University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 0

Darij Grinberg

April 6, 2021

1 Exercise 1: Geometric series and a bit more

1.1 Problem

Let $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$. Prove that the equalities

$$\begin{aligned} &(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+ab^{n-2}+b^{n-1}\right) \\ &= a^n - b^n \end{aligned} \tag{1}$$

and

$$\begin{aligned} &(a-b)^2\left(1a^{n-1}+2a^{n-2}b+3a^{n-3}b^2+\cdots+(n-1)\,ab^{n-2}+nb^{n-1}\right) \\ &= a^{n+1} - (n+1)\,ab^n + nb^{n+1} \end{aligned} \tag{2}$$

hold for each $n \in \mathbb{N}$.

(Here and in the following, $\mathbb{N}$ stands for the set $\{0,1,2,\ldots\}$. We also recall that empty sums – i.e., sums that have no addends at all – evaluate to 0 by definition. This applies, in particular, to the sums $a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+ab^{n-2}+b^{n-1}$ and $1a^{n-1}+2a^{n-2}b+3a^{n-3}b^2+\cdots+(n-1)\,ab^{n-2}+nb^{n-1}$ in the case when $n=0$.)

1.2 Remark

A consequence of the formulas (1) and (2) is that every rational number $x \neq 1$ satisfies

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x} \qquad \text{and}$$
$$1 + 2x + 3x^2 + \cdots + nx^{n-1} = \frac{1 - (n+1)\,x^n + nx^{n+1}}{(1-x)^2}.$$

Indeed, these equalities follow by setting $a = 1$ and $b = x$ in the equalities (1) and (2) and dividing by $1 - x$ or $1 - x^2$, respectively.

More generally, the formulas (1) and (2) remain true when a and b are two commuting elements of an arbitrary ring (we will later learn what this means; for now, let us just say that, e.g., we could let a and b be two commuting matrices instead of rational numbers).

1.3 Solution

We will use the summation sign when we solve this exercise. This will make our formulas both shorter and clearer. For example, instead of "$1a^{n-1} + 2a^{n-2}b + 3a^{n-3}b^2 + \cdots + (n-1)\,ab^{n-2} + nb^{n-1}$", it will let us just write "$\sum_{k=1}^{n} ka^{n-k}b^{k-1}$".

Let us give a crash course on the use of the summation sign. We refer to [Grinbe19, Section 1.4] for details and further information[1].

- Assume that S is a finite set, and that a_s is a number (e.g., a real number) for each $s \in S$. Thus you have $|S|$ many numbers a_s in total. Then, $\sum_{s \in S} a_s$ shall denote the sum of all of these $|S|$ many numbers. For example,

$$\sum_{s \in \{2,5,6\}} s^3 = 2^3 + 5^3 + 6^3$$

(here, $S = \{2,5,6\}$ and $a_s = s^3$ for each $s \in S$) and

$$\sum_{s \in \{5,7,9,11\}} \frac{1}{s} = \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11}$$

(here, $S = \{5,7,9,11\}$ and $a_s = \dfrac{1}{s}$ for each $s \in S$).

The letter s here plays the same role as the letter s in "$\{s^2 \mid s \in \{2,3,4\}\}$" or in "the function that sends each integer s to $s^2 - 1$"; it designates the "moving part" in a definition (it is what is called a "bound variable" or a "running index"). You don't have to use the specific letter s for it; you can use any other letter instead (as long as it does not already have a different meaning) and get the same result. For example, the sum $\sum_{s \in \{2,5,6\}} s^3$ can be rewritten as $\sum_{i \in \{2,5,6\}} i^3$ or as $\sum_{\mathfrak{G} \in \{2,5,6\}} \mathfrak{G}^3$. When the set S is empty (so you have no numbers a_s at all), the sum $\sum_{s \in S} a_s$ is defined to be 0; this is called an *empty sum*.

[1] and to [Grinbe19, Section 2.14] for proofs of well-definedness and basic properties

- Assume that u and v are two integers, and that a_s is a number (e.g., a real number) for each $s \in \{u, u+1, \ldots, v\}$. (When $u > v$, we understand the set $\{u, u+1, \ldots, v\}$ to be empty – it does not contain any "anti-integers" either.) Then, $\sum_{s=u}^{v} a_s$ is just a shorthand for the sum $\sum_{s \in \{u, u+1, \ldots, v\}} a_s$. This sum can also be written as $a_u + a_{u+1} + \cdots + a_v$, but this notation presumes the reader to guess what the "general term" a_s looks like. For example,

$$\sum_{s=5}^{10} s^s = 5^5 + 6^6 + 7^7 + 8^8 + 9^9 + 10^{10} = 5^5 + 6^6 + \cdots + 10^{10}$$

(arguably, guessing the general term is easy here, but look at the sum in (2)). For another example,

$$\sum_{s=-2}^{2} s^2 = (-2)^2 + (-1)^2 + 0^2 + 1^2 + 2^2.$$

- Expressions of the form $\sum_{s \in S} a_s$ and $\sum_{s \in \{u, u+1, \ldots, v\}} a_s$ are called "finite sums", and the $\sum$ symbol is called the "summation sign".

- Finite sums satisfy the rules that you would expect. For example, assume that a finite set S is written as a union of two disjoint subsets A and B (so each element of S belongs to one of A and B, but not to both). Assume that a_s is a number for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{s \in A} a_s + \sum_{s \in B} a_s.$$

For example, if $S = \{1, 2, \ldots, 2n\}$ for some $n \in \mathbb{N}$, and if

$$A = \{\text{the even elements of } S\} = \{2, 4, 6, \ldots, 2n\} \qquad \text{and}$$
$$B = \{\text{the odd elements of } S\} = \{1, 3, 5, \ldots, 2n-1\},$$

then this formula becomes

$$a_1 + a_2 + \cdots + a_{2n} = (a_2 + a_4 + a_6 + \cdots + a_{2n}) + (a_1 + a_3 + a_5 + \cdots + a_{2n-1}).$$

This is exactly what you would expect: To sum the $2n$ numbers $a_1, a_2, \ldots, a_{2n}$, you can first split them into the "even" and the "odd" ones (to be pedantic: rather, the ones with the even subscripts and the ones with the odd subscripts), and separately sum the former and the latter, and subsequently add the two small sums together. See [Grinbe19, Section 1.4.2] for this and several other rules (and for their rigorous proofs, if you are that skeptical). You can use all these rules without saying, except for the "telescoping sums" rule (which you should cite by name when you apply it). For lots of practice with sums, see [GrKnPa94, Chapter 2 and further].

- The "product sign" $\prod$ is analogous to the summation sign $\sum$, but stands for products instead of sums. For example,

$$\prod_{s=5}^{10} s^s = 5^5 \cdot 6^6 \cdot 7^7 \cdot 8^8 \cdot 9^9 \cdot 10^{10} = 5^5 \cdot 6^6 \cdot \cdots \cdot 10^{10}.$$

An empty product (i.e., a product of the form $\prod_{s \in S} a_s$ when S is empty) is defined to be 1. See [Grinbe19, Section 1.4.4] for the properties of products.

