$). Then

$$h \circ h'(x) \;=\; a(a'x) \;=\; (aa')x$$

shows, because $aa' \neq 0$, that $h \circ h' \in H$. Further, the inverse of h in G is the function $h^{-1} : x \mapsto \frac{1}{a}x$. But $h' \in H$ because $\frac{1}{a} \neq 0$. We have proven that H is a subgroup of G. ■

Note that the above proposition also follows from thm.3.3 on p.60.

Proposition 3.8.

The intersection of an arbitrary collection of subgroups is a subgroup.

PROOF:

The proof is given only for the special case of two subgroups, but the general case is shown according to the same principle.

Let $(G, \diamond)$ be a group and let H_1, H_2 be two subgroups of G. Let $H := H_1 \cap H_2$ and $h, h' \in H$. We must prove (3.14) and (3.15). We conclude from $h, h' \in H \subseteq H_1$ that $h \diamond h' \in H_1$ and $h^{-1} \in H_1$ because H_1 is a subgroup. We further conclude from $h, h' \in H \subseteq H_2$ that $h \diamond h' \in H_2$ and $h^{-1} \in H_2$ because H_2 also is a subgroup. It follows from the definition of an intersection that $h \diamond h' \in H_1 \cap H_2$ and $h^{-1} \in H_1 \cap H_2$. This concludes the proof. ■

We now turn our attention to functions which map from a group to another group in such a way that they are, in a sense, compatible with the binary operations on their domain and codomain.

Example 3.7.

Let $(G, \diamond) := (\mathbb{R}, +)$ and $(H, \bullet) := (\,]0, \infty[, \cdot)$. Then both G and H are abelian groups (H is an abelian subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$ since the product of two strictly positive numbers is again strictly positive and because the neutral element 1 is strictly positive). Let

$$\varphi : (G, \diamond) \to (H, \bullet)\,; \quad x \mapsto e^x\,, \qquad \psi : (H, \bullet) \to (G, \diamond)\,; \quad y \mapsto \ln(y)\,.$$

Note that the following is true for φ:

- $\varphi(x + y) \;=\; \varphi(x) \cdot \varphi(y)$ for all $x, y \in G$,
- $\varphi(0) \;=\; 1$: the image of the neutral element is the neutral element.
- $\varphi(-x) \;=\; e^{-x} \;=\; \frac{1}{\varphi(x)}$: the image of the inverse is the inverse of the image.

It does not matter whether you first apply the operation to two items in the domain and then apply the function to the result or whether you first map those two items into the codomain and then apply the operation to the two function values. Further, the inverse of the function value is the function value of the inverse and the function maps the neutral element to the neutral element.

Mathematicians say that a function function φ that has groups both as its domain and it codomain is **structure compatible** with the algebraic (group) operations on its domain and codomain.

The function $\psi(y) = \ln(y)$ also is structure compatible:

- $\psi(x \cdot y) = \psi(x) + \psi(y)$ for all $x, y \in H$,
- $\psi(1) = 0$: the image of the neutral element is the neutral element.
- $\psi\left(\frac{1}{y}\right) = \ln\left(\frac{1}{y}\right) = -\ln(y) = -\psi(y)$: the function value of the inverse is the inverse of the function value.

Note that those two structure compatible functions φ and ψ are inverses of each other. □

We can generalize the above example as follows.

Definition 3.6 (Homomorphisms and isomorphisms)**.**

Let $(G, \diamond)$ and $(H, \bullet)$ be groups with neutral elements e_G and e_H and let us write g^{-1} and h^{-1} for the inverses (in the sense of def. 3.3 on p.56.

Let $\varphi : (G, \diamond) \to (H, \bullet)$ be a function which satisfies the following:

$$\varphi(g_1 \diamond g_2) = \varphi(g_1) \bullet \varphi(g_2)\,. \tag{3.16}$$

Then we call φ a **homomorphism**, more specifically, a **group homomorphism**, from the group $(G, \diamond)$ to the group $(H, \bullet)$.

Let $\psi : (H, \bullet) \to (G, \diamond)$ be a group homomorphism from $(H, \bullet)$ to $(G, \diamond)$ such that φ and ψ are inverse to each other. We call such a bijective homomorphism an **isomorphism**, and we call the groups $(G, \diamond)$ and $(H, \bullet)$ **isomorphic**.

For bijectivity, see Definition **??** on p.**??**). □

Theorem 3.4.

Let $(G, \diamond)$ and $(H, \bullet)$ be two groups and let $\varphi : (G, \diamond) \to (H, \bullet)$ be a homomorphism.
Let e_G be the neutral element of G and e_H be the neutral element of H. Then

- ***(a)*** *$\varphi(e_G) = e_H$,*
- ***(b)*** *Let $g \in G$. Then $\varphi(g^{-1}) = \big(\varphi(g)\big)^{-1}$,*
- ***(c)*** *Direct images of subgroups of G are subgroups of H.*
- ***(d)*** *Preimages of subgroups of G are subgroups of H.*

PROOF of **(a)**: It follows from $\varphi(e_G) = \varphi(e_G \diamond e_g) = \varphi(e_G) \bullet \varphi(e_G)$ and associativity that

$$\begin{aligned} e_H &= \big(\varphi(e_G)\big)^{-1} \bullet \varphi(e_G) = \big(\varphi(e_G)\big)^{-1} \bullet \varphi(e_G \diamond e_G) \\ &= \big(\varphi(e_G)\big)^{-1} \bullet \big[\varphi(e_G) \bullet \varphi(e_G)\big] = \big[\big(\varphi(e_G)\big)^{-1} \bullet \varphi(e_G)\big] \bullet \varphi(e_G) \\ &= e_H \bullet \varphi(e_G) = \varphi(e_G)\,. \end{aligned}$$

PROOF of **(b)**: We apply part **(a)** and (3.16) and obtain

$$e_H = \varphi(e_G) = \varphi(g^{-1} \diamond g)\,. = \varphi(g^{-1}) \bullet \varphi(g)$$

This proves that $\varphi(g^{-1})$ is the inverse of $\varphi(g)$.

The proof of **(c)** and **(d)** is left as an exercise. ■

The next result which is not hard to prove might surprise you. If a group homomorphism possesses an inverse then this inverse is also a group homomorphism

Theorem 3.5.

★ *Let $(G, \diamond)$ and $(H, \bullet)$ be two groups and let $\varphi : (G, \diamond) \to (H, \bullet)$ be a homomorphism which possesses an inverse.*
Then $\varphi^{-1} : H \to G$ also is a homomorphism and thus φ is an isomorphism

PROOF:
We recall that the inverse φ^{-1} of φ satisfies $\varphi \circ \varphi^{-1} = id_H$ and $\varphi^{-1} \circ \varphi = id_G$, i.e.,
$\varphi\big(\varphi^{-1}(h)\big) = h$ for all $h \in H$ and $\varphi^{-1}\big(\varphi(g)\big) = g$ for all $g \in G$.

So let $h, h' \in H$. Since φ is surjective, there exist $g, g' \in G$ such that $\varphi(g) = h$ and $\varphi(g') = h'$. Then,

$$\begin{aligned}
\varphi^{-1}(h \bullet h') &= \varphi^{-1}(\varphi(g) \bullet \varphi(g')) \;=\; \varphi^{-1}(\varphi(g \diamond g')) && \text{(since } \varphi \text{ is a homomorphism)} \\
&= g \diamond g' \;=\; \varphi^{-1}\big(\varphi(g)\big) \diamond \varphi^{-1}\big(\varphi(g')\big) && \text{(since } \varphi^{-1} \circ \varphi = id_G\text{)} \\
&= \varphi^{-1}(h) \diamond \varphi^{-1}(h'). && \text{(definition of } h \text{ and } h'\text{)} \quad ■
\end{aligned}$$

3.2 Commutative Rings and Integral Domains

Introduction 3.3.
The definition of a ring is of great importance in algebra. It will not be given in this document because it is too general for our purposes. We rather restrict ourselves from the outset to so called commutative rings with unit and to integral domains. These definitions not only cover the number systems we all are familiar with, the integers, fractions and real numbers, [4] but also, e.g., the set of all polynomials when considered as functions $p(x)$ of a real variable x. □

Definition 3.7 (Commutative rings with unit)**.**

★ Let R be a nonempty set with two binary operations

$$\oplus : (a, b) \mapsto a \oplus b, \text{ called } \textbf{addition}, \quad \text{and} \quad \odot : (a, b) \mapsto a \odot b, \text{ called } \textbf{multiplication},$$

which assign to any two elements $a, b \in R$ uniquely determined $a \oplus b \in R$ and $a \odot b \in R$ such that the following holds:

[4] See Proposition 3.12 on p.70

(a) $(R, \oplus)$ is an abelian (i.e., commutative) group; we denote the neutral element for addition by 0 and the inverse element of $a \in R$ for addition by $\ominus a$.
(b) $(R, \odot)$ is a commutative monoid, i.e., a monoid for which $a \odot b = b \odot a$ for all $a, b \in R$. We denote the neutral element with respect to multiplication by 1.
(c) Multiplication is **distributive** over addition:

$$a \odot (b \oplus c) \;=\; (a \odot b) \oplus (a \odot c) \quad \text{for all } a, b, c \in R. \tag{3.17}$$

(d) $1 \neq 0$.

The triplet $(R, \oplus, \odot)$ is called a **commutative ring with unit**. We may write R instead of $(R, \oplus, \odot)$ if it is clear which binary operations on R are represented by $\oplus$ and by $\odot$. □

Remark 3.1.

Recall from thm.3.1 and thm.3.2 that the neutral elements 0 and 1 and the additive inverse $\ominus b$ are uniquely determined ($b \in R$). □

Notation 3.1 (Notation Alert for Commutative Rings With Unit)**.**

(a) It is customary to write ab instead of $a \odot b$ if this does not give rise to confusion.
(b) Multiplication has precedence over (binds stronger than) addition: $a \odot b \oplus c$ means $(a \odot b) \oplus c$, not $a \odot (b \oplus c)$.
(c) Let $a, b, \in R$. Recall from thm.3.1 and thm.3.2 that not only the neutral elements 0 and 1 but also the additive inverse $\ominus b$ are uniquely determined. Accordingly, we can define another binary operation, $\ominus$, on $(R, \oplus, \odot)$ as follows:

$$a \;\ominus\; b \;:=\; a \;\oplus\; (\ominus b). \tag{3.18}$$

We call $a \ominus b$ the **difference** of a and b. □

For a set of numbers A we defined in Definition **??** on p.**??** the set $\lambda A + b = \{\lambda a + b : a \in A\}$. This generalizes without difficulty to commutative rings with unit.

