Math 330 - Additional Material

Student edition with proofs

Michael Fochler
Department of Mathematics
Binghamton University

This document contains chapter 6 of the Math 330 lecture notes.

Last update: February 17, 2026

Contents

6 The Integers

Note to Math 330 students: This chapter contains a lot of, but by no means all of the material of chapters 2.3, 2.4, 4, 6 and 7 of [1] Beck/Geoghegan: Art of Proof. On the other hand this chapter also contains some generalizations which cannot be found in that book, and I have given alternate versions of some proofs which I found difficult to follow. An other reason to duplicate that material here is that doing so allows this author to give internal references which you can click on rather than having to go back and forth between two different sources.

Note to Math 330 students: You should read this chapter in parallel with chapters 2, 4, 6 and 7 of [1] Beck/Geoghegan Art of Proof

6.1 The Integers, the Induction Axiom, and the Induction Principles

In ch.**??** (Numbers) on p.**??** we informally defined the integers $\mathbb{Z}$ as those numbers n which can be expressed as finite strings of decimal digits, possibly preceded by a minus sign. This is problematic from a very unexpected perspective: We will need a precise definition of the integers as a prerequisite for a precise definition of finiteness.

We also defined the natural numbers just as informally as the set $\mathbb{N} = \{1, 2, 3, \dots\}$. We will now give precise, axiomatic, definitions of those sets by using as a starting point prop.**??(a)** on p.**??**, which asserts that $(\mathbb{Z}, +, \cdot, \mathbb{N})$ is an ordered integral domain. This "proposition" was stated at a point where the exact definition of $\mathbb{Z}$ and $\mathbb{N}$ was not provided yet. The next axiomatic definition will close that gap.

Since addition and multiplication are associative in integrals domains $(R, \oplus, \odot)$ we will heneforth write $a \oplus b \oplus c$ for either of $(a \oplus b) \oplus c$, $a \oplus (b \oplus c)$, and $a \odot b \odot c$ for either of $(a \odot b) \odot c$, $a \odot (b \odot c)$. Here we assumed that $a, b, c \in R$.

The case of more than three operands will be taken care of later by Theorem 6.7 (Generalized Law of Associativity) on p.220.

Axiom 6.1 (Integers and Natural Numbers)**.**

We postulate the existence of two sets, $\mathbb{Z}$ and $\mathbb{N}$, which satisfy the following:

- **(a)** $\mathbb{Z}$ is endowed with two binary operations "$+$" (called addition) and "$\cdot$" (called multiplication) and with a positive cone $\mathbb{N}$ such that $(\mathbb{Z}, +, \cdot, \mathbb{N})$ is an ordered integral domain. We denote the additive unit of this integral domain by 0 and its multiplicative unit by 1.
- **(b)** **Induction Axiom**: Let $A \subseteq \mathbb{Z}$ such that
  - **(1)** $1 \in A$,
  - **(2)** $k \in A$ implies $k + 1 \in A$.

  Then $A \supseteq \mathbb{N}$.

We call $\mathbb{Z}$ the set of **integers**, and we call $\mathbb{N}$ the set of **natural numbers**. □

So far the only two integers we know are 0 (the neutral element for "+"), and 1 (the neutral element for "·"). That suffices to define eight more elements of $\mathbb{Z}$.

Definition 6.1 (Decimal Digits)**.**

We use 1 (the neutral element for "·") and addition $a+b$ to define the following integers:

$$2 := 1+1,\ 3 := 2+1,\ 4 := 3+1,\ 5 := 4+1,\ 6 := 5+1,\ 7 := 6+1,\ 8 := 7+1,\ 9 := 8+1\,.$$

We call the elements of the set $\{0,1,2,3,4,5,6,7,8,9\}$ **digits** aka **decimal digits**. □

Remark 6.1.

Note that all we needed to define those decimal digits were the existence of $0, 1$, and the "+" operation Thus, we could have defined them for any integral domain, even for any commutative ring with unit. □

Remark 6.2. Let $m, n \in \mathbb{Z}$. We remind the reader that precise definitions were given at the beginning of ch.**??** on p.**??** about statements like, e.g., $m < n$ (it means that $n - m \in \mathbb{N}$), about positivity (n is positive if and only if $n \in \mathbb{N}$), and about negativity (n is negative if and only if $-n \in \mathbb{N}$).

The following simple proposition and its corollary will allow us to generalize the induction axiom to sets of the form $[k_0, \infty[_{\mathbb{Z}} = \{k \in \mathbb{Z} : j \geq k_0\}$ where k_0 is an arbitrary integer.

Proposition 6.1.

Let $i, j, n \in \mathbb{Z}$. Then

$$n + i \in [i, \infty[_{\mathbb{Z}} \Leftrightarrow\ n + j \in [j, \infty[_{\mathbb{Z}}\,.$$

The proof is left as exercise 6.1 (see p.251). ■

Corollary 6.1.

Let $k_0, n \in \mathbb{Z}$. Then

$$n \in [k_0, \infty[_{\mathbb{Z}} \Leftrightarrow\ n - k_0 + 1 \in \mathbb{N}\,.$$

PROOF: We apply prop.6.1 with $n - k_0$ instead of n, k_0 instead of i, and 1 instead of j:

$$(n - k_0) + k_0 \in [k_0, \infty[_{\mathbb{Z}} \Leftrightarrow \ (n - k_0) + 1 \in [1, \infty[_{\mathbb{Z}}, \quad \text{i.e.,} \quad n \in [k_0, \infty[_{\mathbb{Z}} \Leftrightarrow \ n - k_0 + 1 \in \mathbb{N}. \ \blacksquare$$

Theorem 6.1 (Generalization of the Induction Axiom)**.**

Let $k_0 \in \mathbb{Z}$ and let

$$A_{k_0} \ := \ \{k \in \mathbb{Z} : j \geq k_0\} \ = \ [k_0, \infty[_{\mathbb{Z}}$$

be the set of all integers at least as big as k_0. Let $A \subseteq \mathbb{Z}$ such that

(a) *$k_0 \in A$,*

(b) *$k \in A$ implies $k + 1 \in A$.*

Then $A \supseteq A_{k_0}$.

Proof strategy: We will shift everything by the amount $-k_0 + 1$: Let

$$(\mathbf{A}) \qquad B \ := \ 1 - k_0 + A \ = \ \{\, a - k_0 + 1 \ : \ a \in A \,\}\,.$$

Our proof then proceeds as follows.

(1) Show that $1 \in B$.

(2) For an arbitrary $b \in B$ let $a := b + k_0 - 1$ be the corresponding item in A. By assumption, $a + 1 \in A$. Use this to show that $b + 1 \in B$.

(3) It follows from **(1)** and **(2)** that B satisfies both properties **(1)** and **(2)** of the induction axiom, thus $B \supseteq \mathbb{N}$.

(4) We complete the proof by adding $k_0 - 1$ to both B and $\mathbb{N}$ and obtaining $A \supseteq A_{k_0}$.

PROOF of Theorem 6.1:

So let $B := 1 - k_0 + A$. Since $k_0 \in [k_0, \infty[_{\mathbb{Z}}$ and $[k_0, \infty[_{\mathbb{Z}} \subseteq A$, $k_0 \in A$. Thus $1 = k_0 - k_0 + 1 \in B$. This proves step **(1)**.

Let $b \in B$ and $a := b + k_0 - 1$. Then $a \in A$ by definition of B. From assumption **(b)** of this theorem we obtain $a + 1 \in A$ and thus $b + 1 = (a + 1) - k_0 + 1 \in B$ by definition of B. This proves step **(2)**.

We have proven for the set B that $1 \in B$ and that this set contains with each element b also the integer $b + 1$. It follows from the induction axiom that $B \supseteq \mathbb{N}$. This proves step **(3)**.

It follows from $B \supseteq \mathbb{N}$ that $(k_0 - 1) + B \supseteq (k_0 - 1) + \mathbb{N}$, i.e., $A \supseteq [k_0, \infty[_{\mathbb{Z}} = A_{k_0}$. $\blacksquare$

The generalized induction axiom allows us to give a proof for the **principle of mathematical induction** which was introduced in rem.**??** (p.**??**) of ch.**??**.

Theorem 6.2 (Principle of Mathematical Induction)**.**

Assume that for each integer $k \geq k_0$ there is an associated statement $P(k)$ such that

A. Base case. *The statement $P(k_0)$ is true.*

B. Induction Step. *For each $k \geq k_0$ we have the following: Assuming that $P(k)$ is true ("**Induction Assumption**"), it can be shown that $P(k + 1)$ also is true.*

*It then follows that $P(k)$ is true for **each** $k \geq k_0$.*

PROOF: Let $A_{k_0} := \{k \in \mathbb{Z} : j \geq k_0\}$, and let $A := \{k \in A_{k_0} : P(k) \text{ is true }\}$. It follows from **A** that $k_0 \in A$, and it follows from **B** that if $k \in A$ then $k+1 \in A$. We conclude from thm.6.1 above that $A_{k_0} \subseteq A$. Thus $P(k)$ is true for all $k \in A_{k_0}$. ■

Remark 6.3.
The above theorem 6.2 is often stated for the special case $k_0 = 1$. [1]

We remind the reader that several examples for proofs by induction were given in ch.**??**.

Theorem 6.3 (Principle of Strong Mathematical Induction)**.**

Let $k_0 \in \mathbb{Z}$ and assume that for each integer $k \geq k_0$ there is an associated statement $P(k)$ such that the following is valid:

A. Base case.	*The statement $P(k_0)$ is true.*
B. Induction Step.	*For each $k \geq k_0$ we have the following: Assuming that $P(j)$ is true for all $j \in \mathbb{Z}$ such that $k_0 \leq j \leq k$ ("**Induction Assumption**"), it can be shown that $P(k+1)$ also is true.*

*It then follows that $P(k)$ is true for **each** $k \geq k_0$.*

PROOF: Let

$$A_{k_0} := \{k \in \mathbb{Z} : j \geq k_0\}; \quad A := \{k \in A_{k_0} : P(j) \text{ is true for all } j \in [k_0, k]_{\mathbb{Z}}\}.$$

It follows from **A** that $k_0 \in A$, and it follows from **B** that if $k \in A$, i.e., $P(j)$ is true for all $k_0 \leq j \leq k$, then also $P(k+1)$ is true, hence $P(j)$ is true for all $k_0 \leq j \leq k+1$, i.e., $k+1 \in A$. We conclude from thm.6.1 on p.205 that $A_{k_0} \subseteq A$. Thus $P(k)$ is true for all $k \in A_{k_0}$. ■

The following is an example for a proof that is best done with strong induction.

Example 6.1. [2] Let $(x_n)_{n\in\mathbb{N}}$ be the sequence $x_1 := 2,\ x_2 := 8,\ x_n := 4(x_{n-1} - x_{n-2})$ $(n \geq 3)$. Prove that $x_n = n2^n$ for all $n \in \mathbb{N}$.

Solution strategy: This is a two-step recursion: To know the value of the sequence at "time" k we must know x_n for both $n = k-1$ and $n = k-2$. We need strong induction rather than ordinary induction on n, and we must "anchor" the proof with two base cases: $n = 2$ and $n = 1$ so that we can bootstrap ourselves and conclude the validity of $x_n = n2^n$ for $n = 3$ from that of the base cases and the recursion formula $x_n := 4(x_{n-1} - x_{n-2})$.

SOLUTION (by strong induction on n):

Base cases:

$n = 1 \ \Rightarrow\ n2^n = 1 \cdot 2^1 = 2 = x_1,$

$n = 2 \ \Rightarrow\ n2^n = 2 \cdot 2^2 = 8 = x_2.$

[1] [1] Beck/Geoghegan refers to the case $k_0 = 1$ as the Principle of mathematical induction — first form and to the general case as the Principle of mathematical induction — first form revisited.

[2] This is example 3.40 of D'Angelo and West [2].

Induction step:

Induction assumption: We have some $n \in \mathbb{N}$ such that $x_j = j2^j$ for all $j \leq n$. $(\star)$

We **must show under this assumption** that $x_{n+1} = (n+1)2^{n+1}$. $(\star\star)$

$$\begin{aligned} x_{n+1} &= 4(x_n - x_{n-1}) && \text{(recursion formula for } x_n\text{)} \\ &= 4\big(n2^n - (n-1)2^{n-1}\big) && \text{(induction assumption } (\star)\text{)} \\ &= 2n2^{n+1} - (n-1)2^{n+1}\big) \\ &= (2n - n + 1)2^{n+1} \\ &= (n+1)2^{n+1}. \end{aligned}$$

We have shown the validity of $(\star\star)$, and this completes the proof by strong induction. □

Here is another example for a proof by strong induction.

Example 6.2. Example [3] Let $(x_n)_{n\in\mathbb{N}}$ be the following sequence of real numbers: $x_1 := x_2 := 1$, $x_n := \frac{1}{2}(x_{n-1} + 2/x_{n-2})$ $(n \geq 3)$. Prove that $1 \leq x_n \leq 2$ for all $n \in \mathbb{N}$.

SOLUTION (by strong induction on n):

Base cases:

We need both $n = 1$ and $n = 2$ as base cases for the same reason as in example 6.1. Their validity is obvious from $x_1 = x_2 = 1$, since then $1 \leq x_1 \leq 2$ and $1 \leq x_2 \leq 2$.

Induction step:

Induction assumption: We have some $n \in \mathbb{N}$ such that $1 \leq x_j \leq 2$ for all $j \leq n$. $(\star)$

We **must show under this assumption** that $1 \leq x_{n+1} \leq 2$. $(\star\star)$ for all $(n \geq 3)$.

It follows from $(\star)$ that

(i) $x_n \leq 2$, hence $\frac{1}{2}x_n \leq \frac{1}{2} \cdot 2 = 1$,

(ii) $x_{n-1} \geq 1$, hence $\frac{1}{2} \cdot \frac{2}{x_{n-1}} = \frac{1}{x_{n-1}} \leq 1$.

It follows from the recursion formula $x_n = \frac{1}{2}(x_{n-1} + 2/x_{n-2})$ that $x_n \leq 1 + 1 = 2$ for $(n \geq 3)$.

It also follows from $(\star)$ that

(iii) $x_n \geq 1$, hence $\frac{1}{2}x_n \geq \frac{1}{2}$,

(iv) $x_{n-1} \leq 2$, hence $\frac{1}{2} \cdot \frac{2}{x_{n-1}} = \frac{1}{x_{n-1}} \geq \frac{1}{2}$.

It follows from $x_n := \frac{1}{2}(x_{n-1} + 2/x_{n-2})$ that $x_n \geq \frac{1}{2} + \frac{1}{2} = 1$ for $(n \geq 3)$.

We have shown the validity of $(\star\star)$, and this completes the proof by strong induction. □

Remark 6.4.

How do thm.6.2 and thm.6.3 compare? The base case "P_{k_0} is true" is the same for both, and so is the conclusion "P_{k+1} is true". The difference is in the induction assumptions. Strong induction allows you to assume a lot more (the validity of P_j for **a]]** $j \leq k$) than ordinary induction where you only may assume the validity of P_k. □

[3] This is exercise 3.57 of D'Angelo and West [2].

6.2 The Discrete Structure of the Integers

In the previous section the induction principles were derived from the induction axiom and they are very powerful tools for the design of a proof. Accordingly, you encounter such proofs quite frequently. The induction axiom itself is used rather seldom in comparison, but the next theorem is a nice example where this is the case.

Theorem 6.4 (B/G Prop.2.20)**.**

If $k \in \mathbb{N}$, then

(6.1) $$k \geq 1.$$

PROOF:

Let $A := \{n \in \mathbb{N} : n \geq 1$. It suffices to show that $A \supseteq \mathbb{N}$.

(a) Clearly, $1 \geq 1$. Hence, $1 \in A$.

(b) Next, let $a \in A$. Then $a \geq 1$. Hence, $a + 1 \geq 1 + 1 > 1$ (use Proposition **??** on p.**??**).

(c) Thus, $a + 1 \geq 1$ and thus, $a + 1 \in A$.

We have shown in **(a)** and **(c)** that $1 \in A$ and also, that $\in A \Rightarrow a + 1 \in A$. It follows from the induction axiom that $A \supseteq \mathbb{N}$ ■

Proposition 6.2 (B/G Prop.2.21)**.**

There exists no $x \in \mathbb{Z}$ such that $0 < x < 1$.

The proof is left as exercise 6.12 (see p.252). ■

Corollary 6.2 (B/G Cor.2.22)**.**

Let $n \in \mathbb{Z}$. There exists no $x \in \mathbb{Z}$ such that $n < x < n + 1$.

The proof is left as exercise 6.13 (see p.252). ■

Proposition 6.3 (sharpening of B/G Prop.2.13)**.** $\mathbb{N} = \{k \in \mathbb{Z} : k \geq 1\}$.

PROOF: This follows from $1 > 0$ (cor.**??** on p.**??**) and prop.6.2 above. ■

It follows from the last proposition that $\mathbb{N} = [1, \infty[$ and thus $\min(\mathbb{N}) = 1$. We will see in subchapter 6.8 (The Well–Ordering Principle) on p.232 that this is a special case of the following: All nonempty subsets of $\mathbb{N}$ possess a minimum.

6.3 Divisibility

For any two real numbers a and b such that $b \neq 0$ one can construct the quotient $\frac{a}{b}$, and the result is again a real number. The same situation exists for fractions. In contrast there are integers m, $n \neq 0$ for which the quotient $\frac{m}{n}$ is not an integer, e.g., if $m = 12$ and $n = 5$. One says in this case that m is not divisible by n. Questions of divisibility are of great interest in the mathematical discipline of number theory, and we will examine divisibility at various times.