The summation sign lets us rewrite the sum $a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+ab^{n-2}+b^{n-1}$ in (1) as $\sum\limits_{k=1}^{n} a^{n-k}b^{k-1}$, and lets us rewrite the sum $1a^{n-1}+2a^{n-2}b+3a^{n-3}b^2+\cdots+(n-1)\,ab^{n-2}+nb^{n-1}$ in (2) as $\sum\limits_{k=1}^{n} ka^{n-k}b^{k-1}$. So the two equalities (1) and (2) rewrite as

$$(a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1} = a^n - b^n \tag{3}$$

and

$$(a-b)^2\sum_{k=1}^{n} ka^{n-k}b^{k-1} = a^{n+1} - (n+1)\,ab^n + nb^{n+1}, \tag{4}$$

respectively. It is in these forms that we will prove these equalities.

- *Proof of* (3)*:*

  We shall prove (3) by induction on n:

  Induction base: Comparing the equalities $a^0 - b^0 = 1 - 1 = 0$ and

  $$(a-b)\underbrace{\sum_{k=1}^{0} a^{0-k}b^{k-1}}_{=(\text{empty sum})=0} = (a-b)\,0 = 0,$$

  we obtain

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

  In other words, (3) holds for $n = 0$. Thus the induction base is complete.

  Induction step: Let $m \in \mathbb{N}$. Assume that (3) holds for $n = m$. We must prove that (3) holds for $n = m+1$.

  We have assumed that (3) holds for $n = m$. In other words, we have

  $$(a-b)\sum_{k=1}^{m} a^{m-k}b^{k-1} = a^m - b^m. \tag{5}$$

  Now, splitting off the last addend of the sum $\sum\limits_{k=1}^{m+1} a^{(m+1)-k}b^{k-1}$, we obtain

  $$\begin{aligned}\sum_{k=1}^{m+1} a^{(m+1)-k}b^{k-1} &= \sum_{k=1}^{m} \underbrace{a^{(m+1)-k}}_{\substack{=a^{m-k+1}\\=aa^{m-k}}} b^{k-1} + \underbrace{a^{(m+1)-(m+1)}}_{=a^0=1}\underbrace{b^{(m+1)-1}}_{=b^m} \\ &= \sum_{k=1}^{m} aa^{m-k}b^{k-1} + b^m = a\sum_{k=1}^{m} a^{m-k}b^{k-1} + b^m,\end{aligned}$$

so that

$$\begin{aligned}
&(a-b)\sum_{k=1}^{m+1} a^{m+1-k}b^{k-1} \\
&= (a-b)\left(a\sum_{k=1}^{m} a^{m-k}b^{k-1} + b^m\right) \\
&= a\underbrace{(a-b)\sum_{k=1}^{m} a^{m-k}b^{k-1}}_{\substack{=a^m-b^m \\ \text{(by (5))}}} + (a-b)\,b^m = a\left(a^m-b^m\right) + (a-b)\,b^m \\
&= aa^m - ab^m + ab^m - bb^m = \underbrace{aa^m}_{=a^{m+1}} - \underbrace{bb^m}_{=b^{m+1}} = a^{m+1} - b^{m+1}.
\end{aligned}$$

In other words, (3) holds for $n = m+1$. This completes the induction step. Thus, (3) is proven.

- *Proof of* (4)*:*

  We shall prove (4) by induction on n:

  Induction base: Comparing the equalities $a^{0+1} - (0+1)\,ab^0 + 0b^{0+1} = a^1 - a = a - a = 0$ and

$$(a-b)^2 \underbrace{\sum_{k=1}^{0} ka^{0-k}b^{k-1}}_{=(\text{empty sum})=0} = (a-b)^2\,0 = 0,$$

  we obtain

$$(a-b)^2 \sum_{k=1}^{0} ka^{0-k}b^{k-1} = a^{0+1} - (0+1)\,ab^0 + 0b^{0+1}.$$

  In other words, (4) holds for $n = 0$. Thus the induction base is complete.

  Induction step: Let $m \in \mathbb{N}$. Assume that (4) holds for $n = m$. We must prove that (4) holds for $n = m+1$.

  We have assumed that (4) holds for $n = m$. In other words, we have

$$(a-b)^2 \sum_{k=1}^{m} ka^{m-k}b^{k-1} = a^{m+1} - (m+1)\,ab^m + mb^{m+1}. \tag{6}$$

  Now, splitting off the last addend of the sum $\sum_{k=1}^{m+1} ka^{(m+1)-k}b^{k-1}$, we obtain

$$\begin{aligned}
\sum_{k=1}^{m+1} ka^{(m+1)-k}b^{k-1} &= \sum_{k=1}^{m} k\underbrace{a^{(m+1)-k}}_{\substack{=a^{m-k+1} \\ =aa^{m-k}}}b^{k-1} + (m+1)\underbrace{a^{(m+1)-(m+1)}}_{=a^0=1}\underbrace{b^{(m+1)-1}}_{=b^m} \\
&= \sum_{k=1}^{m} kaa^{m-k}b^{k-1} + (m+1)\,b^m = a\sum_{k=1}^{m} ka^{m-k}b^{k-1} + (m+1)\,b^m,
\end{aligned}$$

so that

$$
\begin{aligned}
&(a-b)^2 \sum_{k=1}^{m+1} k a^{m+1-k} b^{k-1} \\
&= (a-b)^2 \left(a \sum_{k=1}^{m} k a^{m-k} b^{k-1} + (m+1)\, b^m \right) \\
&= a \underbrace{(a-b)^2 \sum_{k=1}^{m} k a^{m-k} b^{k-1}}_{\substack{=a^{m+1}-(m+1)ab^m+mb^{m+1} \\ \text{(by (6))}}} + (a-b)^2 (m+1)\, b^m \\
&= a\left(a^{m+1} - (m+1)\, ab^m + mb^{m+1}\right) + (a-b)^2 (m+1)\, b^m \\
&= \underbrace{aa^{m+1}}_{=a^{m+2}} - (m+1) \underbrace{aa}_{=a^2} b^m + mab^{m+1} + \underbrace{(a-b)^2}_{=a^2-2ab+b^2} (m+1)\, b^m \\
&= a^{m+2} - (m+1)\, a^2 b^m + mab^{m+1} + \left(a^2 - 2ab + b^2\right)(m+1)\, b^m \\
&= a^{m+2} - (m+1)\, a^2 b^m + mab^{m+1} + (m+1)\, a^2 b^m - 2(m+1)\, abb^m + (m+1)\, b^2 b^m \\
&= a^{m+2} + mab^{m+1} - 2(m+1)\, a \underbrace{bb^m}_{=b^{m+1}} + (m+1) \underbrace{b^2 b^m}_{=b^{m+2}} \\
&= a^{m+2} + \underbrace{mab^{m+1} - 2(m+1)\, ab^{m+1}}_{\substack{=(m-2(m+1))ab^{m+1} \\ =-(m+2)ab^{m+1}}} + (m+1)\, b^{m+2} \\
&= a^{m+2} - (m+2)\, ab^{m+1} + (m+1)\, b^{m+2} \\
&= a^{(m+1)+1} - ((m+1)+1)\, ab^{m+1} + (m+1)\, b^{(m+1)+1}.
\end{aligned}
$$

In other words, (4) holds for $n = m+1$. This completes the induction step. Thus, (4) is proven.