Definition 3.8 (Translation and dilation of sets)**.**

⋆

Let $R = (R, \oplus, \odot)$ be a commutative ring with unit and $A \subseteq R$. and $\alpha, b \in R$. We define

$$\lambda A \oplus b \;:= \{\lambda a \oplus b : a \in A\}. \tag{3.19}$$

In particular, for $\lambda = \pm 1$, we obtain

$$A \oplus b = \{a \oplus b : a \in A\}, \tag{3.20}$$

$$\ominus A = \{\ominus a : a \in A\}. \ \square \tag{3.21}$$

Remark 3.2.

Note that the above makes sense for any **algebraic structure**, i.e., a set with one or more "algebraic operations", if they have the binary operations "$\oplus$" and/or "$\odot$" of a commutative ring with unit. [5] $\square$

Next, we examine the role of the condition $1 \neq 0$. It turns out that it is equivalent to demanding that R is not the trivial "Null ring" $\{0\}$.

Proposition 3.9.

*Let $(R, \oplus, \odot)$ be a nonempty set with two binary operations $\oplus$ and $\odot$ which satisfies **(a)**, **(b)**, **(c)** of Definition 3.7, i.e., R satisfies all conditions for a commutative ring with unit except that 1 and 0 need not be different elements of R. Then*

- ***(a)*** *$a \ominus a = 0$ for all $a \in R$,*
- ***(b)*** *$a \odot 0 = 0$ for all $a \in R$.*

PROOF of **(a)**: This follows from the definitions of inverse and subtraction: $a \ominus a = a \oplus (\ominus a) = 0$.

PROOF of **(b)**:

$$a \odot 0 \overset{3.2}{=} a(0 \oplus 0) \overset{3.17}{=} a \odot 0 \oplus a \odot 0, \text{ hence} \tag{3.22}$$

$$\begin{aligned} 0 &\overset{3.5}{=} a \odot 0 \ \oplus \big(\ominus (a \odot 0) \big) \overset{3.22}{=} (a \odot 0 \oplus a \odot 0) \ \oplus \big(\ominus (a \odot 0) \big) \\ &\overset{3.1}{=} a \odot 0 \ \oplus \ \big(a \odot 0 \ \oplus (\ominus (a \odot 0)) \big) \overset{3.5}{=} a \odot 0 \oplus 0 \overset{3.2}{=} a \odot 0. \end{aligned} \tag{3.23}$$

The second chain of equations above proves that $a \odot 0 = 0$. ■

Proposition 3.10.

- ***(a)*** *The set $R := \{0\}$ satisfies conditions **(a)**, **(b)**, **(c)** of Definition 3.7,*
- ***(b)*** *Let $(R, \oplus, \odot)$ be a nonempty set with two binary operations $\oplus$ and $\odot$ which satisfies **(a)**, **(b)**, **(c)** of Definition 3.7. Then the following is true: $1 = 0$ if and only if $R = \{0\}$.*

[5] Ignore this if you are not familiar with vector spaces: In a vector space V the scalar product $(\lambda, a) \mapsto \lambda v$ of a real number (scalar) λ and a vector $v \in V$ (not a binary operation since its domain is $\mathbb{R} \times V$ rather than $V \times V$) would take the place of "$\odot$"

PROOF:

Proof of (a):

Note that because 0 is the only element of R, the operations $\oplus$ and $\odot$ are completely determined by the following:

$$0 \oplus 0 = 0; \qquad 0 \odot 0 = 0.$$

We only prove here that $(R, \oplus)$ is a monoid. The proofs of the other properties are just as simple.

Let $a, b, c \in R$. Then $a = b = c = 0$ because R does not contain any other elements. We obtain

$$(a \oplus b) \oplus c = (0 \oplus 0) \oplus 0 = 0 \oplus 0 = 0 \oplus (0 \oplus 0) = a \oplus (b \oplus c),$$

hence $\oplus$ is associative and $(R, \oplus)$ is a semigroup.

Let $a \in R$. Then $a = 0$ because R does not contain any other elements. We obtain

$$a \oplus 0 = 0 \oplus 0 = 0 \oplus a,$$

hence 0 is neutral element for $\oplus$ and the semigroup $(R, \oplus)$ is a monoid.

Proof of (b):

■

Definition 3.9 (Zero Divisors and Cancellation Rule)**.**

Let $(R, \oplus, \odot)$ be a commutative ring with unit.

(a) If $a, b \in R$ such that $a \neq 0$ and $b \neq 0$ and $a \odot b = 0$ then we call a and b **zero divisors**.

(b) We say that the **cancellation rule** holds in R if the following is true for all $a, b, c \in R$ such that $a \neq 0$:

(3.24) If $a \odot b = a \odot c$ then $b = c$. □

For an example of a commutative ring with unit which contains zero divisors see ch.**??** (The Integers Modulo n) on p.**??**.

Definition 3.10 (Integral domains)**.**

Let $(R, \oplus, \odot)$ be a commutative ring with unit which satisfies the

- **no zero divisors condition**: If $a, b \in R$ such that $a \odot b = 0$ then $a = 0$ or $b = 0$ (or both are zero).

The triplet $(R, \oplus, \odot)$ is called an **integral domain**. □

Remark 3.3.

We stated the no zero divisors condition in the definition of an integral domain as follows: If $a, b \in R$ such that $a \odot b = 0$ then $a = 0$ or $b = 0$ (or both are zero). We remind you that there was no need to include the "or both are zero" part since "or" is always the inclusive "or". See the **??** section (OR vs. EITHER ... OR) on p.**??**. □

Remark 3.4.

Integral domains $(R, \oplus, \odot)$ are characterized as follows.

(a)	If $a, b \in R$ then $a \oplus b \in R$ and $a \odot b \in R$	**binary operations**
(b)	If $a, b, c \in R$ then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$	**associativity of $\oplus$**
(c)	If $a, b, c \in R$ then $(a \odot b) \odot c = a \odot (b \odot c)$	**associativity of $\odot$**
(d)	If $a, b \in R$ then $a \oplus b = b \oplus a$	**commutativity of $\oplus$**
(e)	If $a, b \in R$ then $a \odot b = b \odot a$	**commutativity of $\odot$**
(f)	If $a, b, c \in R$ then $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$	**distributivity**
(g)	There exists $0 \in R$ such that $a \oplus 0 = a$ for all $a \in R$	**neutral element f. $\oplus$**
(h)	There exists $1 \in R$ such that $1 \neq 0$ and $a \odot 1 = a$ for all $a \in R$	**neutral element f. $\odot$**
(i)	For each $a \in R$ there exists $a' \in R$ such that $a \oplus a' = 0$	**inverse element f. $\oplus$**
(j)	If $a, b \in R$ such that $a \neq 0$ and $b \neq 0$ then $a \odot b \neq 0$	**no zero divisors**

Proposition 3.11.

Let $(R, \oplus, \odot)$ be a commutative ring with unit. Then R satisfies the No zero divisors condition if and only if the cancellation rule holds in R.

PROOF that the cancellation rule implies the absence of zero divisors:

We assume that the cancellation rule holds in R. Let $a, b \in R$ such that $ab = 0$ and $a \neq 0$. It suffices to show that then $b = 0$. (Why?)

It follows from $ab = 0$ and $b = b \ominus 0$ that $a(b \ominus 0) = 0$, hence $a \odot b = a \odot 0$. The cancellation rule now implies together with $a \neq 0$ that $b = 0$.

PROOF that the absence of zero divisors implies the cancellation rule:

We assume that R has no zero divisors. Let $a, b, c \in R$ such that $ab = ac$ and $a \neq 0$. It suffices to show that $b = c$.

It follows from the distributivity law (3.17) that $0 = ab \ominus ac = a(b \ominus c)$. Because R has no zero divisors, at least one of a or $b \ominus c$ must be zero.

We assumed that $a \neq 0$ and it follows that $b \ominus c = 0$, i.e., $b = c$. ■

Corollary 3.1.

A commutative ring with unit is an integral domain $\Leftrightarrow$ *the cancellation rule holds.*

PROOF: Immediate from prop.3.11. ■

Proposition 3.12.

Each of the following algebraic structures is an integral domain:

- ***(a)*** $(\mathbb{Z}, +, \cdot)$*: the integers with addition and multiplication,*
- ***(b)*** $(\mathbb{Q}, +, \cdot)$*: the rational numbers with addition and multiplication,*
- ***(c)*** $(\mathbb{R}, +, \cdot)$*: the real numbers with addition and multiplication.*
- ***(d)*** [6] $(\mathbb{C}, +, \cdot)$*: the complex numbers with addition and multiplication.*

PROOF Will not be given here. ■

3.3 Arithmetic in Integral Domains

Notation: In this entire chapter we assume that a fixed integral domain $(R, \oplus, \odot)$ is given and phrases such as "let $x \in R$" refer to that integral domain.

Note also that we will, in accordance with notation 3.1**(a)**, often write $a\ b$ instead of $a \odot b$.

Introduction 3.4.

When you look at ch.1.2–1.3 and then again at ch.8.1 of [1] Beck/Geoghegan: The Art of Proof then you notice that identical propositions and theorems are given there: First for integers in ch.1, and then again for real numbers in ch.8. You will not find a third set for the rational numbers, but only because the authors chose instead to define those as a subset of $\mathbb{R}$ instead and, in that manner, inherit their laws of arithmetic from those for the real numbers.

It was mentioned in prop.3.12 on p.70, and it will be proven in ch.**??** (The Integers) and ch.**??** (The Real Numbers) that not only the integers but also the rational numbers and the real numbers with the binary operations of addition and multiplication are integral domains.