Definition 6.2 (Divisibility)**.**

(a) Let $m, n \in \mathbb{Z}$. We say that n **divides** m or, equivalently, that m **is divisible by** n if there exists $j \in \mathbb{Z}$ such that $m = jn$. We then write $n \mid m$, and we write $n \nmid m$ if n does not divide m, i.e., there is no $k \in \mathbb{Z}$ that satisfies $m = kn$.

(b) Let $m \in \mathbb{Z}$. We say that m is an **even** integer if $2 \mid m$. We say that m is an **odd** integer if m is not even, i.e., $2 \nmid m$. □

Proposition 6.4.

Let $m, n \in \mathbb{Z}$ such that $m \neq 0$ and $m \mid n$, i.e., there exists $j \in \mathbb{Z}$ be such that $n = j \cdot m$. Then j is uniquely determined.

PROOF: Assume that there is $j' \in \mathbb{Z}$ such that also $n = j' \cdot m$. Then

$$n \;=\; j' \cdot m \;=\; j \cdot m, \quad \text{hence } (j' - j)m \;=\; 0.$$

The integral domain $\mathbb{Z}$ has no zero divisors, hence $a \cdot b = 0$ implies $a = 0$ or $b = 0$.
It follows from $m \neq 0$ that $j' - j = 0$ and hence $j' = j$. ■

The above result implies that the integer j is unique determined by m and n and hence allows us to make the following definition.

Definition 6.3 (Quotients)**.**

Let $d, n \in \mathbb{Z}$ such that $d \mid n$ and $d, n \neq 0$.
Let $q \in \mathbb{Z}$ be the unique integer for which $n = q \cdot d$. We write either of

$$\frac{n}{d}, \quad n/d, \quad n \div d \quad \text{instead of } q\,,$$

and we call n the **dividend** or **numerator**, d the **divisor** or **denominator**, and q the **quotient** of the expression n/d. We also define $\frac{0}{d} := 0$ if $d \neq 0$, but we leave $\frac{n}{0}$ undefined for all $n \in \mathbb{Z}$. □

Remark 6.5.

Note that the assignment $(d, n) \mapsto n/d$ is **not a "binary operation"** on $\mathbb{Z}$ as is the case for $(m, n) \mapsto m + n$ and $(m, n) \mapsto m \cdot n$. The reason: $m + n$ and $m \cdot n$ are defined for **any** two $m, n \in \mathbb{Z}$ whereas n/d is only defined for those $d, n \in \mathbb{Z}$ which satisfy the condition $d \mid n$.

Also note that the order of n and d is reversed in the expressions n/d and $d \mid n$. □

Proposition 6.5 (B/G prop.1.16)**.**

If m and n are even integers, then so are $m + n$ and mn.

PROOF: Left as an exercise. ■

Proposition 6.6 (B/G prop.1.17)**.**

(a) *If m is an integer then $m \mid 0$. In particular, $0 \mid 0$.*
(b) *If m is a nonzero integer then $0 \nmid m$.*

PROOF: Left as an exercise. ■

Proposition 6.7 (B/G prop.2.18)**.**

Let $n \in \mathbb{N}$. Then
(a) *$n^3 + 2n$ is divisible by 3,*
(b) *$n^4 - 6n^3 + 11n^2 - 6n$ is divisible by 4,*
(c) *$n^2 + n$ is even, i.e., divisible by 2,*
(d) *$n^3 + 5n$ is divisible by 6.*

PROOF of **(a)**: See [1] B/G (Beck/Geoghegan), prop.2.18(i).

PROOF of **(b)**, **(c)**, **(d)**: Left as an excercise. Note that **(c)** will be helpful for the proof of **(d)**. ■

The following example shows how to structure a proof by induction of divisibility. Note that it makes use of Proposition 6.7**(c)**.

Example 6.3 (Divisibility)**.**

Prove by induction that $6 \mid (5n^3 + 7n)$ for $n \in [0, \infty[_{\mathbb{Z}}$.

PROOF:

We need to find $j \in \mathbb{Z}$ such that $5n^3 + 7n = 6j$.

Base case: $n = 0$.

Then $5n^3 + 7n = 0 + 0 = 0 = 0 \cdot 1$. The base case holds since we may choose $j = 0$.

Induction assumption: Assume that $n \in [0, \infty[_{\mathbb{Z}}$ is such that there exists $j \in \mathbb{Z}$ such that

(**IA**) $$5n^3 + 7n = 6j\,.$$

We need to show that

(**NTS**) there exists $j' \in \mathbb{Z}$ such that $5(n+1)^3 + 7(n+1) = 6j'$.

We transform the left side of that equation as follows:

$$\begin{aligned} 5(n+1)^3 + 7(n+1) &= (5n^3 + 15n^2 + 15n + 5) + 7n + 7 \\ &= (5n^3 + 7n) + (15n^2 + 15n + 5) + 7 \\ &= (5n^3 + 7n) + 15(n^2 + n) + 12\,. \end{aligned}$$

According to Proposition 6.7**(c)**, $n^2 + n$ is even and thus equals $2j''$ for a suitable integer j''. We further apply **(IA)** and obtain

$$5(n+1)^3 + 7(n+1) = (6j) + 15(2j'') + 12 = 6(j + 5j'' + 2)\,.$$

Let $j' := j + 5j'' + 2$. Then **(NTS)** is satisfied and the proof by induction is finished ■

Proposition 6.8 (B/G Prop.2.24)**.**

Let $n \in \mathbb{N}$. Then $n^2 + 1 > n$.

PROOF: The proof is left as exercise 6.14 (see p.253). ■

Proposition 6.9 (B/G prop.2.23)**.**

Let $m, n \in \mathbb{N}$. If $m \mid n$ then $m \leq n$

The proof is left as exercise 6.11 (see p.252). ■

6.4 Embedding the Integers Into an Ordered Integral Domain

The presentation of this material follows ch.9 of [1] B/G (Beck/Geoghegan).

Introduction 6.1. Allowing integers to be viewed as certain elements of an ordered integral domain $R = (R, \oplus, \odot, P)$ makes it possible to look at products na of integers n and $a \in R$.

In particular we can multiply binomial coefficients $\binom{n}{k}$ with elements of R and thus formulate and prove the binomial theorem

$$(a \oplus b)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

for elements a and b of such an arbitrary ordered integral domain.

We will "embed" the ordered integral domain $\mathbb{Z} = (\mathbb{Z}, +, \cdot, \mathbb{N})$ into the ordered integral domain $R = (R, \oplus, \odot, P)$ by means of a function $e : \mathbb{Z} \to R$ which respects their algebraic operations (addition and multiplication) and also the order relation induced by their positive cones in a sense which is specified in theorem 6.5 further down (p.216). □

We assume in the following that $R = (R, \oplus, \odot, P)$ is a fixed ordered integral domain.

We distinguish the additive units of the domain $\mathbb{Z}$ and the codomain R by tagging them as $0_{\mathbb{Z}}$ and 0_R, and we distinguish their multiplicatitive units by tagging them as $1_{\mathbb{Z}}$ and 1_R.

We also distinguish order relations $x < y, x \leq y, ...$ by writing $m < n, m \leq n, \ldots$ when dealing with elements $m, n \in \mathbb{Z}$. Lastly, we write $a \prec b, a \preceq b, \ldots$ for $a, b \in R$.

We will see examples for the above notational conventions in the following definition.

Definition 6.4 (Natural Embedding of the Integers Into $(R, \oplus, \odot, P)$)**.**

⋆

We define a function $e : \mathbb{Z} \to R$, partially by recursion, as follows.

$$e(0_{\mathbb{Z}}) \;:=\; 0_R\,, \tag{6.2}$$

$$e(n + 1_{\mathbb{Z}}) \;:=\; e(n) \oplus 1_R \quad \text{for } n \in [0, \infty[_{\mathbb{Z}}\,, \tag{6.3}$$

$$e(n) \;:=\; \ominus\, e(-n) \quad \text{for } n \in \,]-\infty, -1\,]_{\mathbb{Z}}\,. \tag{6.4}$$

We call e the **natural embedding of $\mathbb{Z}$ into** $(R, \oplus, \odot, P)$. □

We establish some properties of the natural embedding.

Lemma 6.1.

$$e(1_{\mathbb{Z}}) \;=\; 1_R, \tag{6.5a}$$

$$e(-k) \;=\; \ominus\, e(k) \quad \textit{for any } k \in \mathbb{Z}. \tag{6.5b}$$

PROOF of (6.5a):

$$e(1_{\mathbb{Z}}) \ = e(0_{\mathbb{Z}} + 1_{\mathbb{Z}}) \overset{(6.3)}{=} e(0_R) \oplus 1_R \overset{(6.2)}{=} 1_R.$$

PROOF (6.5b): (6.5b) is obviously true if $k = 0$. If $k < 0$ then this equation follows from (6.4), and if $k > 0$ then we also obtain it from (6.4) since then $-k < 0$, thus

$$e(-k) \ = \ominus e\big(-(-k)\big) \ = \ \ominus e(k). \ \blacksquare$$

Note that (6.5a) expresses that the image of the multiplicatve unit in $\mathbb{Z}$ is the multiplicative unit in R, and (6.5b) expresses that the image of the additive inverse is the additive inverse of the image.

We now show that the natural embedding e is compatible with the algebraic operations "$+$" of $\mathbb{Z}$ and "$\oplus$" of R in the sense that the image of the sum is the sum of the images.

Proposition 6.10. *Let $m, n \in \mathbb{Z}$. Then $e(m+n) \ = \ e(m) \oplus e(n)$.*

Proof strategy: We will do a proof by cases:

Case 1: $m = 0_{\mathbb{Z}}$ or $n = 0_{\mathbb{Z}}$,
Case 2: $m > 0_{\mathbb{Z}}$ and $n > 0_{\mathbb{Z}}$,
Case 3: $m < 0_{\mathbb{Z}}$ and $n < 0_{\mathbb{Z}}$.

The remaining case that either $m > 0_{\mathbb{Z}}, n < 0_{\mathbb{Z}}$ or $n > 0_{\mathbb{Z}}, m < 0_{\mathbb{Z}}$ only needs to be shown for one of those two possibilities, say, $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$. We subdivide this case into two separate cases as follows:

Case 4: $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$ and $n \geq -m$,
Case 5: $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$ and $n < -m$.

Only the second case needs a proof by induction.

PROOF of **case 1**: $m = 0_{\mathbb{Z}}$ or $n = 0_{\mathbb{Z}}$: This is trivial since if, say, $n = 0_{\mathbb{Z}}$ then

$$e(m+n) \ = e(m) \ \overset{(6.2)}{=} \ e(m) \oplus e(0_R) \ = \ e(m) \oplus e(n).$$

PROOF of **case 2**: $m > 0_{\mathbb{Z}}$ and $n > 0_{\mathbb{Z}}$:

We consider $m > 0$ as fixed but arbitrary and do the proof by induction on n.

Base case: $n = 1_{\mathbb{Z}}$. The assertion $e(m + 1_{\mathbb{Z}}) \ = \ e(m) \oplus 1_R$ is just (6.3).

Induction assumption (IA): Assume that $e(m+n) \ = \ e(m) \oplus e(n)$ for some $n \in \mathbb{N}$.

We must show that $e\big(m + (n + 1_{\mathbb{Z}})\big) \ = \ e(m) \oplus e(n + 1_{\mathbb{Z}})$. This follows from

$$\begin{aligned} e\big(m + (n + 1_{\mathbb{Z}})\big) \ &= \ e\big((m+n) + 1_{\mathbb{Z}}\big) \overset{(6.3)}{=} \ e(m+n) \oplus 1_R \\ &\overset{\text{(IA)}}{=} \ e(m) \oplus \big(e(n) \ \oplus 1_R\big) \overset{(6.3)}{=} \ e(m) \oplus e(n + 1_{\mathbb{Z}}). \end{aligned}$$

PROOF of **case 3**: $m < 0_{\mathbb{Z}}$ and $n < 0_{\mathbb{Z}}$:

Since $-m > 0$ and $-n > 0$ we may apply what we already proved in case 2 above:

$$\begin{aligned} e(m+n) \ &\overset{(6.4)}{=} \ \ominus e\big(-(m+n)\big) \ = \ \ominus e\big((-m) + (-n)\big) \\ &= \ \ominus \big(e(-m) \oplus e(-n)\big) \ = \ \big(\ominus e(-m)\big) \oplus \big(\ominus e(-n)\big) \overset{(6.4)}{=} \ e(m) \oplus e(n). \end{aligned}$$

PROOF of **case 4**: $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$ and $n \geq -m$.

It follows from the assumptions of this case that $n = (n+m) + (-m)$ is the sum of the natural numbers $n+m$ and $-m$. We apply what we proved in case 2 and obtain

$$e(n) \;=\; e(n+m) \oplus e(-m) \overset{(6.5b)}{=} e(n+m) \ominus e(m),$$

thus $e(m+n) = e(m) \oplus e(n)$.

PROOF of **case 5**: $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$ and $n < -m$:

It follows from the assumptions of this case that $-m = -(m+n) + n$ is the sum of the natural numbers $-(n+m)$ and n. We apply what we proved in case 2 and obtain with repeated use of (6.5b) that

$$\ominus\, e(m) \;=\; e(-m) \;=\; e\big(-(m+n)+n\big) \;=\; e\big(-(m+n)\big) \oplus e(n) \;=\; \ominus\, e(m+n) \oplus e(n),$$

thus $e(m+n) = e(m) \oplus e(n)$. ■

We will prove next that the natural embedding e also is compatible with the algebraic operations "$\cdot$" of $\mathbb{Z}$ and "$\odot$" of R in the sense that the image of the product is the product of the images.

Proposition 6.11. *Let $m, n \in \mathbb{Z}$. Then $e(m \cdot n) \;=\; e(m) \odot e(n)$.*

Proof strategy: We do a proof by cases just as we did for prop.6.10, but we only need four cases:

Case 1: $m = 0_{\mathbb{Z}}$ or $n = 0_{\mathbb{Z}}$.
Case 2: $m > 0_{\mathbb{Z}}$ and $n > 0_{\mathbb{Z}}$.
Case 3: $m < 0_{\mathbb{Z}}$ and $n < 0_{\mathbb{Z}}$.

The remaining case that either $m > 0_{\mathbb{Z}}, n < 0_{\mathbb{Z}}$ or $n > 0_{\mathbb{Z}}, m < 0_{\mathbb{Z}}$ only needs to be shown for one of those two, say, $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$ since multiplication is commutative and we obtain the proof for the other case by switching the roles of m and n. Thus we are left with

Case 4: $m < 0_{\mathbb{Z}}$ and $n > 0_{\mathbb{Z}}$.

Only the second case needs a proof by induction.

PROOF of **case 1**: $m = 0_{\mathbb{Z}}$ or $n = 0_{\mathbb{Z}}$: This is trivial since if, say, $m = 0_{\mathbb{Z}}$ then

$$e(m \cdot n) \;= e(0_{\mathbb{Z}}) \overset{(6.2)}{=} 0_R \;=\; e(m) \odot 0_R \overset{(6.2)}{=} e(m) \odot e(0_{\mathbb{Z}}).$$

PROOF of **case 2**: $m > 0_{\mathbb{Z}}$ and $n > 0_{\mathbb{Z}}$:

We consider $m > 0$ as fixed but arbitrary and do the proof by induction on n.

Base case: $n = 1_{\mathbb{Z}}$. The assertion $e(m \cdot 1_{\mathbb{Z}}) \;=\; e(m) \odot e(1_{\mathbb{Z}})$ follows from (6.5b).

Induction assumption (IA): Assume that $e(m \cdot n) \;=\; e(m) \odot e(n)$ for some $n \in \mathbb{N}$.

We must show that $e\big(m \cdot (n + 1_{\mathbb{Z}})\big) \;=\; e(m) \odot e(n + 1_{\mathbb{Z}})$. This follows from

$$\begin{aligned} e\big(m(n+1_{\mathbb{Z}})\big) \;=\; e(mn+m) &\overset{\text{prop.6.10}}{=} e(mn) \oplus e(m) \\ &\overset{\text{(IA)}}{=} \big(e(m) \odot e(n)\big) \;\oplus\; e(m) \;=\; e(m)(e(n) \oplus 1_R) \overset{(6.3)}{=} e(m) \odot e(n+1_{\mathbb{Z}}). \end{aligned}$$

PROOF of **case 3**: $m < 0_{\mathbb{Z}}$ and $n < 0_{\mathbb{Z}}$:

Since $-m > 0$ and $-n > 0$ we may apply what we already proved in case 2 above:

$$e(m \cdot n) \;=\; e\big((-m)(-n)\big) \;=\; e(-m) \odot e(-n) \overset{(6.5b)}{=} \big(\ominus e(m)\big) \cdot \big(\ominus e(n)\big) \;=\; e(m) \odot e(n).$$

PROOF of **case 4**: $n > 0_{\mathbb{Z}}$ and $m < 0_{\mathbb{Z}}$: We again apply what we proved in case 2 to the natural numbers $-m$ and n and obtain with the use of (6.5b) that

$$\ominus e(mn) \;=\; e(-mn) \;=\; e\big((-m)n\big) \;=\; e(-m) \odot e(n) \;=\; \ominus e(m) \odot e(n),$$

thus $e(mn) = e(m) \odot e(n)$. ■

We now turn to the relationship which the natural embedding e establishes between the order relation $m < n$ on $\mathbb{Z}$ (induced by its positive cone $\mathbb{N}$) on the one hand, and the order relation $a < b$ on R (induced by its positive cone P) on the other hand.