So the exercise is solved.

1.4 Remark

The equality (3) can also be proved using the telescope principle; see [Grinbe19, (18)] for this argument.

---

2 Exercise 2: Factorials 101

2.1 Problem

Recall that the *factorial* of a nonnegative integer n is defined by

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n.$$

Thus, in particular, $0! = 1$ (since we defined empty products to be 1); it is easy to see that

$$1! = 1, \qquad 2! = 2, \qquad 3! = 6, \qquad 4! = 24, \qquad 5! = 120, \qquad 6! = 720, \qquad 7! = 5040.$$

This sequence grows very fast (see Stirling's approximation).

Prove the following properties of factorials:

(a) We have $n! = n \cdot (n-1)!$ for each positive integer n.

(b) For each $n \in \mathbb{N}$, we have

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1.$$

(c) For each $n \in \mathbb{N}$, we have

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) = \frac{(2n)!}{2^n n!}.$$

(Here, the left hand side is understood to be the product of the first n odd positive integers, i.e., the product $\prod_{i=1}^{n} (2i-1)$.)

2.2 Solution

(a) Let n be a positive integer. Thus, $n \in \{1, 2, \ldots, n\}$. The definition of $(n-1)!$ yields

$$(n-1)! = \prod_{i=1}^{n-1} i. \tag{7}$$

But the definition of $n!$ yields

$$n! = \prod_{i=1}^{n} i = \left(\prod_{i=1}^{n-1} i \right) \cdot n$$

(here, we have split off the factor for $i = n$ from the product, since $n \in \{1, 2, \ldots, n\}$). Hence,

$$n! = \underbrace{\left(\prod_{i=1}^{n-1} i \right)}_{\substack{=(n-1)! \\ \text{(by (7))}}} \cdot n = (n-1)! \cdot n = n\,(n-1)!.$$

This solves part **(a)** of the exercise.

(b) Claims like this can often be proven in two ways: by (fairly straightforward) induction, and by (usually tricky) transformations. In this particular case, the two proofs are actually very similar, and can easily be transformed into one another; nevertheless, let us show both of them.

Proof by induction: We shall prove the claim of part **(b)** by induction on n:

Induction base: We have

$$1 \cdot 1! + 2 \cdot 2! + \cdots + 0 \cdot 0! = (\text{empty sum}) = 0.$$

Comparing this with $\underbrace{(0+1)!}_{=1!=1} - 1 = 1 - 1 = 0$, we obtain $1 \cdot 1! + 2 \cdot 2! + \cdots + 0 \cdot 0! = (0+1)! - 1$. Thus, the claim of part **(b)** holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that the claim of part **(b)** holds for $n = m$. We must prove that the claim of part **(b)** holds for $n = m + 1$.

We have assumed that the claim of part **(b)** holds for $n = m$. In other words, we have

$$1 \cdot 1! + 2 \cdot 2! + \cdots + m \cdot m! = (m+1)! - 1.$$

Now,

$$\begin{aligned}
&1 \cdot 1! + 2 \cdot 2! + \cdots + (m+1) \cdot (m+1)! \\
&= \underbrace{(1 \cdot 1! + 2 \cdot 2! + \cdots + m \cdot m!)}_{=(m+1)!-1} + (m+1) \cdot (m+1)! \\
&= (m+1)! - 1 + (m+1) \cdot (m+1)! \\
&= \underbrace{(1 + (m+1))}_{=m+2} \cdot (m+1)! - 1 \\
&= (m+2) \cdot (m+1)! - 1. \qquad (8)
\end{aligned}$$

But part **(a)** of this exercise (applied to $n = m+2$) yields

$$(m+2)! = (m+2) \cdot \left(\underbrace{(m+2) - 1}_{=m+1} \right)! = (m+2) \cdot (m+1)!.$$

Hence, (8) becomes

$$1 \cdot 1! + 2 \cdot 2! + \cdots + (m+1) \cdot (m+1)! = \underbrace{(m+2) \cdot (m+1)!}_{\substack{=(m+2)! \\ =((m+1)+1)!}} - 1 = ((m+1)+1)! - 1.$$

In other words, the claim of part **(b)** holds for $n = m+1$. This completes the induction step. Thus, the claim of part **(b)** is proven by induction.

Proof by tricky transformations: This proof shall rely on the following fact:

Proposition 2.1. *Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ real numbers[2]. Then,*

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = a_m - a_0.$$

Proposition 2.1 is known as the "telescope principle" since it contracts the sum $\sum_{i=1}^{m} (a_i - a_{i-1})$ to the single difference $a_m - a_0$, like folding a telescope.

The simplest way to convince yourself that Proposition 2.1 is true is by expanding the left hand side:

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = (a_1 - a_0) + (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_m - a_{m-1})$$

and watching all the terms cancel each other out except for the $-a_0$ and the a_m. More formally, this argument can be emulated by an induction on m. See [18f-hw0s, proof of Proposition 2.2] or [Grinbe19, proof of (16)] for formal proofs of Proposition 2.1.

[2] I am saying "real numbers" just for the sake of saying something definite. You could just as well state this principle for "complex numbers" or "rational numbers" or (once we have learnt what an abelian group is) "elements of an abelian group (where the operation of the group is written as addition)"; the proof will be the same in each case.

Now, how can we apply Proposition 2.1 to part **(b)** of the exercise? We have $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = \sum_{i=1}^{n} i \cdot i!$. If we could write each addend $i \cdot i!$ in the form $a_i - a_{i-1}$ for some $n+1$ real numbers $a_0, a_1, \ldots, a_n$, then we could use Proposition 2.1.

The tricky part is finding these a_i. Namely, set $a_i = (i+1)!$ for each $i \in \{0, 1, \ldots, n\}$. Then, I claim that

$$i \cdot i! = a_i - a_{i-1} \qquad \text{for each } i \in \{1, 2, \ldots, n\}. \tag{9}$$

The *proof of* (9) is not tricky at all: Let $i \in \{1, 2, \ldots, n\}$. Then, part **(a)** of the exercise (applied to $i+1$ instead of n) yields

$$(i+1)! = (i+1) \cdot \left(\underbrace{(i+1)-1}_{=i} \right)! = (i+1) \cdot i! = i \cdot i! + i!.$$

Solving this for $i \cdot i!$, we find

$$i \cdot i! = (i+1)! - i!.$$

Comparing this with

$$\underbrace{a_i}_{\substack{=(i+1)! \\ \text{(by the definition of } a_i\text{)}}} - \underbrace{a_{i-1}}_{\substack{=((i-1)+1)! \\ \text{(by the definition of } a_{i-1}\text{)}}} = (i+1)! - \left(\underbrace{(i-1)+1}_{=i} \right)! = (i+1)! - i!,$$

we obtain $i \cdot i! = a_i - a_{i-1}$. This proves (9).