This is the power of mathematical abstraction:

A formula such as, e.g., $(-x)(-y) = xy$ need not be demonstrated separately for $\mathbb{Z}$, for $\mathbb{Q}$, and then again for $\mathbb{R}$. Rather it should be possible to state and prove it once for integral domains and thus have it validated for all three sets of numbers.

This is the route we are going here. The propositions and theorems in this chapter are almost an exact copy of ch.1.2–1.3, and then again of ch.8.1, of [1] Beck/Geoghegan: The Art of Proof, but we use "$\oplus$" instead of "$+$", "$\ominus$" instead of "$-$" and "$\odot$" instead of "$\cdot$" for the binary operations

of addition, subtraction and multiplication. This is deliberate. The reader then should more easily remember that these rules also apply to other integral domains such as, e.g., the complex numbers and the so called integers modulo n. (See Definition **??** on p.**??**.) □

We just mentioned that a lot of the following material can, in a sense, also be found in ch.1.2–1.3 and ch.8.1, of [1] Beck/Geoghegan: The Art of Proof. The difference is that those authors represent the material first for the integers (ch.1) and then again for the real numbers (ch.8). In contrast we state the material only once, in the framework of integral domains.

Some of the propositions that only deal with one of the operations $\oplus$ and $\odot$ are immediate consequences of the material of Chapter 3.1 (Semigroups and Groups). We include them here to make it easier to read the Beck/Geoghegan text in parallel.

Where applicable we provide the Beck/Geoghegan references for matching definitions, propositions and theorems. Note that we refer to some of the proofs to that book. On the other hand, if a proof is not given in the B/G book then you will generally also not find it in this document. An exception is the first proposition here, prop.3.13, where we supply the proof to help the readers make the transition between the set $(\mathbb{Z}, +, \cdot)$ and the set $(R, \oplus, \odot)$.

Proposition 3.13 (B/G prop.1.6 and B/G prop.8.8)**.**

Let $a, b, c \in R$. Then $(a \oplus b) \odot c \;=\; a \odot c \oplus b \odot c$.

PROOF:

$$(a \oplus b) \odot c \overset{\text{def.3.7.}b}{=} c \odot (a \oplus b) \overset{(3.17)}{=} c \odot a \oplus c \odot b \overset{\text{def.3.7.}b}{=} a \odot c \oplus b \odot c. \quad \blacksquare$$

Proposition 3.14 (B/G prop.1.7 and B/G prop.8.9)**.**

Let $a \in R$. Then $0 \oplus a = a$ and $1 \odot a = a$.

PROOF: It follows from Definition 3.7 on p.65 of a commutative ring with unit that $(R, \oplus)$ is a monoid with neutral element 0 and $(R, \odot)$ is a monoid with neutral element 1. The assertion follows from the definition of a monoid. ■

Proposition 3.15 (B/G prop.1.8)**.**

Let $a \in R$. Then $(\ominus a) \oplus a = 0$.

PROOF: It follows from the definition of inverse elements in groups, even if they are not assumed to be abelian, that $(\ominus a) \oplus a = 0$. See (3.5) on p.56. ■

Proposition 3.16 (B/G prop.1.10 and B/G prop.8.11)**.**

Let $a, b_1, b_2 \in R$. If $a \oplus b_1 = 0$ and $a \oplus b_2 = 0$ then $b_1 = b_2$.

PROOF: Left as an exercise. ■

Note for the following proposition that parts **(b)** and **(c)** hold true for semigroups (not even commutativity of $\oplus$ is needed) and that part **(d)** holds true for commutative monoids.

Proposition 3.17 (B/G prop.1.11 and B/G prop.8.12)**.**

Let $a, b, c, d \in R$. Then

(a) $(a \oplus b)\ (c \oplus d) \ = \ (ac \oplus bc) \oplus (ad \oplus bd)$,
(b) $a \oplus \big(b \oplus (c \oplus d)\big) \ = \ (a \oplus b) \oplus (c \oplus d) \ = \ \big((a \oplus b) \oplus c\big) \oplus d$,
(c) $a \oplus (b \oplus c) \ = \ (c \oplus a) \oplus b$,
(d) $a(bc) \ = \ c(ab)$,
(e) $a\big(b \oplus (c \oplus d)\big) \ = \ (ab \oplus ac) \oplus ad$,
(f) $\big(a(b \oplus c)\big)d \ = \ (ab)d \oplus a(cd)$.

The proof is left as an exercise. ■

Proposition 3.18.

★ *Let $a, b \in R$. Then $b \ominus a \ = \ \ominus(a \ominus b)$.*

PROOF: Since $(R, \oplus)$ is a group and $\ominus x$ denotes the inverse of $x \in R$ this is a reformulation of prop.3.3 on p.58. ■

The following two propositions state that the neutral element with respect to addition is the unique solution of the equation $a \oplus x = a$.

Proposition 3.19 (B/G prop.1.12 and B/G prop.8.13)**.**

Let $x \in R$ satisfy the following:
For each $a \in R$ it is true that $a \oplus x = a$. Then $x = 0$.

PROOF: Left as an exercise. ■

Proposition 3.20 (B/G prop.1.13 and B/G prop.8.14)**.**

Let $x \in R$ satisfy the following:
There exists (at least one) $a \in R$ such that $a \oplus x = a$. Then $x = 0$.

Left as an exercise. ■

Remark 3.5.

Be sure to understand that the last two propositions are different! Both have the same conclusion, $x = 0$, but the assumptions are not the same:

- Prop.3.19 asks for a lot before it allows you to conclude that $x = 0$: **Every** element a of R must satisfy the condition $a \oplus x = a$.
- In contrast prop.3.20 asks for very little so that you may reach the same conclusion: It suffices if you can find **just one** element a of R which satisfies the condition $a \oplus x = a$.

So which of the two propositions is the more powerful one? Of course it is prop.3.20 which allows you to draw the same conclusion under the "weaker" assumption that it suffices to find just one $a \in R$ that satisfies $a \oplus x = a$. □

Proposition 3.21 (B/G prop.1.14 and B/G prop.8.15)**.**

Let $a \in R$. Then $a \odot 0 = 0 = 0 \odot a$.

PROOF: This is Proposition 3.9**(b)**. ■

[1] Beck/Geoghegan: The Art of Proof gives at this spot the definition of divisibilty. We omit it here and provide it in Definition **??** on p.**??**.

The following two propositions show that the neutral element with respect to multiplication is the unique solution of the equation

$$a \odot x = a.$$

Compare them to prop.3.19 and prop.3.20 above, and also review remark 3.5 which follows them.

Proposition 3.22 (B/G prop.1.18 and B/G prop.8.16)**.**

Let $x \in R$ satisfy the following:
For each $a \in R$ it is true that $a \odot x = a$. Then $x = 1$.

PROOF: Left as an exercise. ■

Proposition 3.23 (B/G prop.1.19 and B/G prop.8.17)**.**

Let $x \in R$ satisfy the following:
There exists (at least one) nonzero $a \in R$ such that $a \odot x = a$. Then $x = 1$.

PROOF: See the proof of B/G prop.1.19. ■

Next, we provide more propositions about the additive and multiplicative inverses and about cancellation.

Proposition 3.24 (B/G prop.1.20 and B/G prop.8.18)**.**

Let $a, b \in R$. Then $(\ominus a)(\ominus b) = ab$.

PROOF: See the proof of B/G prop.1.20. ■

Corollary 3.2 (B/G cor.1.21)**.**

$(\ominus 1)(\ominus 1) = 1$.

PROOF: Immediate from prop.3.24. ■

Proposition 3.25 (B/G prop.1.22 and B/G prop.8.19)**.**

(a) *If $a \in R$ then $\ominus(\ominus a) = a$.*
(b) $\ominus 0 = 0$.

PROOF of **(a)**: Left as an exercise.
PROOF of **(b)**: Let $x = \ominus 0$ and $a = 0$. Then

$$a \oplus x \;=\; 0 \oplus (\ominus 0) \;=\; 0 \;=\; a\,.$$

According to Proposition 3.20 (B/G prop.1.13 and B/G prop.8.14) on p.72, the existence of $a \in R$ such that $a \oplus x = a$ implies that $x = 0$. It follows from the above chain of equations that $x = 0$, i.e., $\ominus 0 = 0$. ■

Proposition 3.26 (Unique Solutions of Linear Equations)**.**

Let $(R, \oplus, \odot)$ be an integral domain
and $a, b, y \in R$ such that $a \neq 0$. The equation $y = a \odot x \oplus b$ possesses at most one solution $x \in R$.

PROOF: Let $x, x' \in R$ satisfy $y = a \odot x \oplus b$ and $y = a \odot x' \oplus b$. We must show that $x = x'$.
It follows from our assumptions that $a \odot x \oplus b \;=\; a \odot x' \oplus b$, hence $a \odot x \;=\; a \odot x'$ by prop.3.4 on p.58. It follows from cor.3.1 on p.69 that $x = x'$ ■

Remark 3.6.
Note that the equation $y = a \odot x \oplus b$ need not have a solution. For example, there is no $x \in (\mathbb{Z}, +, \cdot)$ which satisfies the equation $2x + 0 = 1$. □

However the following is true.

Proposition 3.27 (B/G prop.1.23 and B/G prop.8.20)**.**

Let $a, b \in R$. Then there exists one and only one $x \in R$ such that $a \oplus x = b$.

PROOF: Uniqueness follows from Proposition 3.26.

x exists since we can compute it as follows:

$$x \;=\; (\ominus a \oplus a) \oplus x \;=\; \ominus a \oplus (a \oplus x) \;=\; \ominus a \oplus b\,. \;\blacksquare$$

Remark 3.7.

Note that "there exists one and only one ..." is the same as "there exists a unique ..." For this reason a statement like the one in the preceding proposition is also called an **existence and uniqueness statement**. □

Proposition 3.28 (B/G prop.1.24 and B/G prop.8.21)**.**

Let $x \in R$. If $x \odot x = x$ then $x = 0$ or $x = 1$.

PROOF: Left as an exercise. ■

Proposition 3.29 (B/G prop.1.25 and B/G prop.8.22)**.**

Let $a, b \in R$. Then

(a) $\ominus(a \oplus b) \;=\; (\ominus a) \oplus (\ominus b)$,

(b) $\ominus a \;=\; (\ominus 1)a$,

(c) $(\ominus a)b \;=\; a(\ominus b) \;=\; \ominus(ab)$.