Proposition 6.12 (B/G Prop.9.15)**.** *Let $n \in \mathbb{N}$. Then $e(n) \in P$, i.e., $e(n)$ is positive.*

The proof is left as exercise 6.2 (see p.251). ■

The natural embedding e is order preserving both ways in the sense specified in the next proposition.

Proposition 6.13 (B/G Prop.9.19)**.**
Let $m, n \in \mathbb{Z}$. Then

$$m < n \;\Leftrightarrow e(m) \prec e(n)\,, \tag{6.6}$$

$$m \leq n \;\Leftrightarrow e(m) \preceq e(n)\,. \tag{6.7}$$

PROOF of $\Rightarrow$ of (6.7):
Let us assume that $e(m) \preceq e(n)$. We must show that $m \leq n$.
Case 1 – $e(m) \prec e(n)$: then $m < n$ according to the already proven part (6.7), thus $m \leq n$.
Case 2 – $e(m) = e(n)$: We prove that $m = n$, hence $m \leq n$ by showing that both $m < n$ and $n < m$ lead to a contradiction.
If $m < n$ then $n - m \in \mathbb{N}$, thus $e(n) \ominus e(m) = e(n - m) \in P$ according to Proposition 6.12, i.e., $e(n) \ominus e(m) \in P$ since $e(n) \ominus e(m) = e(n - m)$ according to Proposition 6.10 on p.213.
It follows from $0_R \notin P$ that $e(m) \ominus e(n) \neq 0_R$, i.e., $e(m) \neq e(n)$. This contradicts the assumption $e(m) = e(n)$ we made at the beginning of this case 2.
We have shown that it is not possible that $m < n$, i.e., that $m \geq n$. The proof that $n \geq n$ is obtained by switching the roles of m and n in the above reasoning.
We have completed the proof of **case 2** of $\Rightarrow$ of (6.7) and thus the proof of the entire proposition. ■

Corollary 6.3. *The natural embedding $e : \mathbb{Z} \to R$ is injective.*

PROOF:

The proof was already done as part of **case 2** of $\Rightarrow$ of **(B)** of Proposition 6.13 where we saw that equality $e(m) = e(n)$ of function values implies that of the arguments m and n. This is the very definition of injectivity. We give here a streamlined proof that builds on Proposition 6.13.

Let $m, n \in \mathbb{Z}$ such that $m \neq n$. Then either $m < n$ or $m > n$. In the first case it follows from prop.6.13 that $e(m) \prec e(n)$ and thus $e(m) \neq e(n)$, in the second case it follows from **(A)** of prop.6.13 that $e(m) \succ e(n)$ and thus $e(m) \neq e(n)$. ■

We summarize everything said in this subchapter in the following theorem.

Theorem 6.5.

Let $R = (R, \oplus, \odot, P)$ be an ordered integral domain.
The natural embedding $e : (\mathbb{Z}, +, \cdot, \mathbb{N}) \longrightarrow (R, \oplus, \odot, P)$ which is defined as follows:

$$e(0_{\mathbb{Z}}) \;=\; 0_R, \quad e(n + 1_{\mathbb{Z}}) \;=\; e(n) \oplus 1_R \;\; \text{if } n \in \mathbb{N}, \quad e(n) \;=\; \ominus e(-n) \;\; \text{if } n < 0$$

is an injective function with the following structure preserving properties ($m, n \in \mathbb{Z}$):

- ***(a)*** *e maps neutral element to neutral element: $e(0_{\mathbb{Z}}) = 0_R$ and $e(1_{\mathbb{Z}}) = 1_R$.*
- ***(b)*** *Image of the sum = sum of the images: $e(m + n) = e(m) \oplus e(n)$.*
- ***(c)*** *Image of the product = product of the images: $\Rightarrow\; e(m \cdot n) = e(m) \odot e(n)$.*
- ***(d)*** *Image of the additive inverse = additive inverse of the image: $e(-m) = \ominus e(m)$.*
- ***(e)*** *e preserves the order: $m < n \;\Leftrightarrow\; e(m) \prec e(n)$ and $m \leq n \;\Leftrightarrow\; e(m) \preceq e(n)$.*

PROOF: follows from the material presented prior to this theorem. ■

Remark 6.6.

The function e does such nice job of embedding, i.e., injecting the integers into R that it is justified to "identify" the integers with their images in R. One thus does not distinguish between $n \in \mathbb{Z}$ and $e(n) \in R$. □

Functions which prefer algebraic structures play a very important role in abstract algebra, where they are called **homomorphisms**. The group homomorphisms we briefly discussed in Chapter **??** (The Axiomatic Method) are an example of such homomorphisms. Note that **(b)**, **(d)** and the formula $e(0_{\mathbb{Z}}) = 0_R$ in **(a)** of Theorem 6.5 imply that the natural embedding is a group homomorphism $(\mathbb{Z}, +) \to (R, \oplus)$.

Definition 6.5 (Ring homomorphism)**.**

⋆

A function $h : (R, \oplus, \odot) \longrightarrow (R', \oplus', \odot')$ between two commutative rings with unit and in particular between two ordered integral domains [4] which satisfies Theorem6.5.**a**–**d** is called a **ring homomorphism**.

Note that ring homomorphisms play for commutative rings with unit the role which group homomorphisms play for groups. □

Theorem 6.6.

Let $R = (R, \oplus, \odot, P)$ be an ordered integral domain which satisfies the induction axiom. See Axiom 6.1 (Integers and Natural Numbers) on p.203.

*Then the natural embedding $e : (\mathbb{Z}, +, \cdot, \mathbb{N}) \longrightarrow (R, \oplus, \odot, P)$ is an isomorphism of ordered integral domains, i.e., e is bijective and it's inverse, e^{-1}, also satisfies **(a)**–**(e)** of Theorem 6.5.*

PROOF:

Let $A := P \cap e(\mathbb{Z})$

Step **(1)** We show that $A = P$.

Since $1_R = e(1)$ and $1_R > 0$, $1_R \in A$.

Next, let $p \in A$. Since $p \in e(\mathbb{Z})$, there is some $k \in \mathbb{Z}$ such that $p = e(k)$. Then

$$a \oplus 1_R \;=\; e(k) \oplus e(1) \;=\; e(k+1)\,.$$

Thus, $a \oplus 1_R \in e(\mathbb{Z})$. Further, $a \in P$ implies $a \oplus 1_R \in P$.

We have shown that A satisfies the induction axiom and it follows that $A \supseteq P$. By definition, $A \subseteq P$. It follows that $A = P$.

Step **(2)** We show that $-P \subseteq e(\mathbb{Z})$.

Let $x \in \ominus P$ and $a := \ominus x$. Then $a \in P = A$. Thus, there exists $k \in \mathbb{Z}$ such that $= e(k)$. Further, $e(-k) = \ominus a = b$. Thus, $\ominus P \subseteq e(\mathbb{Z})$.

Step **(3)** We show that $R \subseteq e(\mathbb{Z})$.

Since $0_R = e(0) \in e(\mathbb{Z})$, it follows from steps **(1)** and **(2)** that $\{0_R\} \uplus (P) \uplus (-P) \subseteq e(\mathbb{Z})$. As an ordered integral domain, R satisfies $R = \{0_R\} \uplus (P) \uplus (-P)$.

We have shown that e is surjective, hence, bijective.

Step **(3)** We show that e^{-1}, also satisfies **(a)**–**(e)** of Theorem 6.5.

(a) We apply e^{-1} to $e(0_{\mathbb{Z}}) = 0_R$ and $e(1_{\mathbb{Z}}) = 1_R$ and obtain $0_{\mathbb{Z}} = e^{-1}(0_R)$ and $1_{\mathbb{Z}} = e^{-1}(1_R)$.

(b) follows from Theorem **??** on p.**??**.

(c) is obtained by applying the proof of Theorem **??** to "$\odot$" instead of "$\oplus$".

(d) We show that $e^{-1}(\ominus a) = -e^{-1}(a)$ as follows.

Let $a \in R$ and $n := e^{-1}(a)$, i.e., $a = e(n)$. Then

$$e^{-1}(\ominus a) \;=\; e^{-1}\big(\ominus e(n)\big) \;\overset{(6.5b)}{=}\; e^{-1}\big(e(-n)\big) \;=\; -n \;=\; -e^{-1}(a)\,.$$

(e) That e^{-1} preserves both "$\prec$" and "$\preceq$" follows from Theorem6.5.**e** by setting

$$m := e^{-1}(a) \quad \text{and} \quad n := e^{-1}(b) \quad \text{for arbitrary } a, b \in R,$$

and noting that the "$\Leftrightarrow$" arrows allow us to go back and forth between $\mathbb{Z}$ and R. ■

6.5 Recursive Definitions of Sums, Products and Powers in Integral Domains

We start this chapter with the generalizations of some definitions and several of the propositions that you will find in ch.4 of [1] Beck/Geoghegan Art of Proof for the specific ordered integral domain

$(\mathbb{Z}, +, \cdot, \mathbb{N})$ and the specific "start index $j = 1$. Except for those generalizations almost all of the material in this subchapter has been copied almost literally from that book.

Assume in this entire chapter that $R = (R, \oplus, \odot, P)$ is an ordered integral domain

The following definition is a generalization of "Σ" in B/G p.34, 35.

Definition 6.6.

Let $k \in \mathbb{Z}$ and let $(x_j)_{j=k}^{\infty} \in R$. For each $n \in \mathbb{Z}$ such that $k \leq n$, we define an element of R, denoted $\sum_{j=k}^{n} x_j$ or $x_k \oplus x_{k+1} \oplus \cdots \oplus x_n$, as follows.

(6.8) (i) $\sum_{j=k}^{k} x_j = x_k$, (ii) $\sum_{j=k}^{n+1} x_j = \sum_{j=k}^{n} x_j \oplus x_{n+1}$.

We call $\sum_{j=k}^{n} x_j$ the **sum** of $x_k, x_{k+1}, \ldots, x_{n-1}, x_n$. □

The following definition is a generalization of "$\prod$" (B/G p.34, 35).

Definition 6.7 (Definition of $\prod_{j=k}^{n} x_j$)**.**

Let $k \in \mathbb{Z}$ and let $(x_j)_{j=k}^{\infty} \in R$. For each $n \in \mathbb{Z}$ such that $k \leq n$, we define an element of R, denoted $\prod_{j=k}^{n} x_j$ or $x_k \odot x_{k+1} \cdots \odot x_n$, as follows.

(6.9) (i) $\prod_{j=k}^{k} x_j = x_k$, (ii) $\prod_{j=k}^{n+1} x_j = \prod_{j=k}^{n} x_j \odot x_{n+1}$.

We call $\prod_{j=k}^{n} x_j$ the **product** of $x_k, x_{k+1}, \ldots, x_{n-1}, x_n$. □

Note that in the following proposition we make use of the results of ch.6.4 (Embedding the Integers Into an Ordered Integral Domain). It was shown there that we can identify integers k as certain elements $e(k)$ of R by means of the embedding function $e : \mathbb{Z} \to R$. For example the equation $\sum_{j=k}^{n} x_j = n \ominus k \oplus 1$ in part **(b)** of Proposition 6.14 below is to be understood as $\sum_{j=k}^{n} x_j = e(n-k+1)$, an equation between elements of R.

Proposition 6.14 (B/G prop.4.15)**.**

Let $m, n, k \in \mathbb{Z}$, $c \in R$, and let $(x_j)_{j=k}^{\infty}$ be a sequence in R. Then

(a) $c \odot \left(\sum_{j=k}^{n} x_j \right) = \sum_{j=k}^{n} (c \odot x_j)$.

(b) *If $x_j = 1$ for all $j \in [k, n]_{\mathbb{Z}}$ then* $\sum_{j=k}^{n} x_j = (n \ominus k) \oplus 1$.

(c) *If $x_j = c$ for all $j \in [k, n]_{\mathbb{Z}}$ then* $\sum_{j=k}^{n} x_j = \big((n \ominus k) \oplus 1\big) \odot c$.

PROOF: Left as an exercise. ■

Proposition 6.15 (B/G prop.4.16)**.**

Let $m, n, p \in \mathbb{Z}$ such that $m \leq n < p$, and let $(x_j)_{j=m}^{p}$ and $(y_j)_{j=m}^{p}$ be sequences in R. Then

(a) $\sum_{j=m}^{p} x_j = \sum_{j=m}^{n} x_j \oplus \sum_{j=n+1}^{p} x_j$,

(b) $\sum_{j=m}^{p} (x_j \oplus y_j) = \sum_{j=m}^{p} x_j \oplus \sum_{j=m}^{p} y_j$.

PROOF: Left as an exercise. ■

Proposition 6.16 (B/G prop.4.17)**.**

Let $m, n, p \in \mathbb{Z}$ such that $m \leq n$, and let $(x_j)_{j=m}^{n}$ be a sequence in R. Then $\sum_{j=m}^{n} x_j = \sum_{j=m+p}^{n+p} x_{j-p}$.

PROOF: Left as an exercise. ■

Proposition 6.17 (B/G prop.4.18)**.**

Let $m, n \in \mathbb{Z}$ such that $m \leq n$, and let $(x_j)_{j=m}^{n}$ and $(y_j)_{j=m}^{n}$ be sequences in R such that $x_j \leq y_j$ for all $m \leq j \leq n$. Then $\sum_{j=m}^{n} x_j \leq \sum_{j=m}^{n} y_j$.

PROOF: Left as an exercise. ■

We established earlier the convention to write

$$x \oplus y \oplus z \quad \text{for either of} \quad (x \oplus y) \oplus z \ \text{ and } \ x \oplus (y \oplus z)\,,$$
$$x \odot y \odot z \quad \text{for either of} \quad (x \odot y) \odot z \ \text{ and } \ x \odot (y \odot z)\,,$$

since the operations $\oplus$ and $\odot$ are associative and we announced that we will be able to dispense with parentheses in expressions that involve sums or products of more than three items

Theorem 6.7 (Generalized Law of Associativity)**.**

Let $x_1, x_2, \ldots, x_n \in R$. Then the formulas for associativity stated for $n = 3$,

- $x_1 \oplus (x_2 \oplus x_3) \ = \ (x_1 \oplus x_2) \oplus x_3$ *for sums*
- $x_1 \odot (x_2 \odot x_3) \ = \ (x_1 \odot x_2) \odot x_3$ *for products*

extend to $x_1, x_2, \ldots, x_n$ in the following sense: It does not matter how parentheses are used to control the order how the sum and the product of those n items is evaluated.

- *Moreover, the value of any such grouping is $\displaystyle\sum_{j=1}^{n} x_j$ for summation and $\displaystyle\prod_{j=1}^{n} x_j$ for products.*

PROOF: The proof is given for summation only because the proof for products is similar. It is done by induction on the size n of a list of elements of R.

Base case: The proof is obvious for $n = 1, 2, 3$. (We use associativity for $k = 3$).

Induction assumption:

If $k \leq n$ and $y_1, \ldots y_k \in R$ then any grouping with parentheses of $y_1 \oplus \cdots \oplus y_k$ equals $\displaystyle\sum_{j=1}^{k} y_j$.

Let us now assume that we have a sum of $x_1, \ldots x_n, x_{n+1}$, grouped by parentheses. Let A denote that sum. We may assume that $n \geq 4$ and that there are no superfluous parentheses, i.e., no parentheses of the form **(a)** (x_j), **(b)** $((\ldots))$, and **(c)** pairs of parentheses that enclose the entire list of $n + 1$ elements. Because parentheses of type **(a)** and **(c)** are excluded, we have either of

$$\text{case 1: } x_1 \ \oplus \ (\ldots) \qquad \text{or} \qquad \text{case 2: } (\ldots) \oplus x_{n+1} \qquad \text{or} \qquad \text{case 3: } (\ldots) \oplus (\ldots),$$

where $(\ldots)$ contains at most n of the $n + 1$ items.

Case 1: $(\ldots)$ is a sum of the items $x_2, \ldots, x_{n+1}$, grouped by parentheses. It follows from the induction assumption that $A \ = \ x_1 \ \oplus \ \displaystyle\sum_{j=2}^{n+1} x_j \ = \ \sum_{j=1}^{1} x_j \ \oplus \ \sum_{j=2}^{n+1} x_j.$

Case 2: $(\ldots)$ is a sum of the items $x_1, \ldots, x_n$, grouped by parentheses. It follows from the induction assumption that $A \ = \ \displaystyle\sum_{j=1}^{n} x_j \ \oplus \ x_{n+1} \ = \ \sum_{j=1}^{n} x_j \ \oplus \ \sum_{j=n+1}^{n+1} x_j.$

Case 3: There will be some $K \in \mathbb{N}$ such that $2 \leq K < n$ and such that the left grouping $(\dots)$ consists of $x_1, \dots, x_K$ and the right grouping $(\dots)$ consists of $x_{K+1}, \dots, x_{n+1}$. It follows from the induction assumption that $A = \sum_{j=1}^{K} x_j \oplus \sum_{j=K+1}^{n+1} x_j$.

In either case we conclude with the help of prop.6.15**(a)** that $A = \sum_{j=1}^{n} x_{n+1}$. ■

Definition 6.8.

Let $\beta \in R$. For any $n \in \mathbb{Z}_{\geq 0}$ we define $\beta^n \in R$ recursively as follows:

(6.10) (i) $\beta^0 := 1$, (ii) $\beta^{n+1} = \beta^n \odot \beta$.