Now,

$$\begin{aligned}
&1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! \\
&= \sum_{i=1}^{n} \underbrace{i \cdot i!}_{\substack{=a_i - a_{i-1} \\ \text{(by (9))}}} = \sum_{i=1}^{n} (a_i - a_{i-1}) \\
&= \underbrace{a_n}_{\substack{=(n+1)! \\ \text{(by the definition of } a_n\text{)}}} - \underbrace{a_0}_{\substack{=(0+1)! \\ \text{(by the definition of } a_0\text{)}}} \qquad \text{(by Proposition 2.1, applied to } m = n\text{)} \\
&= (n+1)! - \underbrace{(0+1)!}_{=1!=1} = (n+1)! - 1.
\end{aligned}$$

This solves part **(b)** of the exercise again.

(c) Again, we give two proofs:

Proof by induction: We shall prove the claim of part **(c)** by induction on n:

Induction base: We have

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2 \cdot 0 - 1) = (\text{empty product}) = 1.$$

Comparing this with $\dfrac{(2 \cdot 0)!}{2^0 0!} = \dfrac{0!}{1 \cdot 0!} = 1$, we obtain $1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2 \cdot 0 - 1) = \dfrac{(2 \cdot 0)!}{2^0 0!}$. Thus, the claim of part **(c)** holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that the claim of part **(c)** holds for $n = m$. We must prove that the claim of part **(c)** holds for $n = m + 1$.

We have assumed that the claim of part **(c)** holds for $n = m$. In other words, we have

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2m-1) = \frac{(2m)!}{2^m m!}. \tag{10}$$

Our goal is to show that

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2(m+1)-1) = \frac{(2(m+1))!}{2^{m+1}(m+1)!}. \tag{11}$$

We start by rewriting the factorials on the right hand side of this alleged equality in terms of the factorials in (10). Clearly, $2(m+1)$ is a positive integer. Hence, part **(a)** of the exercise (applied to $n = 2(m+1)$) yields

$$\begin{aligned}
(2(m+1))! &= 2(m+1) \cdot \left(\underbrace{2(m+1)-1}_{=2m+1} \right)! = 2(m+1) \cdot \underbrace{(2m+1)!}_{\substack{=(2m+1)\cdot((2m+1)-1)! \\ \text{(by part (a) of the exercise,} \\ \text{applied to } n=2m+1)}} \\
&= 2(m+1) \cdot (2m+1) \cdot \left(\underbrace{(2m+1)-1}_{=2m} \right)! \\
&= 2(m+1) \cdot (2m+1) \cdot (2m)!.
\end{aligned} \tag{12}$$

Also, part **(a)** of the exercise (applied to $n = m+1$) yields

$$(m+1)! = (m+1) \cdot \left(\underbrace{(m+1)-1}_{=m} \right)! = (m+1) \cdot m!. \tag{13}$$

Plugging the two equalities (12) and (13) as well as the obvious equality $2^{m+1} = 2 \cdot 2^m$ into the expression $\dfrac{(2(m+1))!}{2^{m+1}(m+1)!}$, we obtain

$$\frac{(2(m+1))!}{2^{m+1}(m+1)!} = \frac{2(m+1) \cdot (2m+1) \cdot (2m)!}{(2 \cdot 2^m)(m+1) \cdot m!} = \frac{(2m)!}{2^m m!} \cdot (2m+1).$$

Comparing this with

$$\begin{aligned}
1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2(m+1)-1) &= \underbrace{(1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2m-1))}_{\substack{=\dfrac{(2m)!}{2^m m!} \\ \text{(by (10))}}} \cdot \left(\underbrace{2(m+1)-1}_{=2m+1} \right) \\
&= \frac{(2m)!}{2^m m!} \cdot (2m+1),
\end{aligned}$$

we obtain precisely the equality (11) that we were trying to prove. In other words, the claim of part **(c)** holds for $n = m+1$. This completes the induction step. Thus, the claim of part **(c)** is proven by induction.

Proof by tricky transformations: Let $n \in \mathbb{N}$. This time, the trick is to split the product $(2n)! = 1 \cdot 2 \cdot \cdots \cdot (2n)$ into two smaller products – one containing all its even factors and

one containing its odd factors. This yields

$$\begin{aligned}(2n)! &= 1 \cdot 2 \cdot \cdots \cdot (2n) \\ &= \underbrace{(2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n))}_{\substack{=2^n \cdot (1 \cdot 2 \cdot 3 \cdot \cdots \cdot n) \\ \text{(here, we have factored out a 2} \\ \text{from each factor)}}} \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \\ &= 2^n \cdot \underbrace{(1 \cdot 2 \cdot 3 \cdot \cdots \cdot n)}_{\substack{=1 \cdot 2 \cdot \cdots \cdot n = n! \\ (\text{since } n! = 1 \cdot 2 \cdot \cdots \cdot n)}} \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \\ &= 2^n n! \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) .\end{aligned}$$

Solving this equation for $1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)$, we obtain

$$1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) = \frac{(2n)!}{2^n n!}.$$

Thus, part **(c)** is solved again.

---

3 Exercise 3: Binomial coefficients 101

3.1 Problem

For any $n \in \mathbb{Q}$ and $k \in \mathbb{N}$, we define the *binomial coefficient* $\binom{n}{k}$ by

$$\binom{n}{k} = \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

We furthermore set $\binom{n}{k} = 0$ for all rational $k \notin \mathbb{N}$.

For example,

$$\begin{aligned}\binom{5}{3} &= \frac{5 \cdot 4 \cdot 3}{3!} = \frac{60}{6} = 10; \\ \binom{1}{3} &= \frac{1 \cdot 0 \cdot (-1)}{3!} = \frac{0}{6} = 0; \\ \binom{-2}{3} &= \frac{(-2) \cdot (-3) \cdot (-4)}{3!} = \frac{-24}{6} = -4; \\ \binom{1/2}{3} &= \frac{(1/2) \cdot (-1/2) \cdot (-3/2)}{3!} = \frac{3/8}{6} = \frac{1}{16}; \\ \binom{4}{1/2} &= 0 \qquad (\text{since } 1/2 \notin \mathbb{N}) .\end{aligned}$$

Prove the following properties of binomial coefficients:

(a) If $n \in \mathbb{N}$ and $k \in \mathbb{N}$ are such that $n \geq k$, then

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

(This is often used as a definition of the binomial coefficients, but it is a lousy definition, as it only covers the case when $n, k \in \mathbb{N}$ and $n \geq k$.)

(b) If $n \in \mathbb{N}$ and $k \in \mathbb{Q}$ are such that $k > n$, then

$$\binom{n}{k} = 0.$$

(c) If $n \in \mathbb{N}$ and $k \in \mathbb{Q}$, then

$$\binom{n}{k} = \binom{n}{n-k}. \tag{14}$$

(This is known as the *symmetry of binomial coefficients*. Note that it fails if $n \notin \mathbb{N}$.)

(d) Any $n \in \mathbb{Q}$ and $k \in \mathbb{Z}$ satisfy

$$\binom{-n}{k} = (-1)^k \binom{k+n-1}{k}. \tag{15}$$

(This is one of the versions of the *upper negation formula*.)