PROOF: Left as an exercise. ■

Proposition 3.30 (B/G prop.1.26 and B/G prop.8.23)**.**

Let $a, b \in R$. If $ab = 0$ then $a = 0$ or $b = 0$.

PROOF: This is the no zero divisors condition for integral domains. ■

The next proposition is a collection of properties that involve the difference $a \ominus b = a \oplus (\ominus b)$ of two elements a and b of R.

Proposition 3.31 (B/G prop.1.27 and B/G prop.8.24)**.**

Let $a, b, c, d \in R$. Then

(a) $(a \ominus b) \oplus (c \ominus d) = (a \oplus c) \ominus (b \oplus d)$,
(b) $(a \ominus b) \ominus (c \ominus d) = (a \oplus d) \ominus (b \oplus c)$,
(c) $(a \ominus b)(c \ominus d) = (ac \oplus bd) \ominus (ad \oplus bc)$,
(d) $a \ominus b = c \ominus d$ *if and only if* $a \oplus d = b \oplus c$,
(e) $(a \ominus b)c = ac \ominus bc$.

PROOF: For the proof of **(a)** see B/G prop.1.27. The proofs of **(b)** – **(e)** are left as an exercise. ■

3.4 Order Relations in Integral Domains

Introduction 3.5.

It is possible to introduce an order $a < b$ on certain integral domains $(R, \oplus, \odot)$ by marking the elements of an appropriate subset P of R as positive and saying that x is less than y if the difference $y \ominus x$ is positive, i.e., if $y \ominus x \in P$. This is how we proceed with integers, real and rational numbers. For each of those three number systems the set $P = \{x : x > 0\}$ plays that role.

For example 7 is less than 12 since $12 - 7 > 0$, and $-12 < -7$ since $-7 - (-12) > 0$. Moreover P satisfies the following: If $x, y \in P$, i.e., $x > 0$ and $y > 0$ then $x + y > 0$ and $xy > 0$, i.e., $x + y \in P$ and $xy \in P$. We also note that the number zero is not positive (not negative either), and that it is true for any number x that (either) $x < 0$ or $x = 0$ $x > 0$, i.e., $x \in P$ or $-x \in P$ or $x = 0$. □

The above motivates the following definition.

Definition 3.11 (Ordered Integral Domains)**.**

I. Let $(R, \oplus, \odot)$ be an integral domain. Assume there exists $P \subseteq R$ which satisfies the following:

(a) If $p_1, p_2 \in P$ then $p_1 \oplus p_2 \in P$,
(b) If $p_1, p_2 \in P$ then $p_1 \odot p_2 \in P$,
(c) $0 \notin P$,
(d) Let $a \in R$. Then at least one of the following is true: $a \in P$, $\ominus a \in P$, $a = 0$.

We call P a **positive cone** on the integral domain R.

II. We use P to define on R an "order relation" a $<$ b as follows: Let $a, b \in R$. We define

(3.25) $a < b$ if and only if $b \ominus a \in P$ ("a **is less than** b"),
(3.26) $a \leq b$ if and only if $a < b$ or $a = b$, ("a **is less than or equal** b"),
(3.27) $a > b$ if and only if $b < a$, ("a **is greater than** b"),
(3.28) $a \geq b$ if and only if $b \leq a$. ("a **is greater than or equal** b"),

We say that $<$ is the **order induced by** P, and we call the quadruple $(R, \oplus, \odot, P)$ an **ordered integral domain**. Let $a \in R$. If $a \in P$ then we call a a **positive** element of R, and if $\ominus a \in P$

then we call a a **negative** element of R. If a is positive or zero then we call a **nonnegative**, and if a is negative or zero then we call a **nonpositive**. □

Remark 3.8.

It may seem obvious to you that property **(d)** of a positive cone implies that an element of an ordered integral domain cannot be both positive and negative, but this requires proof! The above will follow easily from prop.3.33 on p.78. □

The next proposition gives the integers $\mathbb{Z}$, the fractions $\mathbb{Q}$, and the real numbers $\mathbb{R}$ as examples of ordered integral domains. It uses the naive definitions of ch.**??** (Preliminaries about Sets, Numbers and Functions) for those sets. We will see in ch.**??** and in ch.**??** that things are the other way around $\mathbb{Z}$ and $\mathbb{R}$ are defined there in an exact manner as ordered integral domains (with additional properties).

Proposition 3.32.

Each of the following algebraic structures is an ordered integral domain:

- ***(a)*** $(\mathbb{Z}, +, \cdot, \mathbb{N})$*: The integers with addition and multiplication: The positive cone is the subset of all natural numbers.*
- ***(b)*** $(\mathbb{Q}, +, \cdot, \mathbb{Q}_{>0})$*: The rational numbers with addition and multiplication: The positive cone* $\mathbb{Q}_{>0}$ *is the subset of all fractions* $\frac{m}{n}$*. where both* m, n *are positive integers.* [7]
- ***(c)*** $(\mathbb{R}, +, \cdot, \mathbb{R}_{>0})$*: The real numbers with addition and multiplication. The positive cone here is* $]0, \infty[$.

There is no suitable positive cone to define an order on the complex numbers $(\mathbb{C}, +, \cdot)$ *with addition and multiplication.* [8]

PROOF: This will be obvious when we see the exact definitions for $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. ■

Notation: In this entire chapter we assume that a fixed ordered integral domain $(R, \oplus, \odot, P)$ is given and phrases such as "let $a \in R$" refer to elements of that integral domain. We further assume that order relations such as "$a < b$" and "$a \geq b$" refer to the order induced by the positive cone P.

For the following see Definition **??** on p.**??** and the subsequent notation alert **??** concerning intervals of integers, real numbers and rational numbers. Convince yourself that the definitions and notations given there are consistent with the following ones for intervals in ordered integral domains.

Definition 3.12 (Intervals in Ordered Integral Domains)**.**

[8] Ignore this comment if you have not learned about complex numbers.

(A) For the following let $a, b \in (R, \oplus, \odot, P)$.
$[a,b]_R := \{x \in R : a \leq x \leq b\}$ is called the **closed interval** with endpoints a and b.
$]a,b[_R := \{x \in R : a < x < b\}$ is called the **open interval** with endpoints a and b.
$[a,b[_R := \{x \in R : a \leq x < b\}$ and $]a,b]_R := \{x \in R : a < x \leq b\}$ are called **half-open intervals** with endpoints a and b.

(B) We generalize the symbol "∞" from real numbers (see Definition **??** on p.**??**) to arbitrary ordered integral domains as follows. The symbol "∞" stands for an object which itself is not an element of $(R, \oplus, \odot, P)$ but is larger than any of its elements, and the symbol "$\ominus\infty$" stands for an object which itself is not an element of $(R, \oplus, \odot, P)$ but is smaller than any of its elements. We thus have $\ominus\infty < x < \infty$ for any $x \in R$. We write $\overset{\oplus}{\ominus}\infty$ when we mean "either $\oplus\infty$ or $\ominus\infty$."
We now define

$$]\ominus\infty, a]_R := \{x \in R : x \leq a\} \qquad]\ominus\infty, a[_R := \{x \in R : x < a\}$$
$$]a, \infty[_R := \{x \in R : x > a\} \qquad [a, \infty[_R := \{x \in R : x \geq a\}. \quad \square$$

Remark 3.9.
The above definition (part **A**) to be precise) does not assume that $a < b$:

- If $a > b$, then $[a,b[_R =]a,b[_R =]a,b]_R = [a,b]_R = \emptyset$.
- If $a = b$, we obtain $[a,a[_R =]a,a[_R =]a,a]_R = \emptyset$, and $[a,a] = \{a\}$. $\square$

Remark 3.10. We are in a very similar situation to that of the introductory remark 3.4 of ch.3.3 on p.70. This time you look at ch.2.1 and 2.2, and then at ch.8.2, of [1] Beck/Geoghegan: The Art of Proof. Again you notice that identical propositions and theorems are given there: First for integers in ch.2, and then again for real numbers in ch.8. Now the reason is prop.3.32 on p.77: Both $(\mathbb{Z}, +, \cdot, \mathbb{N})$ and $(\mathbb{R}, +, \cdot, \mathbb{R}_{>0})$ are ordered integral domains. By the way, so are the rational numbers when ordered by $\mathbb{Q}_{>0}$. Because of this a proposition involving inequalities, e.g., $x < y \Rightarrow x \oplus z < y \oplus z$, need not be demonstrated separately for $\mathbb{Z}$, for $\mathbb{Q}$, and then again for $\mathbb{R}$. We will state and prove such statements for ordered integral domains, and it follows that they hold for all three sets of numbers.

As in ch.3.3 we will merely rephrase propositions and theorems of [1] Beck/Geoghegan: The Art of Proof. We again use "$\oplus$" instead of "$+$", "$\ominus$" instead of "$-$" and "$\odot$" instead of "$\cdot$" for addition, subtraction and multiplication to remind the reader that these rules apply to any other ordered integral domains. $\square$

We begin with a sharpening of part **(d)** of the definition of an ordered integral domain. It says that an element of an ordered integral domain is either positive or negative or zero.

Proposition 3.33 (B/G prop.2.2 and B/G prop.8.27)**.**

*Let $a \in R$. Then **either** $a \in P$ **or** $\ominus a \in P$ or $a = 0$.*

PROOF: We examine separately the cases $a = 0$ and $a \neq 0$.

Case 1: $a = 0$.

Since $0 = \ominus 0$ (see Exercise 3.18 on p.95) it follows from Definition 3.11(c) that both $a = 0 \notin P$ and $\ominus a = \ominus 0 = 0 \notin P$. The proposition thus is correct.

Case 2: $a \neq 0$.

It follows in this case from Definition 3.11(d) that at least one of $a \in P$ or $\ominus a \in P$ is true. Thus there are only three possibilities:

(2a) $a \in P, \ominus a \notin P$,
(2b) $a \notin P, \ominus a \in P$,
(2c) $a \in P, \ominus a \in P$,

Case 2 holds if a satisfies **(2a)** or **(2b)** but it is false if a satisfies **(2c)**. Thus all that remains to be shown for **Case 2** is that **(2c)** can be ruled out.