In an expression of the form β^n we call β the **basis**, we call n the **exponent**, and we call β^n the n–th **power** of β. □

Remark 6.7. Note that the above definition implies that $0^0 = 1$.

Proposition 6.18 (B/G prop.4.6: Arithmetic Rules for Exponentiation)**.**

Let $\beta \in R$ and $k, m \in \mathbb{Z}_{\geq 0}$. We have the following:

(a) *If $\beta > 0$ then $\beta^k > 0$,*
(b) $\beta^m \odot \beta^k = \beta^{m+k}$,
(c) $(\beta^m)^k = \beta^{mk}$.

PROOF: The proof of **(a)** is given (for $R = \mathbb{Z}$) in [1] Beck/Geoghegan Art of Proof, ch.4.
The proofs of **(b)** and **(c)** is left as exercise 6.5 (see p.252). ■

Proposition 6.19 (B/G prop.10.9)**.**

Let $a \in R$ such that $0 \leq a \leq 1$, and let $m, n \in \mathbb{N}$ such that $m \geq n$. Then $a^m \leq a^n$.

The proof is left as exercise 6.6 (see p.252). ■

Proposition 6.20 (B/G prop.8.41)**.**

Let $a \in R$. Then $a^2 < a^3$ if and only if $a > 1$.

PROOF: Left as an exercise. ■

Definition 6.9 (Finite Geometric Series)**.**

Let $q \in R$ and $n \in \mathbb{Z}_{\geq 0}$.

We call a sum of the form $\displaystyle\sum_{j=0}^{n} q^j$ a **finite geometric series**. □

Proposition 6.21 (Finite Geometric Series Formula (B/G prop.4.13))**.**

Let $q \in R$. If $n \in \mathbb{Z}_{\geq 0}$ then

$$(1 \ominus q) \odot \sum_{j=0}^{n} q^j \;=\; 1 \ominus q^{n+1}\,.$$

PROOF: Left for as exercise 6.8 (see p.252). That exercise is stated for $R = \mathbb{Z}$, but the proof for general R is no different. ■

Remark 6.8.

Except for prop.6.17 there are no inequalities involved in the formulas for generalized sums, products and powers, and we did not take advantage of the absence of zero divisors either. Thus we could have worked everywhere else with a commutative ring with unit instead of an ordered integral domain. □

6.6 Binomial Coefficients

The material here follows very closely ch.4.4 (The Binomial Theorem) of [1] Beck/Geoghegan.

The recursive definitions of sums $\sum x_j$, products $\prod x_j$, and powers x^n can be generalized to more general objects x_j and x (see ch.6.5 on p.217), but the following definition cannot be generalized to objects n more general than nonnegative integers.

Definition 6.10 (Definition of Factorials)**.**

For any $n \in \mathbb{Z}_{\geq 0}$ we define a natural number $n!$ recursively as follows:

(6.11) (i) $0! := 1$, (ii) $(n+1)! = n! \cdot (n+1)$.

We pronounce $n!$ as n **factorial**. □

Remark 6.9.

If $n \geq 1$ then $n!$ represents the product of the "first n natural numbers":

$$\begin{aligned} 1! &= 0! \cdot 1 = 1, \\ 2! &= 1! \cdot 2 = 1 \cdot 2, \\ 3! &= 2! \cdot 3 = 1 \cdot 2 \cdot 3, \\ &\text{– – – – – – – – – – – – –} \\ n! &= 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n. \ \square \end{aligned}$$

Definition 6.11 (Binomial coefficients)**.**

Let $n, k \in \mathbb{Z}$ such that $0 \leq k \leq n$. We define the **binomial coefficient** $\binom{n}{k}$ (pronounced "n choose k") as follows:

$$\binom{n}{k} := \begin{cases} 1 & \text{if k = 0 or k = n,} \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{otherwise, i.e., } n \geq 2 \text{ and } 0 < k < n. \ \square \end{cases} \tag{6.12}$$

Remark 6.10.

The binomial coefficients form a triangle, the so called **Pascal triangle**. The recursive formula above states that a binomial coefficient $\binom{n}{k}$ which is neither at the left side ($k = 0$) nor at the right side ($k = n$) of that triangle,is computed as the sum of its upper left and upper right ancestors.

Here are the binomial coefficients for $n = 0, 1, 2, 3, 4$.

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

Note that binomial coefficients are natural numbers since they are either 1 or the sum of natural numbers. In particular they are integers and not fractions. $\square$

Proposition 6.22.

Let $n, k \in \mathbb{Z}$ such that $0 \leq k \leq n$. Then

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{6.13}$$

PROOF: We do the proof by strong induction on n.
(6.13) is obvious for $k = 0$ or $k = n$ since $\frac{n!}{0!\cdot n!} = 1$. This takes care of the base cases $n = 0$ and $n = 1$.
Let $n \geq 2$ and $1 \leq k \leq n-1$. Our induction assumption is that

$$\binom{m}{j} = \frac{m!}{j!(m-j)!} \quad \text{if } m < n \text{ and } 0 \leq j \leq m. \tag{6.14}$$

We prove the validity of (6.13) as follows.

$$\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k} \\
&= \frac{(n-1)!}{(k-1)!\cdot((n-1)-(k-1))!} + \frac{(n-1)!}{k!\cdot\big((n-1)-k\big)!} \\
&= \frac{(n-1)!}{(k-1)!\cdot(n-k)!} + \frac{(n-1)!}{k!\cdot\big((n-k)-1\big)!} \\
&= \frac{k\cdot(n-1)!}{k!\cdot(n-k)!} + \frac{(n-1)!\cdot(n-k)}{k!\cdot(n-k)!} \\
&= (k+n-k)\cdot\frac{(n-1)!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)!}{k!\cdot(n-k)!} = \frac{n!}{k!\cdot(n-k)!}.
\end{aligned}$$

Equation #1 above follows from (6.12), #2 follows from the induction assumption (6.14). ■

Note that, in contrast to our approach, B/G uses prop.6.22 above as the definition of the binomial coefficients, and (6.12) of this document then becomes a proposition.

The reduction formula in the following lemma allows to express a binomial coefficient in terms of another with smaller numbers.

Lemma 6.2 (Symmetry and reduction lemma)**.**

$$\binom{n}{k} = \binom{n}{n-k} \quad (0 \leq k \leq n) \qquad \textit{symmetry} \tag{6.15a}$$

$$\binom{n}{k} = \frac{n}{k}\cdot\binom{n-1}{k-1} \quad (1 \leq k \leq n) \qquad \textit{reduction} \tag{6.15b}$$

PROOF of (6.15a):

$$\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!} = \frac{n!}{(n-k)!\cdot k!} = \binom{n}{n-k}$$

PROOF (6.15b):

$$\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)!}{k\cdot(k-1)!\cdot((n-1)-(k-1))!} = \frac{n}{k}\cdot\binom{n-1}{k-1}$$ ■

We recall the binomial formula for squares

$$(a \ + \ b)^2 \quad = \quad 1 \cdot a^2 \ + \ 2 \cdot ab \ + \ b^2.$$

and the one for cubes:

$$(a \ + \ b)^3 \quad = \quad 1 \cdot a^3 \ + \ 3 \cdot a^2 b \ + \ 3 \cdot ab^2 \ + \ 1 \cdot b^3.$$

We see that the coefficients of the terms $a^i b^j$ match the numbers of the Pascal triangle: They are the binomial coefficients $\binom{n}{k}$ for $n = 2$ and $n = 3$. Here is the generalization to compute $(a \ + \ b)^n$ for arbitrary n.

Let $R = (R, \oplus, \odot)$ be an integral domain. We also remember that exponentials x^n and products kx are defined for $n \in [0, \infty[$, $k \in \mathbb{Z}$, $x \in R$, as follows:

$$\begin{aligned} x^n \ &= 1 \ \text{ if } n = 0 \qquad \text{and} \qquad x^n \ = x \odot x^{n-1} \ \text{ if } n > 0\,, \\ kx \ &= e(k) \odot x \qquad \text{where} \quad k \mapsto e(k) \text{ is the embedding } \mathbb{Z} \to R \text{ defined in Chapter 6.4}\,. \end{aligned}$$

Theorem 6.8 (Binomial theorem)**.**

Let $R = (R, \oplus, \odot)$ be an integral domain.
If $n \in \mathbb{Z}_{\geq 0}$ and $a, b \in R$, then

$$(a \oplus b)^n \ = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{6.16}$$

PROOF:
The proof is done by induction over n
Base case $n = 0$: Follows from $\binom{0}{0} = 1$ and $a^0 = b^0 = (a \oplus b)^0 = 1$.
Induction assumption: For some $n \geq 0$ it is true that

$$(a \oplus b)^n \ = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{6.17}$$

We need to show that

$$(a \oplus b)^{n+1} \ = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}. \tag{6.18}$$

It follows from the formulas in ch.6.5 (Recursive Definitions of Sums, Products and Powers in Integral

Domains) and prop.6.22 that

$$\begin{aligned}\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k} &= \binom{n+1}{0}a^0 b^{n+1} \oplus \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} \oplus \binom{n+1}{n+1}a^{n+1}b^0 \\ &= b^{n+1} \oplus \sum_{k=1}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)a^k b^{n+1-k} \oplus a^{n+1} \\ &= b^{n+1} \oplus \sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n+1-k} \oplus \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} \oplus a^{n+1} \\ &= b^{n+1} \oplus \sum_{k=0}^{n-1}\binom{n}{k}a^{k+1} b^{n+1-(k+1)} \oplus \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} \oplus a^{n+1}.\end{aligned}$$

The last equation above results from application of prop.6.16 to the first summation term. We continue by pulling a^{n+1} into the first sum and b^{n+1} into the second sum, using prop.6.15**(a)**. This yields

$$\begin{aligned}\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k} &= \sum_{k=0}^{n}\binom{n}{k}a^{k+1} b^{n-k} \oplus \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\ &\overset{\text{prop.6.14(a)}}{=} a\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \oplus b\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}.\end{aligned}$$

We apply the induction assumption (6.17) to each sum in the last expression and obtain

$$\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k} = a(a\oplus b)^n + b(a\oplus b)^n = (a\oplus b)(a\oplus b)^n = (a\oplus b)^{n+1}.$$

We have proven (6.18), and this completes the induction step. ■

Corollary 6.4.

Let $n \in \mathbb{Z}_{\geq 0}$. Then $\displaystyle\sum_{k=0}^{n}\binom{n}{k} = 2^n.$

PROOF: We apply the binomial theorem with $a = b = 1$. Since $1^j = 1$ for all $j \in \mathbb{Z}_{\geq 0}$,

$$2^b = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}a^j b^{n-k} = \sum_{k=0}^{n}\binom{n}{k}. \quad \blacksquare \tag{6.19}$$

6.7 Bernstein Polynomials ⋆

Note that this chapter is starred, hence optional.

However, be aware that we will cite the results of this chapter later in this document.

The material in this chapter makes extensive use of the properties of binomial coefficients.

Definition 6.12 (Bernstein Polynomials)**.**

⋆

Let $f : [0,1] \to \mathbb{R}$ be a real–valued function on the unit interval which need not necessarily be continuous. If $n \in \mathbb{N}$ then

$$B_n^f : \mathbb{R} \to \mathbb{R}; \qquad x \mapsto B_n^f(x) \ := \sum_{k=0}^{n} \binom{n}{k} f\Big(\frac{k}{n}\Big) x^k (1-x)^{n-k}. \tag{6.20}$$

defines a function of the form (**??**) (see p.**??**), thus B_n^f is a polynomial which we call the n–th **Bernstein polynomial** associated with $f(\cdot)$. □

Remark 6.11. Note that the degree of B_n^f need not be n. For example, any function f such that B_n^f is the zero polynomial has no degree. Obviously such is the case for the zero function $0 : x \to 0$ where $0 \le x \le 1$. Here is a less trivial example. Consider the function

$$g : \mathbb{R} \to [0,1]; \qquad g(x) := \begin{cases} 0 & \text{if } x \in \mathbb{Q}, \\ 1 & \text{else.} \end{cases} \tag{6.21}$$

Since $\frac{k}{n} \in \mathbb{Q}$ for all $n \in \mathbb{N}$ and all integers k such that $0 \le k \le n$ it follows that $g(\frac{k}{n}) = 0$ for such k and n, thus $B_n^g = 0$. □

We now compute the Bernstein polynomials for some specific functions. The proof makes extensive use of the properties of binomial coefficients. Note that all this takes place on the unit interval $[0,1] = \{x \in \mathbb{R} : 0 \le x \le 1\}$.

Proposition 6.23 (The Bernstein polynomials for $1, id(\cdot), id^2(\cdot)$)**.**

Let

$$1 : x \mapsto 1; \qquad id : x \mapsto x; \qquad id^2 : x \mapsto x^2; \qquad (0 \le x \le 1) \tag{6.22}$$

be the constant function 1*, the identity function, and the square function on the unit interval* $[0,1]$*. Then*

$$B_n^1 = 1, \tag{6.23a}$$

$$B_n^{id} = id, \tag{6.23b}$$

$$B_n^{id^2} = \frac{1}{n} id + \frac{n-1}{n} id^2. \tag{6.23c}$$

In other words, for any real number x we have

$$\begin{aligned} B_n^1(x) &= 1 \\ B_n^{id}(x) &= id(x) = x \\ B_n^{id^2}(x) &= \frac{1}{n} id(x) + \frac{n-1}{n} id^2(x) = \frac{1}{n}x + \frac{n-1}{n}x^2. \end{aligned}$$

PROOF of (6.23**(a)**): If $x \in \mathbb{R}$ then

$$B_n^1(x) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} = (x + (1-x))^n = 1^n = 1$$

The second equality results from (6.16) (binomial theorem) on p.225 applied to $a = x$ and $b = 1 - x$.

PROOF of (6.23**(b)**): Let $x \in \mathbb{R}$. We must show that $B_n^{id}(x) = x$. Observe that

$$B_n^{id}(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{k}{n} x^k (1-x)^{n-k} = \sum_{k=1}^{n} \frac{k}{n} \binom{n}{k} x^k (1-x)^{n-k}.$$

We were able to discard the $k = 0$ term because $\frac{k}{n} = 0$. The reduction formula (6.15b) on p.224 yields

$$\frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1} \qquad (1 \le k \le n),$$

thus

$$B_n^{id}(x) = \sum_{k=1}^{n} \binom{n-1}{k-1} x^k (1-x)^{n-k}.$$

We change the summation index to $j := k - 1$, i.e., $k = j + 1$. Then

$$B_n^{id}(x) = \sum_{j=0}^{n-1} \binom{n-1}{j} x \cdot x^j (1-x)^{n-(j+1)}.$$

We rewrite $n - (j+1) = n - j - 1 = (n-1) - j$. This yields (6.23**(b)**):

$$B_n^{id}(x) = x \sum_{j=0}^{n-1} \binom{n-1}{j} x^j (1-x)^{(n-1)-j} = x\left(x + (1-x)\right)^{n-1} = x \cdot 1^{n-1} = x. \tag{6.24}$$

PROOF of (6.23**(c)**): The proof of this formula is significantly more complicated than that of 6.23**(b)**. We have

$$B_n^{id^2}(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{k^2}{n^2} x^k (1-x)^{n-k} = \sum_{k=1}^{n} \frac{k^2}{n^2} \binom{n}{k} x^k (1-x)^{n-k}. \tag{6.25}$$

We were able to throw away the $k = 0$ term because this term is the product of k^2/n^2 with some other stuff and $k^2/n^2 = 0$. As in the proof of part b, we'll use the symmetry and reduction lemma. Moreover, the definition formula for binomial coefficients

$$\binom{n}{k} \;=\; \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{for } 1 \le k \le n-1$$

will be used in this proof. This formula is not valid for $k = n$ and we must split off the corresponding summation term

$$\binom{n}{n}\frac{n^2}{n^2}\, x^n(1-x)^{n-n} \;=\; 1 \cdot 1 \cdot\; x^n(1-x)^0 \;=\; x^n. \tag{6.26}$$

before applying the triangle formula. For $k < n$ we obtain

$$\frac{k^2}{n^2}\binom{n}{k} \;=\; \frac{k^2}{n^2}\,\frac{n}{k}\binom{n-1}{k-1} \;=\; \frac{k}{n}\cdot\left(\binom{n}{k} - \binom{n-1}{k}\right) \tag{6.27}$$

by applying the reduction formula to the first equation and the Pascal triangle formula to the second one. Hence, remembering from (6.26) that the n^{th} term is x^n,

$$\begin{aligned} B_n^{id^2}(x) \;&=\; \sum_{k=1}^{n-1} \frac{k}{n}\cdot\left(\binom{n}{k} - \binom{n-1}{k}\right)\cdot x^k(1-x)^{n-k} \;+\; x^n \\ &=\; \sum_{k=1}^{n-1} \left(\frac{k}{n}\binom{n}{k} - \frac{k}{n}\binom{n-1}{k}\right)\cdot x^k(1-x)^{n-k} \;+\; x^n. \end{aligned} \tag{6.28}$$

We use the symmetry and reduction lemma again and substitute

$$\frac{k}{n}\binom{n}{k} \;=\; \binom{n-1}{k-1}$$

in the left hand side of the difference. This yields

$$\begin{aligned} B_n^{id^2}(x) \;&=\; \sum_{k=1}^{n-1} \binom{n-1}{k-1} x^k(1-x)^{n-k} \;+\; x^n \\ &\quad -\; \sum_{k=1}^{n-1} \frac{k}{n}\binom{n-1}{k} x^k(1-x)^{n-k}. \end{aligned} \tag{6.29}$$