(e) Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{16}$$

(This is the *recurrence of the binomial coefficients*, and is the reason why each entry of Pascal's triangle is the sum of the two entries above it.)

(f) Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{17}$$

3.2 Solution

(a) Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $n \geq k$. From $k \in \mathbb{N}$, we obtain $k \geq 0$, thus $n - k \leq n$. Combining this with $n - k \geq 0$ (since $n \geq k$), we obtain $0 \leq n - k \leq n$. Therefore, we can split the product $1 \cdot 2 \cdot \cdots \cdot n$ into two smaller products by putting its first $n-k$ factors into the first block and its last k factors into the second:

$$1 \cdot 2 \cdot \cdots \cdot n = (1 \cdot 2 \cdot \cdots \cdot (n-k)) \cdot ((n-k+1) \cdot (n-k+2) \cdot \cdots \cdot n).$$

Now, the definition of $n!$ yields

$$\begin{aligned} n! &= 1 \cdot 2 \cdot \cdots \cdot n \\ &= \underbrace{(1 \cdot 2 \cdot \cdots \cdot (n-k))}_{=(n-k)!} \cdot \underbrace{((n-k+1) \cdot (n-k+2) \cdot \cdots \cdot n)}_{=n(n-1)(n-2)\cdots(n-k+1)} \\ &\qquad \text{(since } (n-k)! \text{ was defined as } 1 \cdot 2 \cdot \cdots \cdot (n-k)) \quad \text{(here, we have reversed the order of multiplication)} \\ &= (n-k)! \cdot (n\,(n-1)\,(n-2) \cdots (n-k+1)). \end{aligned}$$

Solving this for $n(n-1)(n-2)\cdots(n-k+1)$, we obtain

$$n(n-1)(n-2)\cdots(n-k+1) = n!/(n-k)!. \tag{18}$$

Now, $k \in \mathbb{N}$; thus, the definition of $\binom{n}{k}$ yields

$$\begin{aligned}\binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!/(n-k)!}{k!} \qquad \text{(by (18))} \\ &= \frac{n!}{k!\,(n-k)!}.\end{aligned}$$

This solves part **(a)** of the exercise.

(b) Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$ be such that $k > n$. We must prove that $\binom{n}{k} = 0$.

If $k \notin \mathbb{N}$, then this follows immediately from the definition of $\binom{n}{k}$ (since $\binom{n}{k}$ is simply defined to be 0 in this case). Thus, we WLOG assume that $k \in \mathbb{N}$ for the rest of this proof.

From $k > n$, we obtain $n < k$, thus $n \leq k-1$ (since both n and k are integers[3]). Thus, $n \in \{0, 1, \ldots, k-1\}$ (since $n \in \mathbb{N}$). Hence, one of the k factors of the product $\prod_{i=0}^{k-1}(n-i)$ is $n-n=0$. Therefore, this product $\prod_{i=0}^{k-1}(n-i)$ has at least one factor equal to 0; thus, the whole product is 0. In other words, $\prod_{i=0}^{k-1}(n-i) = 0$. Now, the definition of $\binom{n}{k}$ yields

$$\binom{n}{k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!} = \frac{0}{k!}$$

(since $\prod_{i=0}^{k-1}(n-i) = 0$). Thus, $\binom{n}{k} = \frac{0}{k!} = 0$. This solves part **(b)** of the exercise.

(c) Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. We must prove the equality (14). If k is not an integer, then this equality trivially holds[4]. Hence, for the rest of this proof, we WLOG assume that k is an integer.

We are in one of the following three cases:

Case 1: We have $k < 0$.

Case 2: We have $k > n$.

Case 3: We have neither $k < 0$ nor $k > n$.

[3] thanks to the $k \in \mathbb{N}$ assumption that we just made

[4] *Proof.* Assume that k is not an integer. If $n-k$ was an integer, then $k = n-(n-k)$ would be an integer as well (being the difference of the two integers n and $n-k$), which would contradict the fact that k is not an integer. Hence, $n-k$ cannot be an integer. Thus, $n-k \notin \mathbb{N}$. Hence, $\binom{n}{n-k} = 0$ (by the definition of $\binom{n}{n-k}$). Also, $k \notin \mathbb{N}$ (since k is not an integer); thus, $\binom{n}{k} = 0$ (by the definition of $\binom{n}{k}$). Comparing these two equalities, we obtain $\binom{n}{k} = \binom{n}{n-k}$. In other words, (14) holds. Thus, we have proven (14) in the case when k is not an integer.

Let us first consider Case 1. In this case, we have $k < 0$. Thus, $k \notin \mathbb{N}$, so that $\binom{n}{k} = 0$ (by the definition of $\binom{n}{k}$). On the other hand, from $k < 0$, we obtain $n - k > n$. Hence, part **(b)** of this exercise (applied to $n - k$ instead of k) yields $\binom{n}{n-k} = 0$. Comparing this with $\binom{n}{k} = 0$, we obtain $\binom{n}{k} = \binom{n}{n-k}$. Hence, (14) is proven in Case 1.

Let us next consider Case 2. In this case, we have $k > n$. Thus, $n - k < 0$, so that $n - k \notin \mathbb{N}$, and thus $\binom{n}{n-k} = 0$ (by the definition of $\binom{n}{n-k}$). On the other hand, part **(b)** of this exercise yields $\binom{n}{k} = 0$. Comparing this with $\binom{n}{n-k} = 0$, we obtain $\binom{n}{k} = \binom{n}{n-k}$. Hence, (14) is proven in Case 2.

Let us finally consider Case 3. In this case, we have neither $k < 0$ nor $k > n$. Hence, we have $k \geq 0$ and $k \leq n$. Thus, $n \geq k$ and $k \in \mathbb{N}$ (since $k \geq 0$). Hence, part **(a)** of this exercise yields $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$. Also, $n - k \geq 0$ (since $n \geq k$), so that $n - k \in \mathbb{N}$. Also, from $k \geq 0$, we get $n \geq n - k$. Thus, part **(a)** of this exercise (applied to $n - k$ instead of k) yields

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

Comparing this with $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$, we obtain $\binom{n}{k} = \binom{n}{n-k}$. Hence, (14) is proven in Case 3.

We have now proven (14) in all three Cases 1, 2 and 3. Thus, (14) always holds. This solves part **(c)** of the exercise.

(d) Let $n \in \mathbb{Q}$ and $k \in \mathbb{Z}$. We must prove the equality (15). If $k \notin \mathbb{N}$, then this equality trivially holds[5]. Hence, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

Thus, the definition of $\binom{-n}{k}$ yields

$$\begin{aligned}
\binom{-n}{k} &= \frac{(-n)\,((-n)-1)\,((-n)-2)\cdots((-n)-k+1)}{k!} \\
&= \frac{1}{k!}\underbrace{\left((-n)\,((-n)-1)\,((-n)-2)\cdots((-n)-k+1)\right)}_{\substack{=(-n)(-(n+1))(-(n+2))\cdots(-(n+k-1)) \\ =(-1)^k(n(n+1)(n+2)\cdots(n+k-1)) \\ \text{(here, we have factored a minus sign out of each factor)}}} \\
&= \frac{1}{k!}\,(-1)^k\,(n\,(n+1)\,(n+2)\cdots(n+k-1))\,. \qquad (19)
\end{aligned}$$

[5] *Proof.* Assume that $k \notin \mathbb{N}$. Then, $\binom{-n}{k} = 0$ (by the definition of $\binom{-n}{k}$) and $\binom{k+n-1}{k} = 0$ (by the definition of $\binom{k+n-1}{k}$). In view of these two equations, the equality (15) rewrites as $0 = (-1)^k 0$, which is obviously true. Thus, we have proven (15) in the case when $k \notin \mathbb{N}$.