To state this positively, we want to prove the following:

(*) At most one $a, \ominus a$ is an element of P.

This will be done by means of an **indirect proof**.

> In an indirect proof we play devil's advocate and assume to the contrary that our assertion is false, (i.e., we assume that both $a \in P$ and $\ominus a \in P$), and we show that this assumption leads to a contradiction. Since the only way to avoid that contradiction is not to assume that our assertion is false. It thus must be true. (In this particular case: the statement **(*)** thus must be true.)

So assume to the contrary that both $a \in P$ and $\ominus a \in P$. It follows from Definition 3.11(a) that

$$a \oplus (\ominus a) \in P \qquad \text{i.e.,} \qquad 0 \in P\,.$$

This contradicts property (c) of the positive cone P and we conclude that the assumption that **(*)** is false is faulty. In other words, **(*)** is correct.

We have thus shown that the case **(2c)** can be ruled out and thus **Case 2** holds.

Since **Case 1** and **Case 2** cover all possibilities the entire proof is completed. ■

We begin with a sharpening of part **(d)** of the definition of an ordered integral domain. It says that an element of an ordered integral domain is either positive or negative or zero.

Proposition 3.34 (B/G prop.2.8 and B/G prop.8.33)**.**

> *Let $a, b \in R$. Then either $a < b$ or $a = b$ or $a > b$.*

PROOF: This follows from applying Proposition3.33 on p.78 to $b \ominus a$, because

- $a < b \;\Leftrightarrow\; b \ominus a \in P$,
- $a > b \;\Leftrightarrow\; a \ominus b = \ominus(b \ominus a) \in P$,
- $a = b \;\Leftrightarrow\; b \ominus a = 0$. ■

Remark 3.11.

(a) Prop.3.33 can be restated as follows: Let $a \in R$. Then either a is positive or a is negative or $a = 0$.

(b) It easily follows from prop.3.33 that 0 is the only element of R which is both nonnegative and nonpositive. □

Prop.3.32 on p.77 had introduced the following three ordered integral domains of number systems that you have been very familiar with even before you entered college: The integers $(\mathbb{Z}, +, \cdot, \mathbb{N})$, the real numbers $(\mathbb{R}, +, \cdot, \mathbb{R}_{>0})$, and the rational numbers $(\mathbb{Q}, +, \cdot, \mathbb{Q}_{>0})$. The positive cones which induce the "$<$" order relation are $\mathbb{Q}_{>0}$ for the rational numbers and $\mathbb{R}_{>0}$ for the real numbers. This makes perfect sense, as we have been taught to call numbers positive if and only if they are greater than zero. We chose $\mathbb{N}$ as the positive cone for the integers, and that fits the general mold because $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\} = \mathbb{N}_{>0}$. It is remarkable that the equation $P = \{x \in R : x > 0\}$, as the next proposition demonstrates, is true for any ordered integral domain.

Proposition 3.35 (B/G prop.2.13 and B/G prop.8.38)**.**

If $(R, \oplus, \odot, P)$ is an ordered integral domain, then $P = \{\, x \in R \,:\, x > 0 \,\}$.

Proof strategy:
We will first prove that $P \subseteq \{x \in R : x > 0\}$ and afterwards that $P \supseteq \{x \in R : x > 0\}$.
PROOF of "$\subseteq$": Let $p \in P$. Then $p \ominus 0 = p \in P$, hence $p > 0$, hence $p \in \{x \in R : x > 0\}$.
PROOF of "$\supseteq$": Let $p \in \{x \in R : x > 0\}$. Then $p > 0$, hence $p \ominus 0 \in P$, i.e., $p \in P$. ■

Remark 3.12.
Since $P = \{x \in R : x > 0\}$ (see prop.3.35) 3.11**(a)** can be formulated as follows in the language of sets: $R = P \uplus (\ominus P) \uplus \{0\}$. In other words, $\mathfrak{A} := \{\, P, \ominus P, \{0\} \,\}$ is a partition of the set R in the sense of Definition **??** on p.**??**. □

We have established that $P = \{\, x \in R : x > 0\}$. However, it is not self–understood that $1 > 0$ (equivalently, $1 \in P$).

Proposition 3.36 (B/G prop.2.3 and B/G prop.8.28)**.**

The multiplicative unit 1 *of R belongs to P.*

PROOF: The proof is left as exercise 3.8 (see p.94). ■

Proposition 3.37.

If $a \in R$ then $a \oplus 1 > a$.

Proof: Left as an exercise. ■

Corollary 3.3.

$1 > 0$.

PROOF: This follows from $1 = 1 \oplus 0$ and prop.3.37, applied to $a := 0$. ■

Proposition 3.38 (B/G prop.2.4 and B/G prop.8.29)**.**

Let $a, b, c \in R$.

(3.29) *If $a < b$ and $b < c$, then $a < c$.*

PROOF: Adopt the proof of B/G prop.2.4. ■

Proposition 3.39.

Let $a, b, c \in R$.

(3.30) *If $a \leq b$ and $b \leq c$, then $a \leq c$.*

PROOF: There are four cases.

(1) $a < b, b < c$: It follows from B/G prop.2.4 (transitivity of "<") that $a < c$, in particular, $a \leq c$.

(2) $a < b, b = c$: It follows that $a < c$. This implies $a \leq c$.

(3) $a = b, b < c$: It follows again that $a < c$, hence $a \leq c$.

(4) $a = b, b = c$: It follows that $a = c$. This implies $a \leq c$. ■

Proposition 3.40 (B/G prop.2.5 and B/G prop.8.30)**.**

For each $a \in R$ there exists $p \in P$ such that $a \oplus p > a$.

PROOF: Left as an exercise. ■

Proposition 3.41 (B/G prop.2.6 and B/G prop.8.31)**.**

Let $a, b \in R$. If $a \leq b \leq a$ then $a = b$.

PROOF: Left as an exercise. ■

Proposition 3.42 (B/G prop.2.7 and B/G prop.8.32)**.**

Let $a, b, c, d \in R$. Then
(a) *If $a < b$ then $a \oplus c < b \oplus c$.*
(b) *If $a < b$ and $(c < d)$ then $a \oplus c < b \oplus d$.*
(c) *If $0 < a < b$ and $0 < c \leq d$ then $ac < bd$.*
(d) *If $0 < a \leq b$ and $0 < c \leq d$ then $ac \leq bd$.*
(e) *If $a < b$ and $c < 0$ then $bc < ac$.*

PROOF of **(a)**, **(b)**, and **(e)**: Left as an exercise.

PROOF of **(c)**: Adopt the proof of B/G prop.2.7(iii).

PROOF of **(d)**: If $a < b$ then the proof follows from **(c)**. We thus may assume that $a = b$. But then we also may assume that $c < d$, since otherwise $c = d$, hence $bd = ac$, and nothing remains to prove.

It follows from $a > 0$ that $a = a \ominus 0 \in P$, and it follows from $c < d$ that $d \ominus c \in P$. Thus $a(d \ominus c) \in P$ by Definition 3.11**(b)** on p.76, i.e., $ad \ominus ac \in P$, hence $ad > ac$, hence $ad \geq ac$. ■

Proposition 3.43.

Let $a, b \in R$. Then
(a) *$ab > 0 \Leftrightarrow a, b > 0$ or $a, b < 0$,*
(b) *$ab < 0 \Leftrightarrow$ [either $a > 0$ and $b < 0$] or [$a < 0$ and $b > 0$]*
(c) *$ab = 0 \Leftrightarrow a = 0$ or $b = 0$*

Proof strategy:
In the current situation it is sufficient to prove the "⇐" direction for each of **(a)**, **(b)**, **(c)** to get the "⇒" direction for free in all three cases. Why? Observe that, on account of prop.3.34, the three left hand sides of **(a)**, **(b)**, **(c)** are mutually exclusive and there is no fourth choice (**either** $ab > 0$ **or** $ab < 0$ **or** $ab = 0$), and that the same is also true for the three right hand sides.

Let us abbreviate the left hand side of **(a)** with LS(a), its right hand side with RS(a), the left hand side of **(b)** with LS(b), etc. Assume that we have proven RS(a) ⇒ LS(a), RS(b) ⇒ LS(b) and RS(c) ⇒ LS(c).

Why is it true that then also LS(a) ⇒ RS(a), LS(b) ⇒ RS(b) and LS(c) ⇒ RS(c)? We will show LS(b) ⇒ RS(b). The proof for the other two cases is obtained by the same reasoning:

Assume to the contrary that LS(b) is true but RS(b) is false. Then one of the other cases RS(a) or RS(c) must be true since there are no other options. But RS(a) is not true since RS(a) ⇒ LS(a) was shown to be correct, thus LS(a) is true. It follows that LS(b) is false since the three left hand

expressions are mutually exclusive. We found a contradiction to our assumption that LS(b) is true. We replace "a" with "c" and the same argument show that RS(c) cannot be true either. Since both RS(a) and RS(c) are false and one of RS(a), RS(b), RS(c) must be true it follows that RS(b) is true. We have proven LS(b) $\Rightarrow$ RS(b).

> You should understand that there is nothing magical about the number 3. Assume you have proven the n statements RS(1) $\Rightarrow$ LS(1), RS(2) $\Rightarrow$ LS(2), ..., RS(n) $\Rightarrow$ LS(n) and that it is the case that **either** LS(1) **or** ... **or** LS(n) is true, and also that **either** RS(1) **or** ... **or** RS(n) is true.
> It then follows that LS(1) $\Rightarrow$ RS(1), LS(2) $\Rightarrow$ RS(2), ..., LS(n) $\Rightarrow$ RS(n).

PROOF of the proposition:

PROOF of RS(a) $\Rightarrow$ LS(a):

If $a, b > 0$ then the product ab is positive by Definition 3.11**(b)** on p.76 of a positive cone, and if $a, b < 0$ then the product $ab = \big((\ominus 1)a\big),\ \big(\ominus 1)b\big)$ is positive for the same reason.