To make the proof easier to follow we abbreviate

$$\Phi_1 \;:=\; \sum_{k=1}^{n-1} \binom{n-1}{k-1} x^k(1-x)^{n-k} \;+\; x^n, \tag{6.30a}$$

$$\Phi_2 \;:=\; \sum_{k=1}^{n-1} \frac{k}{n}\binom{n-1}{k} x^k(1-x)^{n-k}, \tag{6.30b}$$

thus

$$B_n^{id^2}(x) \;=\; \Phi_1 \;-\; \Phi_2. \tag{6.31}$$

We will transform Φ_1 and Φ_2 separately.
First we simplify Φ_1. We substitute the summation index k the same way we did before in part b:

$$j \;:=\; k-1; \qquad \text{i.e.,} \qquad k \;=\; j+1.$$

Since

$$n-k \;=\; (n-1) \;-\; (k-1) \;=\; (n-1) \;-\; j$$

and

$$\binom{n-1}{n-1} \;=1 \;=\; (1-x)^0$$

we conclude that

$$\begin{aligned}\Phi_1 \;&=\sum_{j=0}^{n-2}\binom{n-1}{j}x^{j+1}(1-x)^{(n-1)-j} \;+\; x^n\\ &=\sum_{j=0}^{n-2}\binom{n-1}{j}x\cdot x^{j}(1-x)^{(n-1)-j} \;+\; \binom{n-1}{n-1}x\cdot x^{n-1}(1-x)^0\\ &=x\sum_{j=0}^{n-1}\binom{n-1}{j}x^{j}(1-x)^{(n-1)-j}.\end{aligned}$$

We apply the binomial theorem to the last term and obtain

$$\Phi_1 \;=\; x\big(x+(1-x)\big)^{n-1} \;=\; x\cdot 1^{n-1} \;=\; x. \tag{6.32}$$

Now we simplify Φ_2. Since $\frac{k}{n} \;=\; \frac{n-1}{n}\cdot\frac{k}{n-1}$ we can write

$$\begin{aligned}\Phi_2 \;&:=\sum_{k=1}^{n-1}\frac{k}{n}\binom{n-1}{k}x^k(1-x)^{n-k}\\ &=\frac{n-1}{n}\sum_{k=1}^{n-1}\frac{k}{n-1}\binom{n-1}{k}x^k(1-x)^{n-k}\\ &=\frac{n-1}{n}\sum_{k=1}^{n-1}\binom{n-2}{k-1}x\cdot x^{k-1}(1-x)(1-x)^{(n-1)-k}.\end{aligned}$$

The last equality follows from the reduction formula $\frac{k}{n-1}\binom{n-1}{k}=\binom{n-2}{k-1}$ See (6.15b) on p.224. Since $(n-1)-k=(n-2)-(k-1)$ we conclude that

$$\begin{aligned}\Phi_2 \;&=\frac{n-1}{n}\sum_{k=1}^{n-1}\binom{n-2}{k-1}x\cdot x^{k-1}(1-x)(1-x)^{(n-2)-(k-1)}\\ &=\frac{n-1}{n}x(1-x)\sum_{j=0}^{n-2}\binom{n-2}{j}x^{j}(1-x)^{(n-2)-j}.\end{aligned}$$

We obtained the last equality by substituting again $j := k-1$. Another application of the binomial theorem yields

$$\sum_{j=0}^{n-2} \binom{n-2}{j} x^j (1-x)^{(n-2)-j} \;=\; (x+(1-x))^{n-2} \;=\; 1^{n-2} \;=\; 1.$$

Thus

$$\Phi_2 \;=\; \frac{n-1}{n} x(1-x). \tag{6.33}$$

We finally use the expressions (6.32) for Φ_1 and (6.33) for Φ_2 in the equation $B_n^{id^2}(\cdot) = \Phi_1 - \Phi_2$:

$$\begin{aligned} B_n^{id^2}(\cdot) \;&= \Phi_1 - \Phi_2 \;=\; x \;-\; \frac{n-1}{n} x(1-x) \\ &= x \;-\; \frac{n-1}{n} x \;+\; \frac{n-1}{n} x^2 \\ &= x\Big(1 - \frac{n-1}{n}\Big) \;+\; \frac{n-1}{n} x^2 \\ &= \frac{x}{n} \;+\; \frac{n-1}{n} x^2. \end{aligned} \tag{6.34}$$

This concludes the proof of equation (6.23c). ■

We finish this chapter with the interpretation of the Bernstein polynomials B_n^f as expected values of the discretizations $f_n(k) = f(k/n)$ of a real–valued function defined on the unit interval. You may find it difficult to follow the next remark without some background in probability theory.

Remark 6.12 (Connection between Bernstein polynomials and probability theory)**.**

Let $f : [0,1] \to \mathbb{R}$ be a nonnegative function. For each $n \in \mathbb{N}$ we define

$$f_n : [0,n]_{\mathbb{Z}} \to \mathbb{R}; \quad k \mapsto f(k/n). \tag{6.35}$$

In other words we obtain f_n by "digitizing" or "sampling" f at the points $0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1$.

It is well known to those who have had some exposure to probability theory that for fixed $p \in [0,1]$ the formula

$$P_p\{k\} \;:=\; \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} \tag{6.36}$$

defines a probability on the set $[0,n]_{\mathbb{Z}}$. This is the binomial distribution with parameters n and p, and its meaning is as follows.

Assume that the items in some population Ω possess a certain property B of interest, and that the probability of choosing "at random" an $\omega \in \Omega$ which possesses that property is p. For example let Ω be a box which contains 500 marbles of different colors which are well shuffled, that 100 of those marbles are of green color, that the person who picks a marble is blindfolded, and that the property of interest is B: "A green marble was picked". Then $p = \frac{100}{500} = 0.2$.

Assume now that

- n times in a row an item ω_j is chosen at random from Ω ($j = 1, 2, \ldots, n$),
- it is recorded after pick j whether or not ω_j possesses that property,
- ω_j is put back into Ω in such a way that the probabilistic situation is no different from the one we had before ω_j was chosen. In the example with the marbles this means that the marbles will be thoroughly reshuffled before each pick).

Let $S = S(\omega_1, \omega_2, \ldots, \omega_n)$ denote how many of the n chosen items $\omega_1, \ldots, \omega_n$ satisfy B. We can think of S as a function

$$S : \Omega^n \to [0, n]_{\mathbb{Z}}; \quad (\omega_1, \ldots, \omega_n) \mapsto S(\omega_1, \ldots, \omega_n). \tag{6.37}$$

Consider the preimage of the set $\{k\}$ under the function S, i.e., the set

$$\{S = k\} \;=\; S^{-1}\{k\} \;=\; \{(\omega_1, \ldots, \omega_n) \in \Omega^n : \text{ exactly } k \text{ of the } \omega_j \text{ have property B}\}. \tag{6.38}$$

It is a well known fact that under the above conditions the "random variable" S follows a binomial distribution with parameters n and p as described in (6.36) above, i.e.,

$$\text{probability of } \{S = k\} \;= P_p\{k\} \;=\; \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}. \tag{6.39}$$

After this brief excursion into binomial distributions we go back to the function f which is defined on the codomain of the random variable S. We will subsequently write $\vec{\omega}$ for $(\omega_1, \ldots, \omega_n)$. The compositions $\omega \mapsto f \circ S(\omega)$ and $\omega \mapsto f_n \circ S(\omega)$ itself can be thought of as random variables since their values $f\big(S(\vec{\omega})\big)$ and $f_n\big(S(\vec{\omega})\big)$ depend on the randomly selected argument $\vec{\omega}$. The so–called **expectation** or **expected value** of the random variable $f_n \circ S$ under the probability distribution P_p defined by (6.39) is then given as

$$E_p\big(f_n \circ S\big) \;= \sum_{k=0}^{n} f_n(k) \cdot P_p\{k\} \;= \sum_{k=0}^{n} f(k/n) \cdot \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} \;=\; B_n^{f_n}(p). \;\square \tag{6.40}$$

6.8 The Well–Ordering Principle

Theorem 6.9 (Well–Ordering Principle)**.**

Every nonempty subset of $\mathbb{N}$ *possesses a minimum, i.e., a smallest element.*

PROOF:

Let $A \subseteq \mathbb{N}$ such that A does not possess a minimum. We claim that it suffices to prove that

$$[1, k]_{\mathbb{Z}} \subseteq A^{\complement} \quad \text{for all } k \in \mathbb{N}.$$

Here, $A^{\complement} = \mathbb{N} \setminus A$ denotes the complement of A in $\mathbb{N}$. This is so because, according to Proposition 6.3 on p.208, $1 = \min(\mathbb{N})$ and thus, $\mathbb{N} \;=\; [1, \infty[_{\mathbb{Z}} \;=\; \bigcup_{k=1}^{\infty} [1, k]_{\mathbb{Z}}$.

For $k \in \mathbb{N}$ let $p(k)$ be the statement $[1, k]_{\mathbb{Z}} \subseteq A^{\complement}$.

We will use induction on k to prove that $p(k)$ is true for all $k \in \mathbb{N}$.

Base case $k = 1$: Note that $1 \notin A$, because, as the minimum of $\mathbb{N}$, 1 would also be the minimum of A. Hence, $1 \in A^{\complement}$, hence $[1,1]_{\mathbb{Z}} = \{1\} \subseteq A^{\complement}$, and this proves the base case.

(IA) Induction assumption: $p(k)$ is true, i.e., $[1,k]_{\mathbb{Z}} \subseteq A^{\complement}$.

$(\star)$ We must prove under this assumption that $[1,k+1]_{\mathbb{Z}} \subseteq A^{\complement}$.

- Since $A \subseteq \mathbb{N}$, the induction assumption $[1,k]_{\mathbb{Z}} \subseteq A^{\complement}$ implies that $k < a$ for all $a \in A$.
- Since $]k,k+1[_{\mathbb{Z}} = \emptyset$ by Corollary 6.2 on p.208, it follows that $k+1 \leq a$ for all $a \in A$. Thus, $k+1$ is a lower bound of A.
- If it was true that $k+1 \in A$, then $k+1 = \min(A)$ by definition of a minimum. Since we assumed that A does not possess a minimum, we conclude that $k+1 \notin A$, i.e., $k+1 \in A^{\complement}$.
- Since we assumed $[1,k]_{\mathbb{Z}} \subseteq A^{\complement}$, it follows from $k+1 \notin A$ that $[1,k+1]_{\mathbb{Z}} \subseteq A^{\complement}$.

We have shown $(\star)$ and this finishes the proof by induction. ■

Alternate proof: $\boxed{\star}$

(A) Let $\Gamma := \{k \in \mathbb{N} : \text{ if } B \subseteq \mathbb{N} \text{ such that } [1,k]_{\mathbb{Z}} \cap B \neq \emptyset \text{ then } \min(B) \text{ exists } \}$.

Proof strategy:

(1) We will show that $1 \in \Gamma$.

(2) We will show that $n+1 \in \Gamma$ whenever $n \in \Gamma$.

(3) It follows from the induction axiom that $\Gamma = \mathbb{N}$. We will show how this implies that any nonempty $B \subseteq \mathbb{N}$ possesses a minimum.

Proof of (1): Let $B \subseteq \mathbb{N}$ such that $[1,1]_{\mathbb{Z}} \cap B \neq \emptyset$, i.e., $1 \in B$. (Thus B is nonempty.) It follows from Proposition 6.3 (sharpening of B/G Prop.2.13) on p.208 and $B \subseteq \mathbb{N}$ that 1 is a lower bound of B. Since $1 \in B$, $1 = \min(B)$. We have proved that $1 \in \Gamma$, and we are done with step **(1)**.

Proof of (2): Now assume that $n \in \Gamma$. To prove that $n+1 \in \Gamma$ we proceed as follows.

Let $B \subseteq \mathbb{N}$ such that $[1,n+1]_{\mathbb{Z}} \cap B \neq \emptyset$ (which implies that B had to be nonempty to begin with). Since the set B satisfying this was arbitrarily chosen,

(B) to prove that $n+1 \in \Gamma$ it suffices to show that $\min(B)$ exists.

We consider the two separate cases $[1,n] \cap B = \emptyset$ and $[1,n] \cap B \neq \emptyset$.

Case 1: $[1,n] \cap B \neq \emptyset$.

Since we assume $n \in \Gamma$, we obtain from the definition of Γ that B possesses a minimum.

Case 2: $[1,n] \cap B = \emptyset$. We assumed that $[1,n+1]_{\mathbb{Z}} \cap B \neq \emptyset$, thus $n+1 \in B$. Note that $[1,n] \cap B = \emptyset$ implies that $n+1$ is a lower bound of B. Since $n+1 \in B$, $n+1 = \min(B)$.

Case 1 and **case 2** together prove **(B)**, and we are done with step **(2)**.

Proof of (3): Let $\emptyset \neq A \subseteq \mathbb{N}$ and $a \in A$. Such a exists since A is not empty. We finish the proof of the well–ordering principle by showing that A possesses a minimum.

It follows from **(1)** and **(2)** and the induction axiom that $\Gamma = \mathbb{N}$. From $A \subseteq \mathbb{N}$ we obtain $a \in \Gamma$. Since $[1,a]_{\mathbb{Z}} \cap A \neq \emptyset$, A possesses a minimum by definition of the set Γ. ■

Theorem 6.10 (Extended Well–Ordering Principle)**.**

(a) *Let A be a nonempty subset of $\mathbb{Z}$ which is bounded below. Then A possesses a minimum in $\mathbb{Z}$.*
(b) *Let B be a nonempty subset of $\mathbb{Z}$ which is bounded above. Then B possesses a maximum in $\mathbb{Z}$.*
(c) *Let C be a nonempty bounded subset of $\mathbb{Z}$. Then C possesses both minimum and maximum in $\mathbb{Z}$.*

Proof (outline):

(a) If A has 1 as a lower bound then $A \subseteq \mathbb{N}$ and the theorem simply is the Well-Ordering Principle (B/G theorem 2.32). Next we just assume that A is bounded below. Let $a_\star$ be a lower bound of A. Let $A' := A - a_\star + 1$. Then $a' \geq 1$ for all $a' \in A'$, i.e., $A' \subseteq \mathbb{N}$. and it follows from the Well-Ordering Principle that the minimum $\min(A')$ of A' exists.

It is easy to see from $\min(A') \in A'$ that then $m := \min(A') + a_\star - 1 \in A$ and that m is a lower bound of A because $a_\star$ is a lower bound of A. It follows that $m = \min(A)$.

(b) We assume that B is bounded above. Let $b^\star$ be an upper bound of B. Let $B' := -B$. Then B' has $-b^\star$ as a lower bound and it follows from the already proven part **(a)** that the minimum $\min(B')$ of B' exists. Let $m := -\min(B')$. It follows from $\min(B') \in B'$ that $m \in -B' = -(-B) = B$ and it follows from $\min(B') \leq b'$ for all $b' \in B'$ that $m \geq b$ for all $b \in B$. But then m must be the maximum of A.

(c) is a trivial consequence of **(a)** and **(b)** ■

We have not yet given a precise definition of the real and rational numbers. That will be done in axiom **??** on p.**??** and Definition **??** on p.**??**. For now we have make do with the informal definitions of ch.**??** (Numbers) on p.**??**.

Example 6.4 (The Well-Ordering Principle is not true in $\mathbb{Q}$ and $\mathbb{R}$)**.**

(a) $\mathbb{R}$: The set $A := \{x \in \mathbb{R} : x^2 < 2\}$ is bounded in $\mathbb{R}$ (by ± 2) but has neither min (would have to be $-\sqrt{2} \notin A$) nor max (would have to be $+\sqrt{2} \notin A$).
But: $-\sqrt{2}$ is the greatest lower bound or infimum $\inf(A)$ of A, and $\sqrt{2}$ is the least upper bound or supremum $\sup(A)$ of A.

(b) $\mathbb{Q}$: The set $B := \{x \in \mathbb{Q} : x^2 < 2\} = A \cap \mathbb{Q}$ is bounded in $\mathbb{Q}$ (by ± 2) and also has neither min nor max for the same reasons as A.
Further: $-\sqrt{2}$ is **not** a lower bound of B and $\sqrt{2}$ is **not** an upper bound of B because those numbers are not in our "universe" $\mathbb{Q}$. The set B possesses neither min, max, inf, sup! □

Proposition 6.24.

Let $\emptyset \neq A \subseteq B \subseteq \mathbb{Z}$.
(a) *If B is bounded below (resp., above), then $\min(A) \geq \min(B)$ (resp., $\max(A) \leq \max(B)$).*
(b) *If also $\min(B) \notin A$ (resp., $\max(B) \notin A$), then $\min(A) > \min(B)$ (resp., $\max(A) < \max(B)$).*

PROOF:
This follows from prop.?? on p.?? and the extended well-ordering principle. ■

Proposition 6.25 ($\mathbb{N}$ is unbounded in $\mathbb{Z}$)**.**

For any $k \in \mathbb{Z}$ there exists $n \in \mathbb{N}$ such that $n > k$, i.e., there are no upper bounds for $\mathbb{N}$ in $\mathbb{Z}$.