On the other hand, the definition of $\binom{k+n-1}{k}$ yields

$$\begin{aligned}\binom{k+n-1}{k} &= \frac{(k+n-1)\left((k+n-1)-1\right)\left((k+n-1)-2\right)\cdots\left((k+n-1)-k+1\right)}{k!} \\ &= \frac{1}{k!}\underbrace{(k+n-1)\left((k+n-1)-1\right)\left((k+n-1)-2\right)\cdots\left((k+n-1)-k+1\right)}_{\substack{=(k+n-1)(k+n-2)(k+n-3)\cdots n \\ =n(n+1)(n+2)\cdots(n+k-1) \\ \text{(here, we have reversed the order of multiplication)}}} \\ &= \frac{1}{k!}\left(n\left(n+1\right)\left(n+2\right)\cdots\left(n+k-1\right)\right),\end{aligned}$$

so that

$$\begin{aligned}(-1)^k\binom{k+n-1}{k} &= (-1)^k\frac{1}{k!}\left(n\left(n+1\right)\left(n+2\right)\cdots\left(n+k-1\right)\right) \\ &= \frac{1}{k!}(-1)^k\left(n\left(n+1\right)\left(n+2\right)\cdots\left(n+k-1\right)\right).\end{aligned}$$

Comparing this with (19), we obtain $\binom{-n}{k} = (-1)^k\binom{k+n-1}{k}$. Thus, (15) is proven. This solves part **(d)** of the exercise.

(e) Let $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. We must prove the equality (16). If $k \notin \mathbb{N}$, then this equality trivially holds[6]. Hence, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

We are in one of the following two cases:

Case 1: We have $k = 0$.

Case 2: We have $k \neq 0$.

Let us first consider Case 1. In this case, we have $k = 0$. Thus, $k-1 = -1 \notin \mathbb{N}$, so that $\binom{n-1}{k-1} = 0$ (by the definition of $\binom{n-1}{k-1}$). But $0 \in \mathbb{N}$; thus, the definition of $\binom{n}{0}$ yields

$$\binom{n}{0} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-0+1\right)}{0!}.$$

Since $n\left(n-1\right)\left(n-2\right)\cdots\left(n-0+1\right) = (\text{empty product}) = 1$ and $0! = 1$, this rewrites as

$$\binom{n}{0} = \frac{1}{1} = 1.$$

This rewrites as $\binom{n}{k} = 1$ (since $k = 0$). The same argument (applied to $n-1$ instead of n) yields $\binom{n-1}{k} = 1$. Now, the equality (16) boils down to $1 = 1+0$ (since $\binom{n}{k} = 1$ and $\binom{n-1}{k} = 1$ and $\binom{n-1}{k-1} = 0$), which is true. Hence, (16) is proven in Case 1.

[6] *Proof.* Assume that $k \notin \mathbb{N}$. If we had $k-1 \in \mathbb{N}$, then we would have $k = \underbrace{k-1}_{\in\mathbb{N}} + \underbrace{1}_{\in\mathbb{N}} \in \mathbb{N}$ as well, which would contradict the fact that $k \notin \mathbb{N}$. Hence, we must have $k-1 \notin \mathbb{N}$. Hence, $\binom{n-1}{k-1} = 0$ (by the definition of $\binom{n-1}{k-1}$). Also, $k \notin \mathbb{N}$; thus, $\binom{n}{k} = 0$ (by the definition of $\binom{n}{k}$) and $\binom{n-1}{k} = 0$ (by the definition of $\binom{n-1}{k}$). Now, the equality (16) boils down to $0 = 0+0$ (since $\binom{n}{k} = 0$ and $\binom{n-1}{k} = 0$ and $\binom{n-1}{k-1} = 0$), which is clearly true. Thus, we have proven (16) in the case when $k \notin \mathbb{N}$.

Let us next consider Case 2. In this case, we have $k \neq 0$. Thus, k is a positive integer (since $k \in \mathbb{N}$), so that $k-1 \in \mathbb{N}$.

Exercise 2 **(a)** (applied to k instead of n) yields $k! = k \cdot (k-1)!$, so that $(k-1)! = k!/k$ and thus $\dfrac{1}{(k-1)!} = \dfrac{1}{k!/k} = \dfrac{1}{k!} \cdot k$.

Recall that $k-1 \in \mathbb{N}$. Hence, the definition of $\dbinom{n}{k-1}$ yields

$$\begin{aligned}\binom{n}{k-1} &= \frac{n\,(n-1)\,(n-2)\cdots(n-(k-1)+1)}{(k-1)!} \\ &= \frac{1}{(k-1)!} \cdot \left(n\,(n-1)\,(n-2)\cdots(n-(k-1)+1)\right).\end{aligned}$$

The same argument (applied to $n-1$ instead of n) yields

$$\begin{aligned}\binom{n-1}{k-1} &= \underbrace{\frac{1}{(k-1)!}}_{=\frac{1}{k!}\cdot k} \cdot \underbrace{\left((n-1)\,((n-1)-1)\,((n-1)-2)\cdots((n-1)-(k-1)+1)\right)}_{=(n-1)(n-2)\cdots(n-k+1)} \\ &= \frac{1}{k!} \cdot k \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right). \qquad (20)\end{aligned}$$

On the other hand, the definition of $\dbinom{n}{k}$ yields

$$\begin{aligned}\binom{n}{k} &= \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!} \\ &= \frac{1}{k!}\left(n\,(n-1)\,(n-2)\cdots(n-k+1)\right). \qquad (21)\end{aligned}$$

The same argument (applied to $n-1$ instead of n) yields

$$\begin{aligned}\binom{n-1}{k} &= \frac{1}{k!}\underbrace{\left((n-1)\,((n-1)-1)\,((n-1)-2)\cdots((n-1)-k+1)\right)}_{\substack{=(n-1)(n-2)\cdots(n-k) \\ =((n-1)(n-2)\cdots(n-k+1))\cdot(n-k)}} \\ &= \frac{1}{k!} \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right) \cdot (n-k) \\ &= \frac{1}{k!}\,(n-k) \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right).\end{aligned}$$

Adding (20) to this equality, we obtain

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{1}{k!}\,(n-k) \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right) \\ &\qquad + \frac{1}{k!} \cdot k \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right) \\ &= \frac{1}{k!} \cdot \underbrace{\left((n-k)+k\right)}_{=n} \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right) \\ &= \frac{1}{k!} \cdot \underbrace{n \cdot \left((n-1)\,(n-2)\cdots(n-k+1)\right)}_{=n(n-1)(n-2)\cdots(n-k+1)} \\ &= \frac{1}{k!}\left(n\,(n-1)\,(n-2)\cdots(n-k+1)\right) = \binom{n}{k}\end{aligned}$$

(by (21)). Hence, (16) is proven in Case 2.