PROOF of RS(b) $\Rightarrow$ LS(b):

Assume that $a > 0$ and $b < 0$. It follows from prop.3.42**(e)** (setting $a = 0$) that $a \odot b < 0 \odot b$, i.e., $a \odot b < 0$. We now obtain the proof for $a < 0$ and $b > 0$ by switching the roles of a and b.

PROOF of RS(c) $\Rightarrow$ LS(c): This is true since $u \odot 0 = 0$ for all $u \in R$. (See prop.3.9 on p,67). ■

Next should be the translation of B/G prop.2.9: If $a \in \mathbb{Z}$ and $a \neq 0$ then $a^2 \in \mathbb{N}$. This following proposition does exactly that if you remember that the positive cone for $(\mathbb{Z}, +, \cdot)$ is the set $\mathbb{N}$ of all natural numbers.

Proposition 3.44 (B/G prop.2.9 and prop.8.34)**.**

Let $a \in R$. If $a \neq 0$ then $a^2 \in P$.

The proof is left as exercise 3.10 (see p.94). ■

Proposition 3.45 (B/G prop.2.10 and B/G prop.8.35)**.**

The equation $x^2 = \ominus 1$ has no solution (in R).

The proof is left as exercise 3.11 (see p.94). ■

Proposition 3.46 (B/G prop.2.11 and B/G prop.8.36)**.**

Let $a \in R$ and $p \in P$. If $ap \in P$, then $a \in P$.

PROOF: Left as an exercise. ■

Proposition 3.47 (B/G prop.2.12 and B/G prop.8.37)**.**

Let $a, b, c \in R$. Then

(a) $\ominus a < \ominus b$ *if and only if* $a > b$.
(b) *If* $c > 0$ *and* $ac < bc$ *then* $a < b$.
(c) *If* $c < 0$ *and* $ac < bc$ *then* $b < a$.
(d) *If* $a \leq b$ *and* $0 \leq c$ *then* $ac \leq bc$.

PROOF: Left as an exercise. ■

Ordered integral domains have enough structure to define absolute values.

Definition 3.13 (Absolute value)**.**

For an element x of the ordered integral domain R, we define its **absolute value** as

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ \ominus x & \text{if } x < 0. \end{cases} \quad \square$$

Here are some properties of squares and absolute values.

Proposition 3.48 (Generalization of B/G prop.10.5)**.**

Let $x, y \in P \cup \{0\}$, i.e., $x, y \geq 0$. Then

(a) $x \leq y$ *if and only if* $x^2 \leq y^2$,
(b) $x = y$ *if and only if* $x^2 = y^2$,
(c) $x < y$ *if and only if* $x^2 < y^2$.

The proof is left as exercise 3.12 (see p.94). ■

Proposition 3.49 (B/G prop.10.6)**.**

Let $a \in R$. Then $|a|^2 = a^2$.

The proof is left as exercise 3.13 (see p.94). ■

Proposition 3.50 (B/G prop.10.7)**.**

Let $a, b \in R$. Then $|a| < |b| \;\Leftrightarrow\; a^2 < b^2$.

PROOF: Left as an exercise. ■

The next two propositions are very similar. We will see in ch.**??** (Normed Vector Spaces) that prop.3.51 shows that if $(R, \oplus, \odot, P) = (\mathbb{R}, +, \cdot, \mathbb{R}_{>0})$ then the absolute value satisfies the properties of a norm.

The subsequent proposition 3.52 shows that the assignment $(a, b) \mapsto |b \ominus a|$ turns the ordered integral domain $(\mathbb{R}, +, \cdot, \mathbb{R}_{>0})$ into a metric space. See Chapter**??** (Metric Spaces and Topological Spaces – Part I).

Proposition 3.51 (B/G prop.10.8)**.**

Let $a, b \in R$. Then the following holds:
- ***(a)*** $|a| = 0$ *if and only if* $a = 0$,
- ***(b)*** $|ab| = |a| \odot |b|$,
- ***(c)*** $\ominus|a| \le a \le |a|$,
- ***(d)*** $|a \oplus b| \le |a| \oplus |b|$,
- ***(e)*** *if* $\ominus b < a < b$ *then* $|a| < b$, *in particular,* $b \ge 0$.

PROOF: The proofs of **(a)** and **(d)** can be found in [1] Beck/Geoghegan Art of Proof The proof of the other parts is left as an exercise. ■

Remark 3.13.

Actually B/G prop.10.8**(e)** states that $\ominus b < a < b$ then $|a| < |b|$.

But we see that $b \ge 0$ (and hence $b = |b|$) as follows:

$\ominus b < a < b$ implies that $\ominus b < b$. Assume to the contrary that $b < 0$. Then $\ominus b > 0$, thus $\ominus b < a < b < 0 < \ominus b$, thus $\ominus b < \ominus b$. We have reached a contradiction. □

Proposition 3.52 (B/G prop.10.10)**.**

If $a, b, c \in R$, then
- ***(a)*** $|a \ominus b| = 0 \;\Leftrightarrow\; a = b$,
- ***(b)*** $|a \ominus b| = |b \ominus a|$,
- ***(c)*** $|a \ominus b| \le |a \ominus c| \oplus |c \ominus b|$,
- ***(d)*** $|a \ominus b| \ge \big||a| \ominus |b|\big|$.

PROOF: The proof is left as exercise 3.14 (see p.94). ■

We will give two (very short) proofs for the next proposition. Which one do you prefer?

Proposition 3.53.

*This proposition is similar to prop.3.51**(e)**.*
*Let $a, b \in R$ such that both **#1)** $\ominus a \leq b$ and **#2)** $a \leq b$. Then $|a| \leq b$.*

FIRST PROOF:

Case 1) $a \geq 0$: It follows from #**2** that $|a| = a \leq b$, which is what we had to show.

Case 2) $a < 0$: It follows from #**1** that $|a| = \ominus a \leq b$, which is what we had to show.

SECOND PROOF:

Here is an alternate proof which avoids using separate cases.

#**1** is equivalent to $a \geq \ominus b$, thus #**1** and #**2** together yield, $\ominus b \leq a \leq b$. It follows from prop.3.51**(e)** above that $|a| < b$. ■.

3.5 Minima, Maxima, Infima and Suprema in Ordered Integral Domains

Notation: In this entire chapter we assume that a fixed ordered integral domain $(R, \oplus, \odot, P)$ is given and phrases such as "let $a \in R$" refer to elements of that integral domain. We further assume that order relations such as "$a < b$" and "$a \geq b$" refer to the order induced by the positive cone P. **Do not confuse** the symbol R for this integral domain with the symbol $\mathbb{R}$ for the real numbers!

We have seen in prop.3.34 that any two elements a, b of R can be compared: Either $a < b$ or $a = b$ or $a > b$. [9] This makes it possible to introduce boundedness, least upper bounds, greates lower bounds, maxima and minima for certain subsets of R. [10]

Definition 3.14 (Upper and lower bounds, maxima and minima)**.**

Let $A \subseteq R$ and let $l, u \in R$.

- **(a)** We call l a **lower bound** of A if $l \leq a$ for all $a \in A$.
- **(b)** We call u an **upper bound** of A if $u \geq a$ for all $a \in A$.
- **(c)** We call A **bounded above** if this set has an upper bound.
- **(d)** We call A **bounded below** if A has a lower bound.
- **(e)** We call A **bounded** if A is both bounded above and bounded below.
- **(f)** A **minimum** (min) of A is a lower bound l of A such that $l \in A$.
- **(g)** A **maximum** (max) of A is an upper bound u of A such that $u \in A$. □

[9] In ch.?? (Cartesian Products and Relations) we will call sets which carry such an order relation linearly, or totally, ordered. See Definition ?? on p.??.

[10] Those concepts will also be introduced for so called partially ordered sets. See Definition ?? on p.??.

Remark 3.14. The empty set does not possess a maximum or minimum because either would have to be an element of $\emptyset$. $\square$

Proposition 3.54.

Let $A \subseteq R$. If A has a maximum or a minimum, then it is unique.

Proof for maxima: Let u_1 and u_2 be two maxima of A: both are upper bounds of A and both belong to A.

As u_1 is an upper bound it follows that $a \leq u_1$ for all $a \in A$. Hence $u_2 \leq u_1$.

Now we switch the roles of u_1 and u_2 and the same reasoning as above yields $u_1 \leq u_2$.

We thus have equality $u_1 = u_2$. The proof for minima is similar. ■

The last proposition makes it possible to write $\min(A)$ for the minimum of A and $\max(A)$ for the maximum of A in case those items exist for a subset A of R.

Definition 3.15.

Let $A \subseteq R$. If A possesses a minimum, we write

$$\min(A) \quad \text{or} \quad \min A$$

for this uniquely determined element of R. Likewise, if A possesses a maximum, we write

$$\max(A) \quad \text{or} \quad \max A$$

for that uniquely determined element of R. $\square$

Definition 3.16.

$\star$ Let $A \subseteq R$. We define

$$\begin{aligned} A_{lowb} &:= \{l \in R : l \text{ is lower bound of } A\} \\ A_{uppb} &:= \{u \in R : u \text{ is upper bound of } A\}. \end{aligned} \tag{3.31}$$

$\square$

Remark 3.15. The sets A_{lowb} and/or A_{uppb} may be empty. Examples to that effect are $A = \mathbb{R}$, $A =]0, \infty[$, $A = A =]-\infty, 0[$. $\square$

Remark 3.16. Note that A is bounded above if and only if $A_{uppb} \neq \emptyset$ and bounded below if and only if $A_{lowb} \neq \emptyset$. □

If A is a nonempty subset of R then the set A_{lowb} of its lower bounds need not not necessarily possess a maximum, but if $max(A_{lowb})$ exists then this element of R will be the greatest of all lower bounds of A. This warrants the following definition.

Definition 3.17 (Infimum and supremum in an ordered integral domain)**.**

Let A be a nonempty subset of R.

(a) If $\max(A_{lowb})$ exists then it is unique by prop.3.54. We write $\inf(A)$ or g.l.b.(A) for $\max(A_{lowb})$ and call this number the **infimum** or **greatest lower bound** of A.