PROOF: Assume to the contrary that there exists an upper bound of $\mathbb{N}$. According to thm.6.10 (extended well-ordering principle) on p.233 $\mathbb{N}$ has a maximum. Let $u^\star := \max(\mathbb{N})$. Then $u^\star + 1$ belongs to $\mathbb{N}$ as the sum of two natural numbers. It follows from $u^\star + 1 > u^\star$ that $u^\star$ is not an upper bound of $\mathbb{N}$ and we have reached a contradiction. ■

6.9 The Division Algorithm

You will find a more detailed treatment of this subject in [1] Beck/Geoghegan Art of Proof, ch.6.2.

Theorem 6.11 (Division Algorithm for Integers (B/G thm.6.13))**.**

Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ Then there exists a unique pair of integers q and r such that

(6.41) $$m = qn + r \qquad \text{and} \qquad 0 \leq r < n.$$

*We call q the **quotient** and r the **remainder** when dividing n into m.*

PROOF: The proof is left as exercise 6.16 (see p.253). ■

The next two propositions are easy to prove with help of the division algorithm. Hint: What is n?

Proposition 6.26 (B/G prop.6.15)**.**

Let $m \in \mathbb{Z}$.
Then m is odd if and only if there exists $q \in \mathbb{Z}$ such that $m = 2q + 1$.

PROOF: Left as an exercise. ■

Proposition 6.27.

Any product of odd numbers is odd.

The proof is left as exercise 6.17 (see p.253). ■

Proposition 6.28 (B/G prop.6.16)**.**

Let $n \in \mathbb{Z}$. Then n is even or $n+1$ is even.

PROOF: Left as an exercise. Hint: It suffices to show that if n is odd then $n+1$ is even. WHY? ■

Proposition 6.29 (B/G prop.6.17)**.**

Let $n \in \mathbb{Z}$. Then n is even if and only if n^2 is even.

PROOF: Left as an exercise. Hint: It suffices to show that if n is odd then n^2 is odd, and if n is even then n^2 is even: See the proof strategy of the proof of prop.**??** on p.**??**. ■

Proposition 6.30 (Division Algorithm for Polynomials (B/G prop. 6.18))**.**

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}$ and let

$$n(x) := \sum_{j=0}^{\alpha} a_j x^j, \qquad m(x) := \sum_{j=0}^{\beta} b_j x^j, \tag{6.42}$$

be two polynomials with real coefficients a_j, b_j such that $n(x)$ is not the null polynomial $p(x) = 0$. Then there exist polynomials $q(x)$ and $r(x)$ such that $r(x)$ has degree less than α or $r(x) = 0$ (and hence has no degree), such that

$$m(x) := q(x)n(x) + r(x). \tag{6.43}$$

PROOF:

Case 1: $\alpha = 0$, i.e., $n(x) = a_0 = \text{const}$.

Note that $n \neq 0$ because we assume that $n(x)$ is not the null polynomial. Let $q(x) := \frac{m(x)}{a_0}$ and $r(x) := 0$. Then $m(x) = n(x)q(x) + r(x)$ yields the desired decomposition 6.43 of $m(x)$.

Case 2: $\alpha > 0$ and $\beta < \alpha$.

Let $q(x) := 0$ and $r(x) := m(x)$. Then $m(x) = n(x)q(x) + r(x)$ satisfies 6.43.

Case 3: $\alpha > 0$ and $\beta \geq \alpha$.

We handle this case using strong induction on β. First some notation. Let

$$A := \sum_{j=0}^{\alpha-1} \frac{b_\beta a_j}{a_\alpha} x^{j+\beta-\alpha}, \qquad B := \sum_{j=0}^{\beta-1} b_j x^j, \tag{6.44}$$

$$p(x) := m(x) - \frac{b_\beta}{a_\alpha} x^{\beta-\alpha} n(x) = b_\beta x^\beta + B - \frac{b_\beta}{a_\alpha} x^{\beta-\alpha} a_\alpha x^\alpha - A = B - A. \tag{6.45}$$

Note that none of the terms of A and B has a power of x with an exponent larger than $\beta - 1$ and, hence, that any constant multiple of $p(x)$ would be a suitable candidate for $r(x)$ as far as the degree is concerned.

Base case: $\beta = \alpha$.

(6.45) yields $p(x) = m(x) - \frac{b_\alpha}{a_\alpha} n(x)$. We have $m(x) = p(x) + \frac{b_\alpha}{a_\alpha} n(x)$. Let $q(x) := \frac{b_\alpha}{a_\alpha}$ and $r(x) := p(x)$. Then $m(x) = n(x)q(x) + r(x)$ yields the desired decomposition 6.43 of $m(x)$.

Induction assumption: Any polynomial $m'(x)$ with degree less than β can be written as $m'(x) = q'(x)n(x) + r'(x)$ such that $r'(x)$ has degree less than α or $r'(x) = 0$.

We use again the notation of (6.44) and (6.45). We have seen that the degree of $p(x)$ is less than β (unless it has no degree because $p(x) = 0$). It follows from (6.45) that $m(x) = p(x) + \frac{b_\beta}{a_\alpha} x^{\beta-\alpha} n(x)$. Let $q(x) := \frac{b_\beta}{a_\alpha} x^{\beta-\alpha}$ and $r(x) := p(x)$. It follows that $m(x) = n(x)q(x) + r(x)$ satisfies 6.43. ■

For the next proposition recall that a root of a polynomial $p(x)$ is a number z such that $p(z) = 0$ (see Definition **??** on p.**??**).

Proposition 6.31 (B/G prop.6.19)**.**

Let $p(x)$ be a polynomial and $z \in \mathbb{R}$. Then z is a root of p if and only if there exists a polynomial $q(x)$ such that

$$p(x) = (x - z)q(x) \text{ for all } x \in \mathbb{R}. \tag{6.46}$$

PROOF: Left as an exercise. Hint: Use the division algorithm for polynomials for the proof of "only if". ■

6.10 The Integers Modulo n

In this chapter we assume that $n \in \mathbb{N}$ is fixed.

Proposition 6.32 (B/G prop.6.24)**.**

For two integers a and b we define

$$a \sim b \quad \text{if and only if} \quad n \mid (a - b). \tag{6.47}$$

Then

- ***(a)*** *(6.47) defines an equivalence relation on $\mathbb{Z}$,*
- ***(b)*** *The equivalence class for $m \in \mathbb{Z}$ is $[m] = [r]$, where r is the remainder of m modulo n. See thm.6.11 (division algorithm for integers) on p.235.*
- ***(c)*** *If $r \in [0, n-1]_{\mathbb{Z}}$ then $[r] = \{qn + r : q \in \mathbb{Z}\}$.*
- ***(d)*** *This equivalence relation has exactly n distinct equivalence classes $[0], [1], \ldots, [n-1]$.*

PROOF: See [1] Beck/Geoghegan Art of Proof, ch.6.3. ■

Definition 6.13 (Equivalence Modulo n)**.**

(a) We write $a \equiv b \mod n$ for $a \sim b$. We call n the **modulus**, and we say that a **equals** b **modulo** n.

(b) We write

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} := \{[0],[1],\ldots,[n-1]\} \tag{6.48}$$

for the set of equivalence classes resulting from the equivalence relation $a \sim b$. (See prop.6.32**(b)** above.) We call $\mathbb{Z}_n$ the set of **integers modulo** n. □

Remark 6.13.

⋆ It is beyond the scope of this document to discuss the reason why mathematicians choose to write the set $\mathbb{Z}_n$ set as a "quotient" $\mathbb{Z}$ divided by $n\mathbb{Z}$. If you take a course in abstract algebra then you will learn that the subset $n\mathbb{Z}$ of $\mathbb{Z}$ is what one calls an **ideal** in the commutative ring with unit $\mathbb{Z}$. Given a commutative ring with unit R and an ideal $\mathfrak{x} \subseteq R$ one can define an equivalence relation $a \sim b$ on R whose set of equivalence classes $R/\mathfrak{x} := \{[a] : a \in R\}$ is called the **quotient ring** of R with respect to the ideal $\mathfrak{x}$ The reason: One can define operations $[a] \oplus [b]$ and $[a] \odot [b]$ on $R/\mathfrak{x}$ which render this set into a commutative ring with unit. In the special case of $R = \mathbb{Z}$ and $\mathfrak{x} = n\mathbb{Z}$ the equivalence relation $a \sim b$ turns out to be (6.47) above, the quotient ring of equivalence classes is $\mathbb{Z}_n$, and addition and multiplication will be the operations defined in Definition 6.14 below. □

Remark 6.14.

We want to introduce

$$\text{addition } [a] \oplus [b] := [a+b] \quad \text{and multiplication } [a] \odot [b] := [a \cdot b] \tag{6.49}$$

as binary operations on the mod n equivalence classes.

Since binary operations on $\mathbb{Z}_n$ are functions

$$\oplus, \odot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n\,,$$

they must define the definition of a function. For example, $\oplus$ is such a function, if and only if for each $([a],[b]) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a UNIQUE $[c] \in \mathbb{Z}_n$ such that

$$\big(([a],[b]),[c]\big) \in \Gamma_\oplus\,, \quad \text{the graph of the function } \oplus. \tag{6.50}$$

Considering (6.49), this can be equivalently expressed as

$$[a] \oplus [b] = [c] \quad \text{and this in turn is equivalent to } a + b \sim c\,. \tag{6.51}$$

Why would that assertion not be obvious? Note that the integers a and b are not the only elements of their equivalence classes

$$[a] \;=\; \{qn + a : q \in \mathbb{Z}\}\,; \qquad [b] \;=\; \{q'n + b : q' \in \mathbb{Z}\} \tag{6.52}$$

Now, if we select some arbitrary $q, q' \in \mathbb{Z}$ in (6.52) and define

$$a' \;:=\; qn \,+\, a\,; \quad b' \;:=\; q'n \,+\, b$$

then the uniqueness of $[c]$ in (6.50) with respect to the definition of $\oplus$ given in (6.49) and the equivalent formulation given in (6.51) demands that also

$$[a' \odot b'] \;=\; [c] \quad \text{i.e., } a' \,+\, b' \;\sim\; c\,. \tag{6.53}$$

Here, we smade use of the definitions $a' = qn + a$, $b' = q'n + b$. We remove the middleman $[c]$ in (6.51) and (6.53) and obtain that being able to define $[a] \oplus [b] := [a + b]$, requires that

$$a + b \;\sim\; (qn + a) \,+\, (q'n + b) \quad \text{for all } q, q' \in \mathbb{Z}\ .$$

In a likewise manner, one shows that

$$a \cdot b \;\sim\; (qn + a) \cdot (q'n + b)$$

must be satisfied for all $q, q' \in \mathbb{Z}$ if one wants to define $[a] \odot [b] := [a \cdot b]$. □

Proposition 6.33 (B/G prop.6.25)**.**

Let $a, a', b, b' \in \mathbb{Z}$ such that $a \sim a'$ and $a \sim a'$, i.e., $n \mid (a - a')$ and $n \mid (b - b')$.
Then $a + b \sim a' + b'$ and $ab \sim a'b'$.

PROOF: Left as an exercise. ■

According to Remark 6.14, that last proposition allows it to define operations $[a] \oplus [b]$ and $[a] \odot [b]$ on $\mathbb{Z}_n$.

Definition 6.14.

Let $a, b \in \mathbb{Z}$.
We define addition $[a] \oplus [b]$ and multiplication $[a] \odot [b]$ for the corresponding equivalence classes $[a], [b] \in \mathbb{Z}_n$ in terms of ordinary addition and multiplication in $\mathbb{Z}$ as follows.

$$[a] \oplus [b] \;:=\; [a + b]; \qquad [a] \odot [b] \;:=\; [ab]. \tag{6.54}$$

We further define $[a]^0 := [1]$. □

The next theorem involves prime numbers: A prime number aka prime is an integer $p \geq 2$ which can be divided evenly only by ± 1 or $\pm p$ Primes will be formally introduced in Section 6.12 (Prime Numbers) on p.243.

Theorem 6.12 (B/G prop.6.26 and B/G project 6.27)**.**

(a) *The operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ of Definition 6.14 above turn $(\mathbb{Z}_n, \oplus, \odot)$ into a commutative ring with unit.*

(b) *$(\mathbb{Z}_n, \oplus, \odot)$ is an integral domain, i.e., there are no zero divisors, if and only if n is prime.*

PROOF: The proof is left as exercise 6.18 (see p.253). ■

The following cannot be found in the B/G text.

Proposition 6.34 (Arithmetic mod n)**.**

Let $m_1, m_2, \ldots m_k,\ a_1, a_2, \ldots a_k \in \mathbb{Z}$. Then

$$[m_1 + m_2 + \cdots + m_k] = [m_1] \oplus [m_2] \oplus \cdots \oplus [m_k], \tag{6.55}$$

$$[m_1 \cdot m_2 \cdots m_k] = [m_1] \odot [m_2] \odot \cdots \odot [m_k], \tag{6.56}$$

$$[\ \sum_{j=1}^{k} a_j x^j\ ] = \sum_{j=1}^{k} [a_j] \odot [x]^j. \tag{6.57}$$

PROOF: We only give the proof of (6.56). It is done by induction on the number of factors k. The proof of (6.55) is similar and (6.57) is a simple consequence of the two first equations.

Basis: The proof is obvious for $k = 1$. We note that (6.56) is true for two factors (prop.6.33 and Definition 6.14 above.

Induction assumption: We assume that (6.56) holds for some $k \in \mathbb{N}$. We then obtain for $k+1$ that

$$\begin{aligned}
[m_1 \cdot m_2 \cdots m_{k+1}] &= [(m_1 \cdot m_2 \cdots m_k) \cdot m_{k+1}] \\
&= \big([m_1 \cdot m_2 \cdots m_k]\big) \odot [m_{k+1}] \quad \text{(B/G def. of ``}a \odot b\text{'')} \\
&= \big([m_1] \odot [m_2] \odot \cdots \odot [m_k]\big) \odot [m_{k+1}]. \quad \text{(Induction assumption (6.56))}
\end{aligned}$$ ■

6.11 The Greatest Common Divisor

We follow [1] Beck/Geoghegan Art of Proof ch.2 and ch.6.

We learned long before college about computing the greatest common divisor of two integers. To find, e.g., $\gcd(90, 225)$ we factor both 90 and 225 into their primes: $90 = 2 \cdot 3 \cdot 3 \cdot 5$, $225 = 3 \cdot 3 \cdot 5 \cdot 5$, and we extract the factors both "prime factorizations" have in common. In the case above that would be two factors 3 and one factor 5, so $\gcd(90, 225) = 3 \cdot 3 \cdot 5 = 45$.

Unfortunately we need to prove certain properties of the greatest common divisor as a stepping stone for the proof that any natural number greater than 1 can be factored uniquely, up to permutations of the factors, into prime numbers. We will get to that in ch.6.12 (Prime Numbers) on p.243, but first we must learn a few things about gcds.

We start with the following lemma [5]

Lemma 6.3 (B/G prop.2.34)**.**

For $m, n \in \mathbb{Z}$ let

$$S := S(m,n) := \{k \in \mathbb{N} : k = mx + ny \text{ for some } x, y, \in \mathbb{Z}\}. \tag{6.58}$$

Then S is empty if and only if $m = n = 0$.

The proof is left as exercise 6.19 (see p.253). ■

Lemma 6.4.

For $m, n \in \mathbb{Z}$ let $S(m,n)$ be defined as in (6.58). Then

(a) $S(m,n) = S(n,m)$,
(b) $S(m,n) = S(-m,n) = S(m,-n) = S(-m,-n)$,
(c) $S(m,n) = S(|m|,|n|)$.

PROOF of **(a)**: $S(m,n) = S(n,m)$ follows from the symmetry of the expression $mx+ny$ with respect to m and n.

PROOF of **(b)**:

It suffices to prove that $S(m,n) = S(-m,n)$ for all $m, n \in \mathbb{Z}$, because then $S(-n,m) = S(n,m)$, and it follows from **(a)** that $S(m,-n) = S(-n,m)$. Thus $S(m,-n) = S(-n,m) = S(n,m)$, and we have proven the first equation of **(b)**. The remaining equations are shown in a similar fashion.

Now to the proof that $S(m,n) = S(-m,n)$. Let $k \in S(m,n)$, i.e., there exist $x, y \in \mathbb{Z}$ such that $k = xm + yn$ and $k > 0$. Let $x' := -x$ and $y' := y$. Then $x', y' \in \mathbb{Z}$ and $x'(-m) + y'n = k$. It follows from $k > 0$ that $k \in S(-m,n)$. Since k is an arbitrary element of $S(m,n)$, it follows that $S(m,n) \subseteq S(-m,n)$. We apply this result to $-m$ instead of m and obtain, since $-(-m) = m$, the reverse inclusion $S(-m,n) \subseteq S\big(-(-m),n\big) = S(m,n)$.

PROOF of **(c)**: This follows from **(b)** since $|m| = m$ or $|m| = -m$, and $|n| = n$ or $|n| = -n$. ■

It follows from lemma 6.3 that if $m \neq 0$ or $n \neq 0$ then $S(m,n) \neq \emptyset$. According to the extended well ordering principle, $S(m,n)$ possesses a minimum. This enables us to make the next definition.