We have now proven (16) in both Cases 1 and 2. Thus, (16) always holds. This solves part **(e)** of the exercise.

(f) Let $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. We must prove the equality (17). If $k \notin \mathbb{N}$, then this equality trivially holds[7]. Hence, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

We are in one of the following two cases:

Case 1: We have $k = 0$.

Case 2: We have $k \neq 0$.

Let us first consider Case 1. In this case, we have $k = 0$. Thus, $k-1 = -1 \notin \mathbb{N}$, so that $\dbinom{n-1}{k-1} = 0$ (by the definition of $\dbinom{n-1}{k-1}$). Hence, $n\dbinom{n-1}{k-1} = n \cdot 0 = 0$. Comparing this with $\underbrace{k}_{=0}\dbinom{n}{k} = 0$, we obtain $k\dbinom{n}{k} = n\dbinom{n-1}{k-1}$. Hence, (17) is proven in Case 1.

Let us next consider Case 2. In this case, we have $k \neq 0$. Thus, k is a positive integer (since $k \in \mathbb{N}$), so that $k-1 \in \mathbb{N}$.

As in the solution to part **(e)** above, we can prove the equality (20). Multiplying both sides of this equality by n, we obtain

$$\begin{aligned} n\binom{n-1}{k-1} &= n \cdot \frac{1}{k!} \cdot k \cdot ((n-1)(n-2)\cdots(n-k+1)) \\ &= k \cdot \frac{1}{k!} \cdot \underbrace{n \cdot ((n-1)(n-2)\cdots(n-k+1))}_{=n(n-1)(n-2)\cdots(n-k+1)} \\ &= k \cdot \frac{1}{k!} \cdot (n(n-1)(n-2)\cdots(n-k+1)). \end{aligned} \tag{22}$$

On the other hand, the definition of $\dbinom{n}{k}$ yields

$$\begin{aligned} \binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \\ &= \frac{1}{k!}(n(n-1)(n-2)\cdots(n-k+1)). \end{aligned} \tag{23}$$

Multiplying both sides of this equality by k, we find

$$k\binom{n}{k} = k \cdot \frac{1}{k!}(n(n-1)(n-2)\cdots(n-k+1)).$$

Comparing this with (22), we obtain $k\dbinom{n}{k} = n\dbinom{n-1}{k-1}$. Hence, (17) is proven in Case 2.

We have now proven (17) in both Cases 1 and 2. Thus, (17) always holds. This solves part **(f)** of the exercise.

[7] *Proof.* Assume that $k \notin \mathbb{N}$. If we had $k-1 \in \mathbb{N}$, then we would have $k = \underbrace{k-1}_{\in\mathbb{N}} + \underbrace{1}_{\in\mathbb{N}} \in \mathbb{N}$ as well, which would contradict the fact that $k \notin \mathbb{N}$. Hence, we must have $k-1 \notin \mathbb{N}$. Hence, $\dbinom{n-1}{k-1} = 0$ (by the definition of $\dbinom{n-1}{k-1}$). Also, $k \notin \mathbb{N}$; thus, $\dbinom{n}{k} = 0$ (by the definition of $\dbinom{n}{k}$). Now, the equality (17) boils down to $k \cdot 0 = n \cdot 0$ (since $\dbinom{n}{k} = 0$ and $\dbinom{n-1}{k-1} = 0$), which is clearly true (since both sides equal 0). Thus, we have proven (17) in the case when $k \notin \mathbb{N}$.

4 Exercise 4: General associativity for binary operations

4.1 Problem

Let S be a set. A *binary operation* on S means a map from $S \times S$ to S. (In other words, a binary operation on S means a function that takes two elements of S and outputs an element of S. For example, subtraction of integers is a binary operation on $\mathbb{Z}$, sending each pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ to $a - b \in \mathbb{Z}$. Other binary operations on $\mathbb{Z}$ are addition and multiplication, but not division[8].)

Fix a binary operation $*$ on S. In the following, we will write this operation $*$ in *infix notation*. This means that if $a, b \in S$, then we write $a * b$ (rather than $*(a, b)$) for the image of (a, b) under $*$. (This is how binary operations are commonly written: For example, addition, subtraction and multiplication are all written this way. For instance, you write $a + b$ for the sum of two numbers a and b, not $+(a, b)$.)

Now, assume that we have

$$a * (b * c) = (a * b) * c \qquad \text{for all } a, b, c \in S \ . \tag{24}$$

(This is often called the *associativity law* for $*$; a binary operation $*$ satisfying this law is called *associative*.[9])

[8] Division is not a binary operation on $\mathbb{Z}$, because $1/2 \notin \mathbb{Z}$ (and also because $1/0$ is not defined).

[9] For example, the operation $+$ on integers is associative, since every three integers a, b, c satisfy $a+(b+c) = (a+b)+c$. Similarly, the operation $\cdot$ (multiplication) on integers is associative. But the operation $-$ on integers is not associative, since not every three integers a, b, c satisfy $a - (b - c) = (a - b) - c$ (in fact, a specific counterexample is $a = 0$, $b = 0$ and $c = 1$).

Here are five more examples of associative operations:

- The binary operation gcd on positive integers (sending each $(a, b) \in \{1, 2, 3, \ldots\}^2$ to the greatest common divisor $\gcd(a, b)$ of a and b) is associative. (This will be proven later in class.) Note that this operation is usually **not** written infix: We write $\gcd(a, b)$, not $a \gcd b$.
- The binary operation min on integers (sending each $(a, b) \in \mathbb{Z}^2$ to $\min\{a, b\}$, which is the smaller of the two numbers a and b) is associative. (This is easy to check: If $a, b, c \in \mathbb{Z}$, then both $\min\{a, \min\{b, c\}\}$ and $\min\{\min\{a, b\}, c\}$ equal the smallest of the three numbers a, b, c.)
- If $n \in \mathbb{N}$, then multiplication of $n \times n$-matrices (say, with real entries) is associative. (We will elaborate on this later in class.)
- The binary operation $\#$ on the open interval $(-1, 1) \subseteq \mathbb{R}$ defined by

$$a \# b = \frac{a + b}{1 + ab}$$

  is associative (check this!). This operation $\#$ is sometimes known as *relativistic addition of velocities* (renormalized so that the speed of light is 1); see Keith Conrad, *Relativistic addition and group theory* for more about it.
- If A is any set, and A^A is the set of all maps from A to A, then the composition of maps (i.e., the binary operation that sends each $(f, g) \in \left(A^A\right)^2$ to $f \circ g$) is associative.

The equality (24) entails that if $a, b, c \in S$ are three elements, then the "triple product"[10] expression $a * b * c$ makes sense; indeed, the two reasonable ways to interpret this expression are $a*(b*c)$ and $(a*b)*c$ (corresponding to the two possible orders in which the $*$ operations can be performed), and the associativity law (24) says precisely that these two ways lead to the same result. This result can therefore be called $a * b * c$ without risking ambiguity.