(b) If $\min(A_{uppb})$ exists then it is unique by prop.3.54. We write $\sup(A)$ or l.u.b.(A) for $\min(A_{uppb})$ and call this element of R the **supremum** or **least upper bound** of A. □

Remark 3.17. If the set A has no upper bounds then A_{uppb} is empty, hence does not possess a minimum (see rem3.14 above), hence $\sup(A)$ does not exist. Likewise, if A has no lower bounds then $\inf(A)$ does not exist. We will introduce infima and suprema for unbounded sets later in this chapter. See Definition 3.18 on p.90. □

Example 3.8.

(a) Let $A := \{\frac{1}{j} : j \in \mathbb{N}\}$. If we consider A as a subset of $\mathbb{Q}$ then $A_{lowb} =]-\infty, 0]_{\mathbb{Q}}$ possesses 0 as it maximum, i.e., $\inf(A) = 0$, but A has no minimum because $0 \notin A$.

(b) Let $A := \{\frac{1}{j} : j \in \mathbb{N}\}$, just as in **(a)**, but now we consider A as a subset of $\mathbb{R}$. Then $A_{lowb} =]-\infty, 0]$ possesses 0 as it maximum, i.e., $\inf(A) = 0$, but A has no minimum because $0 \notin A$. Thus the situation is the same as for $\mathbb{Q}$.

(c) [11] We remind the reader that the real number $\sqrt{2}$ is not rational. [12]

Let $B := \{\frac{n}{d} : n, d \in \mathbb{N} \text{ and } \frac{n^2}{d^2} < 2\}$, i.e., the set of all positive, rational, numbers with a square less than 2. Then $\inf(B) = 0$ and $\min(B)$ does not exist ($0 \notin B$!) regardless whether we consider B a subset of the integral domain $R = \mathbb{Q}$ or $R = \mathbb{R}$. However we have different outcomes for the upper "boundary" of B.

One can prove that $\sup(B)^2 = 2$, i.e., that $\sup(B) = \sqrt{2}$ exists as an element of $\mathbb{R}$. [13] On the other hand it follows from $\sup(B)^2 = 2$ that $\sup(B) \notin B$. Thus the set B has a supremum but not a maximum in $\mathbb{R}$.

In contrast to the above $\sup(B)$ does not exist in $\mathbb{Q}$ because, as mentioned, the square of $\sup(B)$ would have to be 2 and $\sqrt{2}$ is not rational. Thus B possesses neither supremum nor maximum in $\mathbb{Q}$.

[11] An example very similar to this one is example **??** on p.**??**.
[12] See rem.**??** on p.**??**.
[13] The proof is given in prop.**??** on p.**??**.

(d) Let $(R, +, \cdot)$ be the ordered integral domain of either the rational or the real numbers, and let $C := \{k \in R : 0 < 2k < 7\}$. For both $R = \mathbb{Q}$ and $R = \mathbb{R}$ we have $\inf(C) = 0$, $\sup(C) = 3/2$. However, both $\min(C)$ and $\max(C)$ do not exist since neither 0 nor $3/2$ belongs to C.

(e) Let $R = \mathbb{Z}$ and $C := \{k \in R : 0 < 2k < 7\}$. Then $\min(C) = 1$ and $\max(C) = 3$. The reason: $1 \in C$ is a lower bound of C, $3 \in C$ is an upper bound of C, and 1 and 3 belong to R. □

We stay away from using functions in the context of integral domains as much as possible because we use them mainly as a generalization of the number systems given by the integers, the rational numbers, and the real numbers. The following is an exception because this material on minima, maxima, infima and suprema is referred to in later chapters.

Notation 3.2.

Notational conveniences:

(a) We may drop the parentheses in expressions like $\max(A)$, $\sup(\{f(x) : x \in B\})$ (here $f : X \to R$ is a function which takes values in an ordered integral domain R and where $B \subseteq X$), etc., if this does not lead to any confusion. We also can write the above as $\max A$ and $\sup\{f(x) : x \in B\}$.

(b) If A consists of two elements $x, y \in R$, i.e., $A = \{x, y\}$ then it is customary to write $\max(x, y)$, $\min(x, y)$, $\sup(x, y)$, and $\inf(x, y)$. □

Proposition 3.55. *Let $A \subseteq R$. If A has a maximum then it also has a supremum, and* $\max(A) = \sup(A)$. *Likewise, if A has a minimum then it also has an infimum, and* $\min(A) = \inf(A)$.

PROOF: The proof is left as exercise 3.15. ■

Remark 3.18.

One can say informally that a supremum is a generalized maximum – generalized in the sense that it need not belong to the set under consideration. Examples for this are given in ch.**??** when looking at the ordered integral domain of the real numbers. See examples **??** and **??** on p.**??**.

Proposition 3.56.

Let $\emptyset \neq A \subseteq B \subseteq R$.

(a) *If both A and B possess an infimum (resp., supremum) then* $\inf(A) \geq \inf(B)$ *(resp.,* $\sup(A) \leq \sup(B)$*).*

(b) *If both A and B possess a minimum (resp., maximum) then* $\min(A) \geq \min(B)$ *(resp.,* $\max(A) \leq \max(B)$*).*

(c) *If both A and B possess a minimum (resp., maximum) and* $\min(B) \notin A$ *(resp.,* $\max(B) \notin A$*) then* $\min(A) > \min(B)$ *(resp.,* $\max(A) < \max(B)$*).*

PROOF: We prove **(a)** for suprema. The proof for infima is similar. It follows from $A \subseteq B$ that any upper bound of B also is an upper bound of A. We obtain in particular $\sup(B) \in A_{upp}$, hence $\sup(A) = \min(A_{upp}) \leq \sup(B)$.

Note that **(b)** follows from **(a)** because if a set has a minimum then it equals its infimum and if a set has a maximum then it equals its supremum.

We now prove **(c)** for minima. The proof for maxima is similar. If $\min(B) \notin A$ then $\min(A) \in A$ implies $\min(B) \neq \min(A)$. That together with $\min(B) \leq \min(A)$ yields $\min(B) < \min(A)$. ■

Remark 3.19.

It is expedient to define $\inf(A)$ if $A \subseteq R$ is empty or has no lower bounds and to define $\sup(A)$ if A is empty or has no upper bounds. If A has no lower bounds (and hence is not empty)

(A) We recall that if $\inf(A)$ exists then it is a lower bound of A, and if $\sup(A)$ exists then it is an upper bound of A. Thus $\inf(A) \leq a \leq \sup(A)$ for all $a \in A$. If A is not bounded below then $\ominus\infty$ is the only object x that satisfies $x \leq a$ for all $a \in A$; if A is not bounded above then ∞ is the only object x that satisfies $x \geq a$ for all $a \in A$. It thus makes sense to define $\inf(A) := \ominus\infty$ if A has no lower bounds and $\sup(A) := \infty$ if A has no upper bounds.

(B) Prop.3.56**(a)** above suggests how to handle the empty set: Since $\emptyset \subseteq B$ for all $B \subseteq R$ and the infimum becomes bigger for smaller sets we would want $\inf(\emptyset)$ to be as large as possible, i.e., $\inf(\emptyset)$ should be ∞. Further $\sup(\emptyset)$ should be as small as possible, i.e., this value should be $\ominus\infty$. □

So we arrive at the following definition.

Definition 3.18 (Supremum and Infimum of unbounded and empty sets)**.**

⋆

Let $A \subseteq R$. If A is not bounded above, we define

$$\sup A = \infty \tag{3.32}$$

If A is not bounded below, we define

$$\inf A = \ominus\infty \tag{3.33}$$

Finally, we define

$$\sup \emptyset = \ominus\infty, \qquad \inf \emptyset = \oplus\infty. \ \square \tag{3.34}$$

The definitions given above for the empty set will work harmoniously with (**??**) on p.**??** in ch.**??** (More on Set Operations) where $\bigcup_{i\in\emptyset} A_i$ and $\bigcap_{i\in\emptyset} A_i$ are defined.

Remark 3.20.

Be aware that even though we allow $\sup(A) = \overset{\oplus}{\ominus}\infty$ and $\inf(A) = \overset{\oplus}{\ominus}\infty$ we do not allow $\max(A) = \overset{\oplus}{\ominus}\infty$ or $\min(A) = \overset{\oplus}{\ominus}\infty$.

The reason: By definition of, e.g., the maximum, if $\max(A)$ exists then it must satisfy $\max(A) \in A$, hence $\max(A) \in R$. Since the infinity values are not elements of R it is not possible that, e.g., $\max(A) = \overset{\oplus}{\ominus}\infty$. □

Proposition 3.57.

Let $A \subseteq B \subseteq R$.
(a) *If* $\inf(A)$ *and* $\inf(B)$ *both exist then* $\inf(A) \geq \inf(B)$.
(b) *If* $\sup(A)$ *and* $\sup(B)$ *both exist then* $\sup(A) \leq \sup(B)$.

PROOF:
The above was proven in prop.3.56 under the condition that $\inf(A)$, $\inf(B)$, $\sup(A)$, $\sup(B)$ exist as elements of R, i.e., we did not permit the values $\overset{\oplus}{\ominus}\infty$.

We prove this proposition for suprema. The proof for infima is similar. If $A \neq \emptyset$ (hence $B \neq \emptyset$) and B is bounded above (hence A is bounded above) then **(B)** follows from prop.3.56.

Otherwise $A = \emptyset$ in which case $\sup(A) = \ominus\infty \leq \inf(B)$, or B is not bounded above, in which case $\sup(A) \leq \infty = \sup(B)$. In either case **(B)** holds. ■

Recall for the following that $\ominus A = \{\ominus a : a \in A\}$ (see Definition 3.8 on p.66).

Proposition 3.58.