Definition 6.15 (Greatest Common Divisor)**.**

[5] a lemma is a "proof subroutine" which is not remarkable on its own but very useful as a reference for other proofs

For $m, n \in \mathbb{Z}$ let $S = S(m,n)$ be the set defined in (6.58). Let

$$\gcd(m,n) := \begin{cases} 0 & \text{if m = n = 0,} \\ \min(S) & \text{otherwise.} \end{cases} \tag{6.59}$$

We call $\gcd(m,n)$ the **greatest common divisor** of m and n. □

Proposition 6.35 (B/G prop.6.29)**.**

Let $m, n \in \mathbb{Z}$. Then
(a) *$gcd(m,n) \mid m$ and $gcd(m,n) \mid n$,*
(b) *If $m \neq 0$ or $n \neq 0$ then $gcd(m,n) > 0$,*
(c) *Let $k \in \mathbb{Z}$ such that $k \mid m$ and $k \mid n$. Then $k \mid gcd(m,n)$.*

PROOF: The proof given here is that of B/G prop.6.29 with some minor cosmetic changes. In the following we abbreviate $g := \gcd(m,n)$.

Case 1: $m = n = 0$.

Then $g = 0$ according to Lemma 6.3 on p.241. Thus **(a)** holds since $0 \mid 0$ and **(c)** holds since $k \mid 0$ is true for any integer k.

Case 2: $m \neq 0$ or $n \neq 0$.

Then $g = \min(S)$, thus $g \in S$, thus $g \in \mathbb{N}$, and this proves **(b)**. We divide the proof of **(a)** and **(c)** into two cases as follows.

Case 2a: Either $m = 0$ and $n \neq 0$ or $n = 0$ and $m \neq 0$.

We may assume $m = 0$ since the set S is defined symmetrically with respect to m and n. Then

$$S \;= \{ny : y \in \mathbb{Z} \text{ and } ny > 0\} \;=\; \{|n|y : y \in \mathbb{N}\}\,,$$

thus $g = \min(S) = |n|$. It follows that **(a)** holds since $|n| \mid n$ and $|n| \mid 0$. Further, **(c)** holds since $k \mid n \Rightarrow k \mid |n|$, i.e., $k \mid g$.

Case 2b: Both $m \neq 0$ and $n \neq 0$.

Since $S(m,n) = S(|m|,|n|)$, we may assume that $m > 0$ and $n > 0$. Since $g \in \mathbb{N}$ by the already proven part **(b)** we may apply the Division Algorithm (Theorem 6.11 on p.235) and obtain integers q, q', r, r' such that

$$m \;= qg + r \qquad \text{and} \qquad n \;= q'g + r' \qquad \text{and} \qquad 0 \;\leq r, r' \;< g\,. \tag{6.60}$$

We now prove that $r = 0$. Since $g = mx + ny$ for suitable $x, y \in \mathbb{Z}$ it follows from (6.60) that

$$r \;=\; m - qg \;=\; m - q(mx + ny) \;=\; m(1 - qx) + n(-qy)\,,$$

thus $r > 0$ would imply $r \in S$. Since $r < g$ and $g = \min(S)$ it would not be true that $\min(S)$ is a lower bound of S. Thus the assumption that $r > 0$ contradicts the definition of a minimum, thus

$r = 0$. It follows that $m = qg$, i.e., $g|m$. We obtain in likewise manner that $g|n$ and the proof of **(a)** is done.

Proving **(c)** is much simpler: Assume that $k \in \mathbb{Z}$ satisfies both $k|m$ and $k|n$. By definition of divisibility there exist integers j, j' such that $m = jk$ and $n = j'k$. Hence, for any $x, y \in \mathbb{Z}$,

$$mx + ny = (jk)x + (j'k)y = (jx + j'y)k,$$

hence $k \mid mx + ny$. Since $g \in S$, $g = mx + ny$ for suitable $x, y \in \mathbb{Z}$. Thus $k \mid g$ and **(c)** follows. ■

Remark 6.15.

- Proposition 6.35**(a)** justifies us calling $\gcd(m, n)$ a common divisor of m and n.
- If $i, j \in \mathbb{N}$ such that $i \mid j$ then $i \leq j$ according to Proposition 6.9 (B/G prop.2.23) on p.211. Thus Proposition 6.35**(c)** shows that $\gcd(m, n)$ is in fact the largest possible of all common divisors of m and n. □

Proposition 6.36 (B/G prop.6.30)**.**

Let $k, m, n \in \mathbb{Z}$. Then $\gcd(km, kn) = |k| \cdot \gcd(m, n)$.

PROOF: Left as exercise 6.24 on p.254. ■

6.12 Prime Numbers

Definition 6.16 (Prime numbers and prime factorizations)**.**

(a) Let $p \in \mathbb{N}, p \geq 2$. p is a **prime number** or p is **prime** if $q \in \mathbb{Z}$ and $q \mid p$ implies that $q = \pm 1$ or $q = \pm p$. We note that 1 is **not** prime.

(b) Let $p \in \mathbb{N}, p \geq 2$. p is called a **composite number** or just a **composite** if p is not prime.

(c) Let $m \in \mathbb{N}, m \geq 2$. If there are primes $p_1, \ldots, p_k$ such that $m = p_1 \cdot p_2 \cdots p_k$ then $p_1, \ldots, p_k$ are called **factors** or **prime factors** of m and $p_1 \cdot p_2 \cdots p_k$ is called a **prime factorization** or just a **factorization** of m.

(d) If the prime factorizations of $m, n \in \mathbb{N}$ both contain the prime number p then we call p a **common factor** of m and n.

(e) If $m \in \mathbb{Z}$ satisfies $m \leq -2$ and if $p_1 \cdot p_2 \cdots p_k$ is a prime factorization of the positive(!) integer $-m$ then we call $-(p_1 \cdot p_2 \cdots p_k)$ a prime factorization of m. □

Remark 6.16.

Note the following for the previous definition.

- no need for minus signs anywhere in part **(c)** since we assume that m is positive.
- It follows from Proposition 6.35 (B/G prop.6.29) on p.242 that $p \mid \gcd(m, n)$. □

Proposition 6.37 (B/G prop.6.28)**.**

Let $n \in \mathbb{N}$ such that $n > 1$. Then n has a prime factorization.

PROOF: The proof is left as exercise 6.20. See p.254.

Lemma 6.5.

Let p be prime and let $n \in \mathbb{N}$. We have the following:
(a) *Either $gcd(p, n) = 1$ or $gcd(p, n) = p$.*
(b) *If $p \nmid n$ (p does not divide n) then $gcd(p, n) = 1$.*

The proof is left as exercise 6.21 (see p.254). ■

Definition 6.17 (relatively prime)**.**

Let $m, n \in \mathbb{Z}$. We say that m and n are **relatively prime** if their greatest common divisor satisfies

$$\gcd(m, n) = 1. \ \square$$

Proposition 6.38.

Two natural numbers are relatively prime $\Leftrightarrow$ they possess no common factors.

PROOF: The proof is left as exercise 6.22 (see p.254). ■

Remark 6.17.

Lemma 6.5 above can now also be formulated this way: If p is prime and $n \in \mathbb{N}$ then
(a) Either p and n are relatively prime or $\gcd(p, n) = p$.
(b) If $p \nmid n$ then p and n are relatively prime.

We next look at Euclids Lemma and the unqueness of prime number factorizations. Thm.6.13 below states the following: Every integer ≥ 2 can be factored uniquely (i.e. up to permutation) into primes. The proof of that theorem requires Euclid's lemma which in turn uses lemma 6.5 above.

Proposition 6.39 (B/G prop.6.31: Euclid's Lemma for Two Factors)**.**

Let p be prime and $m, n \in \mathbb{N}$. If $p \mid (mn)$ then $p \mid m$ or $p \mid n$.

PROOF: The proof is left as exercise 6.25 (see p.254). ■

The generalization of Euclid's lemma to more than two factors is a straightforward proof by induction.

Proposition 6.40 (Euclid's Lemma for more than two factors)**.**

Let p be prime and $m_1, m_2, \ldots, m_k \in \mathbb{N}$. If $p \mid (m_1 m_2 \cdots m_k)$ then $p \mid m_j$ for some $1 \leq j \leq k$.

PROOF: Done by strong induction on the number of factors k.

Basis: There is nothing prove for $k = 1$ and prop.6.39 (Euclid's lemma for two factors) shows the validity for $k = 2$.

Induction assumption: We assume that if p divides a product $n = n_1 n_2 \cdots n_j$) of less than k factors then $p \mid n_i$ for some $1 \leq i \leq j$.

To prove that $p \mid m_i$ for some $1 \leq i \leq k$ we write $m_1 m_2 \cdots m_k = (m_1 m_2 \cdots m_{k-1}) m_k$. It follows from prop.6.39 that $p \mid m_k$ or $p \mid (m_1 m_2 \cdots m_{k-1})$. If p divides m_k then we are done. Otherwise we apply the induction assumption to the product $m_1 m_2 \cdots m_{k-1}$ of less than k factors and obtain that there is some $1 \leq i < k$ such that p divides m_i. ■

Theorem 6.13 (B/G thm 6.32: Uniqueness of prime factorizations)**.**

Every integer ≥ 2 can be factored uniquely (i.e., up to permutation) into primes.

PROOF: by strong induction on n.

Base case: $n = 2$: 2 is its own and obviously unique prime factorization.

Induction assumption: assume that if $2 \leq j < n$ then j has a unique PF (up to reordering).

We now show that n has a unique PF (up to reordering).

Case 1: n is prime: then n is the only and hence unique PF of itself.

Case 2: Else let $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ be two PFs for n. $p_1 \mid q_1 q_2 \cdots q_l$, hence $p_1 \mid q_{j_0}$ for some j_{j_0} by the generalized form of Euclid's lemma.

But then $p_1 = q_{j_0}$ because $p_1 \neq 1$ and q_{j_0} is the only integer bigger than 1 that divides the prime q_{j_0}.

Let us reorder the q_j in such a way that $j_0 = 1$. Then

$$n = p_1 n_2 \qquad \text{where} \qquad n_2 = p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l$$

is an integer less than n. It follows from the induction assumption that $q_2 \cdots q_l$ is just a reordering of $p_2 \cdots p_k$. ■

As an easy corollary of the uniqueness of prime factorizations up to the order in which they occur we obtain the following proposition which will be used in ch.**??** (Cardinality I: Finite and Countable Sets) to show the existence of a bijection $\mathbb{N} \to \mathbb{N}^2$.

Notation 6.1 ("The" prime factorization of an integer greater than 1)**.**

When we talk about prime factorizations of some $n \in [2, \infty[$ it usually does not matter in which order the prime factors of n occur. We will in such instances talk about **the** prime factorization of n. For example, We might say, "The prime factorization of n does not contain the number 2." □

Remark 6.18.
Let $m, n \in [2, \infty[_\infty$ and p prime. Let the prime factorizations of m and n be

$$m = p_1 \cdot p_2 \cdots p_i, \qquad n = q_1 \cdot q_2 \cdots q_j$$

for suitable $i, j \in \mathbb{N}$. The following are immediate consequences of the uniqueness of prime factorizations up to reordering of the factors.

(a) $p_1 \cdots p_i \cdot q_1 \cdots q_j$ is the prime factorization of $m \cdot n$.
(b) If p is a prime factor of m then $p = p_k$ for some suitable $1 \leq k \leq i$.
(c) It follows from **(b)** that if $p > p_k$ for each $1 \leq k \leq i$ then p is not a prime factor of m.
(d) If p is prime and $p \mid mn$ then p is a prime factor of mn. If p is not a prime factor of m then it follows from **(a)** that p is a prime factor of n. That is of course just a reformulation of Euclid's lemma, but note that we used the uniqueness of prime factorizations to deduce this. □

The next proposition essentially states the same as **(c)** above.

Proposition 6.41 (B/G Prop.6.33)**.**

Let $a, b \in \mathbb{N}$, and assume that $a \mid b$. Further, assume that p is a prime factor of b that is not a prime factor of a. Then $a \mid \frac{b}{p}$.

PROOF: The proof is left as exercise 6.26 (see p.254). ■

Proposition 6.42 (B/G Prop.6.34)**.**

Let p be a prime and $k \in \mathbb{N}$ such that $0 < k < p$. Then $p \mid \binom{p}{k}$.

PROOF:
Since $k! = 2 \cdot 3 \cdots k$, $(p-k)! = 2 \cdot 3 \cdots (p-k)$ and $(p-1)!$ are product of integers that belong to $[2, p-1[$, it follows from item **(b)** of the previous remark that p is not a prime factor of $k!(p-k)!$.

Obviously p divides $p! = \binom{p}{k} \cdot \big(k!(p-k)!\big)$ It follows from item **(c)** of that remark that p is a prime factor of $\binom{p}{k}$, in particular that $p \mid \binom{p}{k}$ ■

Since $\binom{p}{k} \cdot k! = p(p-1)\cdots(p-k+1)$, it follows that $p \,\big|\, \binom{p}{k} \cdot (k!)$.
Thus p is a prime factor of $\binom{p}{k}(k!)$. Since all prime factors of $k! = 1 \cdot 2 \cdots k$ are bounded by k and we assume $k < p$, the number p is not a prime factor of $k!$.
Hence p must be a prime factor of $\binom{p}{k}$. In particular, $p \mid \binom{p}{k}$. ■

Theorem 6.14 (Fermat's Little Theorem (B/G thm 6.35))**.**

If $m \in \mathbb{Z}$ and p is prime, then $m^p \equiv m \mod p$.

The proof is left as exercise **??** (see p.**??**). ■

Remark 6.19.
We note that if $p = 2$ then Fermat's Little Theorem states that either both m^2 and m have remainder zero (both are even) or both have remainder 1, i.e., both are odd. This is true according to prop.6.29 on p.236.

Proposition 6.43 (Corollary to Fermat's Little Theorem (B/G cor.6.36))**.**

Let p be prime and let $m \in \mathbb{N}$ such that $p \nmid m$. Then

$$m^{p-1} \equiv 1 \mod p.$$

The proof is left as exercise 6.23 (see p.254). ■

6.13 The Base–β Representation of the Integers

Introduction 6.2.
We have learned in school that any nonnegative integer n which is written as a string of digits $d_\mu d_{\mu-1} \ldots d_1 d_0$ represents the number $n = \sum_{j=0}^{\mu} d_j 10^j$. Example: $8375 = 5 \cdot 10^0 + 7 \cdot 10^1 + 3 \cdot 10^2 + 8 \cdot 10^3$. What is the difference between the 'string" or "word" 8375 and the mathematical expression $5 \cdot 10^0 + 7 \cdot 10^1 + 3 \cdot 10^2 + 8 \cdot 10^3$? None whatsoever for the mathematician who DEFINES the string $d_n d_{n-1} \ldots d_1 d_0$ of decimal digits d_j, i.e., integers between 0 and 9 (see Definition 6.1 on p.204), to be the integer $\sum_{j=0}^{n} d_j 10^j$.

Especially if you have done some programming you know that besides "base" 10 one also can expess n as a sum $n = \sum_{j=0}^{\mu} d_j \beta^j$ where the base β is an integer 2 or bigger and each d_j is now an integer between 0 and $\beta - 1$.

If $\beta = 2$, then each d_j is either zero or one, and one speaks of a binary representation. For example, the word 10001010 which we will write as $10001010_{(2)}$, i.e., we will tag it with the base in parentheses, is a binary representation of the integer

$$0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7$$

which equals the word $138_{(10)} = 8 \cdot 10^0 + 3 \cdot 10^1 + 1 \cdot 10^2$ when one chooses 10 as a base.

If $\beta = 16$, then $n = \sum_{j=0}^{\mu} d_j 16^j$ is the hexadecimal representation of n. Here each "hexadecimal digit" d_j is an integer between 0 and 15. It is customary to write the additionally needed hex digits as

$$A := 10,\ B := 11,\ C := 12,\ D := 13,\ E := 14,\ F := 15\,.^6$$

For example the word $(60)_{(10)}$ in base 10 becomes, since $60 = 3 \cdot 16 + 1 \cdot 12 = 3 \cdot 16^1 + C \cdot 16^0$, the word $3C_{(16)}$ in hexadecimal representation.

To show that, given a fixed base β, we can replace a nonegative integer n with its equivalent word of base β digits, we must do some work. First we must show that each for each such n there exists an index μ and base β digits $d_0, \ldots, d_\mu$ such that $n = \sum_{j=0}^{\mu} d_j \beta^j$ Second we must show that the association of n with $d_0 d_1 \ldots d_\mu$ is unique in the following sense: If $n = \sum_{j=0}^{\mu'} d'_j \beta^j$ yields a second collection of base β digits $d'_0, \ldots, d'_{\mu'}$ and if both representations are minimal, i.e., $d_\mu > 0$ and $d'_{\mu'} > 0$, then $\mu = \mu'$ and $d_j = d'_j$ for all $0 \le j \le \mu$.
We now set out to do that. □

Definition 6.18.

★ If $\beta \in \mathbb{Z}_{\ge 2}$ then we mean by a set of **base** β **digits** a set of $\beta - 1$ distinct symbols $\{d_i : i \in \mathbb{Z}, 0 \le i < \beta$ such that each d_i represents the integer i. □

Example 6.5.
When we talked above about hexadecimal representations, we had defined the hex digits as

$$\begin{cases} d_j := & \text{decimal digit for } j \in \mathbb{Z} \text{ if } 0 \le j \le 9, \\ d_{9+1} := & A,\ d_{9+2} := B,\ d_{9+3} := C,\ d_{9+4} := D,\ d_{9+5} := E,\ d_{9+6} := F. \end{cases}$$

No further digits are needed because $9 + 7 = \beta = 10_{(\beta)}$.
□

[6] To be picky, the right–hand sides of the equations of this line are base 10 representations $A = 10 = 9 + 1$, $B = 11 = 9 + 2$, etc.

Proposition 6.44 (B/G thm.7.7: Existence of base–β representations)**.**

Let $n \in \mathbb{N}$ and $\beta \in \mathbb{N}$ such that $\beta \geq 2$. Then there exists a nonnegative integer $\mu = \mu(n)$, and there exist integers d_j $(0 \leq j \leq \mu)$ such that $0 \leq d_j < \beta$ for each j and $d_\mu > 0$, and also

$$n = \sum_{j=0}^{\mu} d_j \beta^j. \tag{6.61}$$

PROOF: ⋆ The proof is done by strong induction on n.

Base case $n = 1$: Let $\mu = 0$ and $d_0 = 1$. Then $1 = d_0 \cdot \beta^0$. This proves the base case.

Induction assumption. If k is a natural number such that $k < n$ then there exists $\mu(k) \in \mathbb{Z}_{\geq 0}$ and integers c_j $\big(0 \leq j \leq \mu(k)\big)$ such that $0 \leq c_j < \beta$ for each j and $c_{\mu(k)} > 0$, and such that $k = \sum_{j=0}^{\mu(k)} c_j \beta^j$.

Step 1: The function $j \mapsto \beta^j$ is strictly increasing: If $i, j \in \mathbb{Z}_{\geq 0}$ and $i < j$ then $\beta^{j-i} \geq 2$, hence $\beta^i < (\beta^i)(\beta^{j-i}) = \beta^j$. Moreover it follows from exercise **??** on p.**??** that $\beta^n > n$ for $n \in \mathbb{Z}_{\geq 0}$.

All this implies that the set $A := \{j \in \mathbb{N} : \beta^j \leq n\}$ has n as an upper bound, hence it possesses a maximum $\mu := \max(A)$ (extended well–ordering principle). Clearly $\beta^\mu \leq n < \beta^{\mu+1}$. If $\beta^\mu = n$ then we have a representation (6.61) for n because we can choose $d_j = 0$ for $0 \leq j < \mu$ and $d_\mu = 1$. So we rule out this case and assume from now on that

$$\beta^\mu < n < \beta^{\mu+1}. \tag{6.62}$$

Step 2: Let $n' := n - \beta^\mu$. It follows from (6.62) that $n' \in \mathbb{N}$. Since $n' < n$ the induction assumption yields $\mu(n') \in \mathbb{Z}_{\geq 0}$ and integers a_j $\big(0 \leq j \leq \mu(n')\big)$ such that $0 \leq a_j < \beta$ for each j and $a_{\mu(n')} > 0$, and such that $n' = \sum_{j=0}^{\mu(n')} a_j \beta^j$.

Step 3: We show that $\mu(n') \leq \mu$. Otherwise we would have $\mu(n') \geq \mu + 1$. Since $a_{\mu(n')} \geq 1$,

$$n - \beta^\mu = n' = \sum_{j=0}^{\mu(n')} a_j \beta^j \geq 1 \cdot \beta^{\mu(n')} \geq \beta^{\mu+1} > n$$

(the last inequality results from (6.62)), and we would have reached a contradiction. If $\mu(n') \neq \mu$, i.e., $\mu(n') < \mu$, we define $\alpha_j = 0$ for $\mu(n') \leq j \leq \mu$. It follows that $n' = \sum_{j=0}^{\mu} a_j \beta^j$.

Step 4: We show that $a_\mu < \beta - 1$. Otherwise we would have

$$n - \beta^\mu = n' = \sum_{j=0}^{\mu} a_j \beta^j \geq (\beta - 1) \cdot \beta^\mu = \beta^{\mu+1} - \beta^\mu,$$

hence $n \geq \beta^{\mu+1}$, a contradiction to (6.62).

Step 5: It follows from $n - \beta^\mu = \sum_{j=0}^{\mu} a_j \beta^j$ and $a_\mu < \beta - 1$ that

$$n = (n - \beta^\mu) + \beta^\mu = \sum_{j=0}^{\mu} a_j \beta^j + \beta^\mu = \sum_{j=0}^{\mu} d_j \beta^j \quad \text{where } d_j = \begin{cases} a_j & \text{if } j < \mu, \\ a_j + 1 & \text{if } j = \mu. \end{cases}$$

Since $d_\mu = a_\mu + 1 \neq 0$ we have found a representation of the form (6.61) for n. ■

Remark 6.20. The proof of prop.6.44 shows that if $n = \sum_{j=0}^{K} d_j \beta^j$ then the maximal index i for a nonzero d_i is $i = \mu = \max\{j \in \mathbb{N} : \beta^j \leq n\}$. In other words, if $n < \beta^j$ then $d_j = 0$. □

Proposition 6.45 (B/G prop.7.9: Uniqueness of base–β representations)**.**

Let $n \in \mathbb{N}$ and $\beta \in \mathbb{N}$ such that $\beta \geq 2$. Assume that

$$n = \sum_{j=0}^{\mu} d_j \beta^j = \sum_{j=0}^{\mu'} d'_j \beta^j \tag{6.63}$$

where $\mu, \mu' \in \mathbb{Z}_{\geq 0}$, each d_i and each d'_i is a base β digit, $d_\mu \neq 0$ and $d'_{\mu'} \neq 0$.
Then $\mu = \mu'$ and $d_i = d'_i$ for all i.

PROOF: The proof is left as exercise 6.27 on p.**??**. ■

We learn at a very young age that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. For example, the number $3 \mid 2,784$ since $2 + 7 + 8 + 4$ is divisible by 3, and $3 \nmid 528$, since $5+2+8$ is not divisible by 3. We will prove this as an application of the base–10 Representation of the Integers.

Proposition 6.46 (B/G Prop.7.11)**.**

Let $n := \sum_{j=0}^{\mu} x_j 10^j$, where each x_j is a digit and $x_\mu \neq 0$. Then

$$n = x_0 + x_1 + \cdots + x_\mu \mod 3. \tag{6.64}$$

The proof is left as exercise 6.28 (see p.255). ■

6.14 The Addition Algorithm for Two Nonnegative Numbers (Base 10)

We give a simpler version of the addition algorithm than the one found in ch.7.2 of B/G.

Remark 6.21 (Addition subroutine)**.**
Given are

$$x := \sum_{n=0}^{K} x_n \cdot 10^n, \quad y := \sum_{n=0}^{K} y_n \cdot 10^n$$

in base–10 representation, i.e., x_n, y_n are digits $0, 1, 2 \ldots, 9$. We may choose the same ending index K for both x and y by "filling up" the number with less digits with leading zeros.

Here is the pseudocode for a subroutine, Add(n, x_n, y_n, z_n), whose task it is to compute the n–th digits z_n for the sum $z := \sum_{n=0}^{K+1} z_n \cdot 10^n \ := \ x + y$.

Subroutine Add($n, x_n, y_n, i_{n-1}, z_n, i_n$) :
//*
//* Inputs: n, x_n, y_n, i_{n-1}
//* Output: z_n, i_n
//*
If $n = 0$ then {
$i_{-1} := 0$;
}

$$i_n \ := \begin{cases} 0 & \text{if } x_n + y_n + i_{n-1} < 10 \\ 1 & \text{if } x_n + y_n + i_{n-1} \geq 10 \end{cases}$$

$$z_n \ := (x_n + y_n + i_{n-1}) \ - \ i_n \cdot 10$$

end-of-Subroutine

Note that the "sum digit" z_n and the "carry" i_n are associated with the "Euclidean division algorithm decomposition"

$$x_n + y_n + i_{n-1} \ = \ 10 \cdot q + r$$

for the integer $x_n + y_n + i_{n-1}$ as follows:

$$i_n = q \quad \text{and} \quad z_n = r. \ \square$$

6.15 Exercises for Ch.6

Exercise 6.1.

Prove prop.6.1 on p.204 of this document: If $i, j, n \in \mathbb{Z}$ and $A_i \ = \ \{k \in \mathbb{Z} : k \geq i\}$ then $n + i \in A_i \ \Leftrightarrow \ n + j \in A_j$. $\square$

Exercise 6.2.

Prove prop.6.12 on p.215 of this document: If $n \in \mathbb{N}$ then $e(n) \in P$. $\square$

Exercise 6.3.

Prove the following part of prop.6.13 on p.215 of this document:

Let $m, n \in \mathbb{N}$. Then $e(n) \prec e(m) \ \Rightarrow \ n < m$. $\square$

Exercise 6.4.

Let $x_0 = 8, \ x_1 = 16, \ x_{n+1} = 6x_{n-1} - x_n$ for $n \in \mathbb{N}$. Prove that $x_n = 2^{n+3}$ for every integer $n \geq 0$. Hint: Use strong induction. $\square$

Exercise 6.5.

Prove parts **(b)** and **(c)** of prop.6.18 on p.221 of this document:

Let $\beta \in \mathbb{Z}$ and $k, m \in \mathbb{Z}_{\geq 0}$. Then

(b) $\beta^m \odot \beta^k = \beta^{m+k}$,

(c) $(\beta^m)^k = \beta^{mk}$. □

Exercise 6.6.

Prove prop.6.19 on p.221 of this document: Let $a \in R$ such that $0 \leq a \leq 1$, and let $m, n \in \mathbb{N}$ such that $m \geq n$. Then $a^m \leq a^n$. □

Exercise 6.7.

Let $R = (R, \oplus, \odot, P)$ be an ordered integral domain, let $n \in [2, \infty[_{\mathbb{Z}}$, and let $x_j \in R$ for $j \in \mathbb{N}$. Prove by induction that

$$\prod_{j=1}^{n} |x_j| = \left| \prod_{j=1}^{n} x_j \right|.$$

You may use that: for any two $x, y \in R$ it is true that $|a| \odot |b| = |a \odot b|$. □

Exercise 6.8.

Prove prop.6.21 on p.222 of this document:

Let $q \in \mathbb{Z}$. If $n \in \mathbb{Z}_{\geq 0}$ then $(1 - q) \sum_{j=0}^{n} q^j = 1 - q^{n+1}$.

Hint: Prove the case $q \neq 1$ by induction on n. □

Exercise 6.9.

Let $R \subseteq \mathbb{Z}^2$ be the divisibility relation on $\mathbb{Z}$: $mRn \Leftrightarrow m \mid n$.

(a) Prove that R is reflexive and transitive.

(b) Prove that R is not antisymmetric (and hence not a partial order relation) by finding two different integers m, n such that $m|n$ and $n|m$. □

Exercise 6.10.

Prove Theorem 6.4 on p.208 of this document: If $k \in \mathbb{N}$ then $k \geq 1$. □

Exercise 6.11.

Prove prop.6.9 on p.211 of this document: Let $m, n \in \mathbb{N}$. If $m \mid n$ then $m \leq n$ □

Exercise 6.12.

Prove prop.6.2 on p.208 of this document: There exists no $x \in \mathbb{Z}$ such that $0 < x < 1$. □

Exercise 6.13.

Prove cor.6.2 on p.208 of this document: If $n \in \mathbb{Z}$ then there exists no $x \in \mathbb{Z}$ such that $n < x < n+1$. □

Exercise 6.14.

Prove prop.6.8 on p.211: Let $n \in \mathbb{N}$. Then $n^2 + 1 > n$. Try to prove this with and without the use of induction. □

Exercise 6.15.

Let $a \in \mathbb{Z}$. Prove that there exists $b \in]-\infty, 0[$ such that $b < a$, i.e., there are no lower bounds for $]-\infty, 0[$ in $\mathbb{Z}$. Do so without making use of prop.6.25 ....

Hint: ..... But base your proof on that of prop.6.25. □

Exercise 6.16.

Prove prop.6.11 on p.235 of this document: Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ Then there exists a unique pair of integers q and r such that

$$m = qn + r \qquad \text{and} \qquad 0 \leq r < n.$$

(a) Prove uniqueness of the "decomposition" $m = qn + r$: If you have a second such decomposition $m = \tilde{q}n + \tilde{r}$ then show that this implies $q = \tilde{q}$ and $r = \tilde{r}$. Start by assuming that $r \neq \tilde{r}$ which means that one of them is smaller than the other and take it from there.

(b) Prove the existence of q and r. This is much harder than **(a)**.

Hint for **(b)**: Review the extended well–ordering principle (thm.6.10 on p.233). Its use will give the easiest way to prove this theorem. Apply it to the set

$$A := A(m, n) := \{x \in \mathbb{Z}_{\geq 0} : x = m - kn \text{ for some } k \in \mathbb{Z}\}$$

. Hint for both **(a)** and **(b)**: Prop.**??** and cor.**??** on p.**??** from ch.**??** (Minima, Maxima, Infima and Suprema in Ordered Integral Domains) in their formulation for $(R, \oplus, \odot, P) = (\mathbb{Z}, +, \cdot, \mathbb{N})$ will come in handy in connection with the condition $0 \leq r < n$. □

Exercise 6.17.

Prove prop.6.27 on p.235 of this document:

Any product of odd numbers is odd.

Hint: Use induction on k to prove that the product $n_1 n_2 \cdots n_k$ of k odd numbers x_j is odd. □

Exercise 6.18.

Prove Theorem 6.12 on p.240 of this document:

(a) The operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ of Definition 6.14 above turn $(\mathbb{Z}_n, \oplus, \odot)$ into a commutative ring with unit.

(b) $(\mathbb{Z}_n, \oplus, \odot)$ is an integral domain, i.e., there are no zero divisors, if and only if n is prime. □

Exercise 6.19.

Prove lemma 6.3 on p.241 of this document: For $m, n \in \mathbb{Z}$ let

$$S := S(m, n) := \{k \in \mathbb{N} : k = mx + ny \text{ for some } x, y, \in \mathbb{Z}\}.$$

Then S is empty if and only if $m = n = 0$.

Hint: The difficult part is proving that S is not empty if at least one of m, n is not zero. What does S look like if $m = 0$ and $n \neq 0$? Do that case first, then do the case where both m and n are not zero. Play around with specific number to see what happens before you attempt to do the proof. □

Exercise 6.20.

Prove prop.6.37 on p.244: Any integer ≥ 2 has a prime factorization. $\square$

Exercise 6.21.

Prove lemma 6.5 on p.244 of this document: Let p be prime and let $n \in \mathbb{N}$. We have the following:

(a) Either $\gcd(p, n) = 1$ or $\gcd(p, n) = p$.

(b) If $p \nmid n$ (p does not divide n) then $\gcd(p, n) = 1$. $\square$

Exercise 6.22.

Prove that two natural numbers m and n are relatively prime if and only if they possess no common factors: $\square$

Exercise 6.23.

Prove prop.6.43 on p.247 of this document: Let p be prime and let $m \in \mathbb{N}$ such that $p \nmid m$. Then $m^{p-1} \equiv 1 \mod p$.

Hint: Modify the problem so that you can apply Fermat's Little Theorem to it. $\square$

Exercise 6.24.

Prove prop.6.36 on p.243 of this document:

Let $k, m, n \in \mathbb{Z}$. Then $\gcd(km, kn) = |k| \cdot \gcd(m, n)$.

Hint: You must distinguish the cases where $S(m, n)$ and/or $S(km, kn)$ is empty from the others, and you want to work with nonnegative k, m, n as much as possible. Do the following cases in the sequence given:

Case 1: $k = 0$ • **Case 2:** $m = n = 0$ • **Case 3:** $m \geq 0, n \geq 0$. At least one of $m, n \neq 0$, $k > 0$ • **Case 4:** $k < 0$, at least one of $m, n \neq 0$.

Cases 1 and 2 are trivial

For case 3 abbreviate $g := \gcd(m, n)$, $g' := \gcd(km, kn)$, $S := S(m, n), S' := S(km, kn)$.

(i) Show that $kg \in S'$ and use that to prove that $g \leq kg'$.

(ii) Show that there exists $z \in S$ such that $g' = kz$. Use that to prove that $g \geq kg'$.

It is easy to prove case 4 using case 3 and lemma 6.4**(c)**: $S(a, b) = S(|a|, |b|)$. $\square$

Exercise 6.25.

Prove prop.6.39 on p.244 of this document: Let p be prime and $m, n \in \mathbb{N}$. If $p \mid (mn)$ then $p \mid m$ or $p \mid n$. $\square$

Exercise 6.26.

Prove prop.6.41 on p.246 of this document: Let $a, b \in \mathbb{N}$, and assume that $a \mid b$. Assume that p is a prime factor of b that is not a prime factor of a. Then $a \mid \frac{b}{p}$. $\square$

Exercise 6.27.

Prove prop.6.45 on p.250:

Let $n \in \mathbb{N}$ and $\beta \in \mathbb{N}$ such that $\beta \geq 2$. Assume that $n = \sum_{j=0}^{\mu} d_j \beta^j = \sum_{j=0}^{\mu'} d'_j \beta^j$ where $\mu, \mu' \in \mathbb{Z}_{\geq 0}$, each d_i and each d'_i is a base β digit, $d_\mu \neq 0$ and $d'_{\mu'} \neq 0$. Then $\mu = \mu'$ and $d_i = d'_i$ for all i. $\square$

Exercise 6.28.

Prove prop.6.46 on p.250 of this document: Let $n := \sum_{j=0}^{\mu} x_j 10^j$, where each x_j is a digit and $x_\mu \neq 0$. Then $n = x_0 + x_1 + \cdots + x_{\nu(n)-1} \mod 3$. $\square$

6.16 Blank Page after Ch.6

This page is intentionally left blank.

References

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

[2] John P. D'Angelo and Douglas B. West. Mathematical Thinking: Problem-Solving and Proofs - Pearson Modern
Pearson, 2nd edition, 2018.

List of Symbols

Index