Let $A \subseteq R$ and $x \in R$. Then

$$x \leq a \text{ for all } a \in A \quad \Leftrightarrow \quad \ominus x \geq a' \text{ for all } a' \in \ominus A, \tag{3.35}$$

$$x \in A_{lowb} \quad \Leftrightarrow \quad \ominus x \in (\ominus A)_{uppb}, \tag{3.36}$$

$$\ominus A_{lowb} \quad = \quad (\ominus A)_{uppb}, \tag{3.37}$$

$$x \geq a \text{ for all } a \in A \quad \Leftrightarrow \quad \ominus x \leq a' \text{ for all } a' \in \ominus A, \tag{3.38}$$

$$x \in A_{uppb} \quad \Leftrightarrow \quad \ominus x \in (\ominus A)_{lowb}, \tag{3.39}$$

$$\ominus A_{uppb} \quad = \quad (\ominus A)_{lowb}, . \tag{3.40}$$

PROOF: We have

$$x \leq a \text{ for all } a \in A \quad \Leftrightarrow \quad \ominus x \geq \ominus a \text{ for all } a \in A \quad \Leftrightarrow \quad \ominus x \geq \ominus a \text{ for all } \ominus a \in \ominus A.$$

Replacing $\ominus a$ with a' yields (3.35). We now obtain (3.36) from (3.35) and (3.31). (3.37) follows from

$$x \in \ominus A_{lowb} \;\Leftrightarrow\; \ominus x \in A_{lowb} \overset{(3.36)}{\Longleftrightarrow} \ominus(\ominus x) \in (\ominus A)_{uppb} \;\Leftrightarrow\; x \in (\ominus A)_{uppb}.$$

We exchange the roles of $\leq$ and $\geq$ and apply similar arguments to obtain (3.38) through (3.40). ■

Proposition 3.59.

Let $\emptyset \neq A \subseteq R$. If the maximum of A_{lowb} exists, the following holds true:
A has lower bounds, $\ominus A$ has lower bounds, the minimum of $(\ominus A)_{\text{uppb}}$ exists, and we have

$$\ominus \max(A_{\text{lowb}}) = \min\big((\ominus A)_{\text{uppb}}\big), \tag{3.41}$$

$$\ominus \min(A_{\text{uppb}}) = \max\big((\ominus A)_{\text{lowb}}\big). \tag{3.42}$$

PROOF: Let $a^\star := \max(A_{\text{lowb}})$. Since a set contains it maximum, $a^\star \in A_{\text{lowb}}$, hence $\ominus a^\star \in \ominus A_{\text{uppb}}$ by (3.36). To prove that $\ominus a^\star = \min\big((\ominus A)_{\text{uppb}}\big)$ we must show that $u \geq \ominus a^\star$ for all $u \in (\ominus A)_{\text{uppb}}$.
So let $u \in (\ominus A)_{\text{uppb}}$. It follows from (3.31) that $u \geq a'$ for all $a' \in \ominus A$, hence, by (3.41), $\ominus u \leq a$ for all $a \in A$. Thus $\ominus u$ is a lower bound of A, i.e., $\ominus u \in A_{\text{lowb}}$. Since $a^\star = \max(A_{\text{lowb}})$ it follows that $\ominus u \leq a^\star$, i.e., $u \geq \ominus a^\star$. This is what we needed to show. ■

Corollary 3.4.

The following equations are to be understood in the sense that if the item on the left exists and vice versa, and both sides then are equal.

$$\ominus \inf(A) = \sup(\ominus A), \tag{3.43}$$

$$\ominus \sup(A) = \inf(\ominus A), \tag{3.44}$$

$$\ominus \min(A) = \max(\ominus A). \tag{3.45}$$

$$\ominus \max(A) = \min(\ominus A), \tag{3.46}$$

PROOF: (3.43) is obtained from (3.41) and (3.44) is obtained from (3.42) by the very definition of suprema as minimal upper bounds and infima as maximal lower bounds. We now obtain (3.45) and (3.46) from prop.3.55 on p.89. ■

Draw a picture for numbers a, b, c to visualize the content of the following proposition and its corollary.

Proposition 3.60.

Let a, b be nonnegative elements of R. Then

$$|b \ominus a| \leq \max(a, b), \quad \textit{i.e.,} \tag{3.47}$$

$$\ominus \max(a, b) \leq b \ominus a \leq \max(a, b). \tag{3.48}$$

PROOF: The proof is left as exercise 3.16 (see p.95). ■

Corollary 3.5.

Let $a, b, c \in R$ such that $0 \leq a, b < c$. Then

(3.49) $$\ominus c \ < b \ominus a \ < \ c.$$

PROOF: Follows from prop.3.60 with $c := \max(a, b)$. ■

3.6 Exercises for Ch.3

Exercise 3.1.

From example 3.1 on p.54:

(a) What laws for the addition of numbers do you need to use to prove that $(\mathbb{Z}, +)$ (the integers with addition) is an abelian group?

(b) What laws for the multiplication of numbers do you need to use to prove that $(\mathbb{Q} \setminus \{0\}, \cdot)$ (the nonzero rational numbers with with multiplication) is an abelian group?

(c) What about $(\mathbb{R}, \cdot)$ Is that a semigroup? a monoid? a group? an abelian group? □

Exercise 3.2.

Let $(G, \diamond)$ be a commutative group with neutral element e. Let $g, h_1, h_2 \in G$ such that

$$g \diamond h_1 \ = e \qquad \text{and} \qquad g \diamond h_2 \ = e\,.$$

Use the material before Proposition 3.2 on p.57 to prove that $h_1 = h_2$. □

Exercise 3.3.

Let $(S, \diamond)$ be a semigroup. Let $a, b, c, d \in S$. Use the definition of a semigroup only to prove that

(a) $a \diamond \big(b \diamond (c \diamond d)\big) \ = \ (a \diamond b) \diamond (c \diamond d)$,

(b) $\big(a \diamond (b \diamond c)\big) \diamond d \ = \ (a \diamond b) \diamond (c \diamond d)$. □

Exercise 3.4.

Let $(S, \diamond)$ be a commutative semigroup, i.e., S is a semigroup which satisfies $s \diamond t \ = \ t \diamond s$ for all $s, t \in S$. Let $a, b, c \in S$. Prove that

$$a \diamond (b \diamond c) \ = \ c \diamond (a \diamond b)$$

Exercise 3.5.

Prop.3.3 on p.58 of this document states that if g, h are elements of a group $(G, \diamond)$ then $h \diamond g^{-1} = (g \diamond h^{-1})^{-1}$. The proof only demonstrated that $(h \diamond g^{-1}) \diamond (g \diamond h^{-1}) = e$. Prove what has been omitted, i.e., the equation $(g \diamond h^{-1}) \diamond (h \diamond g^{-1}) = e$. □

Exercise 3.6.

Prove part **(b)** of prop.3.10 on p.67 of this document:

Let $(R, \oplus, \odot)$ be a nonempty set with two binary operations $\oplus$ and $\odot$ which satisfies **(a)**, **(b)**, **(c)** of Definition 3.7. Then the following is true:

$1 = 0 \Leftrightarrow R = \{0\}$. □

Exercise 3.7.

Let $(R, \oplus, \odot)$ be an integral domain and $a, b, c, d \in R$. Prove that $\big(a \oplus (b \oplus c)\big) \oplus d = (a \oplus b) \oplus (c \oplus d)$. Do so without using the results of prop.3.17! □

Exercise 3.8. Prove prop.3.36 on p.80: The multiplicative unit 1 of R belongs to P. □

Exercise 3.9.

Use everything up to AND including prop.3.36 on p.80 to prove prop.3.37 on p.80 of this document: If R is an ordered integral domain and $a \in R$ then $a \oplus 1 > a$. □

Exercise 3.10. Prove prop.3.44 on p.83 of this document:

If $a \in (R, \oplus, \odot, P)$ and $a \neq 0$ then $a^2 \in P$. □

Exercise 3.11. Prove prop.3.45 on p.83 of this document:

The equation $x^2 = \ominus 1$ has no solution (in R). □

Exercise 3.12.

Prove prop.3.48 on p.84 of this document: If $x, y \in P \cup \{0\}$ then

- **(a)** $x \leq y$ if and only if $x^2 \leq y^2$,
- **(b)** $x = y$ if and only if $x^2 = y^2$,
- **(c)** $x < y$ if and only if $x^2 < y^2$.

Hint: Do the proof of **(a)**, $\Leftarrow$) separately for $x^2 = y^2$ and $x^2 < y^2$. □

Exercise 3.13.

Prove prop.3.49 on p.84 of this document:

Let $a \in R$. Then $|a|^2 = a^2$. □

Exercise 3.14.

Prove prop.3.52 on p.85 of this document: Let $a, b, c \in R$. Then the following are true.

- **(a)** $|a \ominus b| = 0 \Leftrightarrow a = b$,
- **(b)** $|a \ominus b| = |b \ominus a|$,
- **(c)** $|a \ominus b| \leq |a \ominus c| \oplus |c \ominus b|$,
- **(d)** $|a \ominus b| \geq \big||a| \ominus |b|\big|$. □

Exercise 3.15.

Prove prop.3.55 on p.89 of this document: Let $A \subseteq R$. If A has a maximum then it also has a supremum, and $\max(A) = \sup(A)$. Likewise, if A has a minimum then it also has an infimum, and $\min(A) = \inf(A)$. □

Exercise 3.16.

Prove prop.3.60 on p.92 of this document: Let a, b be nonnegative elements of R. Then

$$|b \ominus a| \;\leq\; \max(a,b), \quad \text{i.e.,} \quad \ominus \max(a,b) \;\leq\; b \ominus a \;\leq\; \max(a,b).$$

Hint: Handle separately the cases $b \geq a$ and $b < a$. □

Exercise 3.17.

Let $R := (R, \oplus, \odot, P)$ be an ordered integral domain and $W \subseteq R$.

(A) Prove that the set W_{uppb} of the upper bounds of W satisfies either of the following:

(a) $W_{uppb} = [z, \infty[_R$ for some suitable $z \in R$,
(b) $W_{uppb} =]z, \infty[_R$ for some suitable $z \in R$,
(c) $W_{uppb} =] \ominus \infty, \infty[_R$ (i.e., $W_{uppb} = R$).

(B) For what sets W is $W_{uppb} = R$? □

Exercise 3.18.

Prove that if $(G, \diamond)$ is a group with neutral element e then e has itself as an inverse, i.e.,

(3.50) $$e^{-1} \;=\; e\,.$$ □

References

[1] Matthias Beck and Ross Geoghegan. The Art of Proof. Springer, 1st edition, 2010.

List of Symbols

Index