Less obvious is the case of a "quadruple product" expression $a*b*c*d$ when $a, b, c, d \in S$ are four elements. There are not 2 but 5 different ways of interpreting this expression:

$$a * (b * (c * d)), \qquad a * ((b * c) * d), \qquad (a * b) * (c * d),$$
$$(a * (b * c)) * d, \qquad ((a * b) * c) * d.$$

It can again be shown using (24) that these 5 ways produce one and the same result. (For example, the second and the fourth of these 5 ways produce the same result, because applying (24) to a, $b*c$ and d instead of a, b and c yields $a*((b*c)*d) = (a*(b*c))*d$.) Thus, the "quadruple product" $a*b*c*d$ can, too, be given a non-ambiguous meaning: Just evaluate any of its 5 possible interpretations; the result doesn't depend on which one you chose.

In this exercise, we will generalize this to arbitrary "k-tuple product" expressions $a_1 * a_2 * \cdots * a_k$ (with $a_1, a_2, \ldots, a_k \in S$). The main claim is that all possible ways of interpreting such an expression yield the same result. Even formulating this claim rigorously is not easy!

We will circumnavigate this difficulty as follows: Rather than try to explain what "interpreting this expression" means, we will first **define** the value of $a_1 * a_2 * \cdots * a_k$ in a specific way – namely, by performing the $*$ operations "from left to right" (i.e., we will define it to be $(\cdots((a_1 * a_2) * a_3) * \cdots) * a_k$); we will actually denote this value by $P(a_1, a_2, \ldots, a_k)$ (in order to avoid being tempted by the overly suggestive notation $a_1 * a_2 * \cdots * a_k$ into believing something that needs to proven first!), and we will define it recursively (in order to avoid having "$\cdots$" in our definition). Once this $P(a_1, a_2, \ldots, a_k)$ is defined, we will prove[11] that every positive integer k, every $a_1, a_2, \ldots, a_k \in S$ and every $i \in \{1, 2, \ldots, k-1\}$ satisfy

$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_k)),$$

and this will show that the value $P(a_1, a_2, \ldots, a_k)$ is also obtained if we interpret the expression $a_1 * a_2 * \cdots * a_k$ starting with any of the $*$ signs. (By induction, this freedom to start with any of the $*$ signs means that we can also continue with any of the remaining $*$ signs, and so on.)

Here is the definition we promised:

Definition.

For every positive integer k and any k elements $a_1, a_2, \ldots, a_k \in S$, we define an element $P(a_1, a_2, \ldots, a_k) \in S$ by recursion on k, as follows:

- For $k = 1$, we simply set
$$P(a_1) = a_1. \tag{25}$$
- If $k > 1$, then we set
$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_{k-1})) * a_k. \tag{26}$$

[10] The word "product" is meant in the wider sense. Of course, $*$ does not have to be multiplication of numbers. When it is, our "products" are products in the usual sense.

[11] This is part **(a)** of the exercise.

By unrolling this recursive definition, you can see what it means for each specific value of k: Namely,

$$\begin{aligned} P(a_1) &= a_1; \\ P(a_1, a_2) &= a_1 * a_2; \\ P(a_1, a_2, a_3) &= (a_1 * a_2) * a_3; \\ P(a_1, a_2, a_3, a_4) &= ((a_1 * a_2) * a_3) * a_4; \\ &\cdots \\ P(a_1, a_2, \ldots, a_k) &= (\cdots((a_1 * a_2) * a_3) * \cdots) * a_k. \end{aligned}$$

So, as you see, $P(a_1, a_2, \ldots, a_k)$ is just (a formal way to say) "the expression $a_1 * a_2 * \cdots * a_k$ interpreted by performing the $*$ operations from left to right".

Now comes the actual exercise:

(a) Prove that every positive integer k, every elements $a_1, a_2, \ldots, a_k \in S$ and every $i \in \{1, 2, \ldots, k-1\}$ satisfy

$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_k)). \tag{27}$$

Now, we define the value of the "k-tuple product" expression $a_1 * a_2 * \cdots * a_k$ (where k is a positive integer and $a_1, a_2, \ldots, a_k \in S$ are k elements) to be $P(a_1, a_2, \ldots, a_k)$. Then, the equality (27) rewrites as

$$a_1 * a_2 * \cdots * a_k = (a_1 * a_2 * \cdots * a_i) * (a_{i+1} * a_{i+2} * \cdots * a_k),$$

which means precisely that you can start evaluating the expression $a_1 * a_2 * \cdots * a_k$ with any of the $*$ signs and you still get the same result. (Of course, the two smaller sub-expressions $a_1 * a_2 * \cdots * a_i$ and $a_{i+1} * a_{i+2} * \cdots * a_k$ can also be evaluated by starting with any of the $*$ signs, and so on. Thus, by induction, you can perform the $*$ operations in any order and still get the same result.)

Note that this notation $a_1 * a_2 * \cdots * a_k$ generalizes the sum $a_1 + a_2 + \cdots + a_k$ and the product $a_1 \cdot a_2 \cdot \cdots \cdot a_k$ of k numbers.

So far we have only defined the value of "k-tuple products" $a_1 * a_2 * \cdots * a_k$ when $k > 0$; our next goal is to also give them a meaning in the case when $k = 0$. While this is a degenerate border case (we are defining a "product" with no factors!), it tends to be rather useful.

Let e be an element of S such that

$$a * e = e * a = a \qquad \text{for all } a \in S. \tag{28}$$

(Such an element e is called *neutral* for the operation $*$. For example, $0 \in \mathbb{Z}$ is neutral for the operation $+$, while $1 \in \mathbb{Z}$ is neutral for the operation $\cdot$. Not every binary operation has a neutral element.[12])

Now, using e, let us extend our definition of $P(a_1, a_2, \ldots, a_k)$ (which, so far, only covered the case $k > 0$) to the case when $k = 0$. This is a very degenerate case: In this case, $(a_1, a_2, \ldots, a_k)$ is the empty list $()$, so we just need to define $P()$. We define it by setting

$$P() = e.$$

Now we can extend the result of part **(a)** of the exercise somewhat, by allowing k to be 0 and allowing i to be 0 or k:

[12]However, it is easy to show that any binary operation has **at most one** neutral element. In other words, if e_1 and e_2 are two elements of S that are both neutral for $*$, then $e_1 = e_2$.

(b) Prove that every nonnegative integer k, every elements $a_1, a_2, \ldots, a_k \in S$ and every $i \in \{0, 1, \ldots, k\}$ satisfy

$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_k)).$$

4.2 Remark

Part **(a)** of this exercise (and, occasionally, part **(b)** as well) is known as the *general associativity law*. Notice the power of this law: Once you check the associativity law (24) for "$*$-products" of 3 elements, it allows you to define "k-tuple products" $a_1 * a_2 * \cdots * a_k$ and gives you an associativity law for them for free.

This is used tacitly in many places. For example, in linear algebra, one commonly defines the product AB of two matrices A and B, and then shows that this product satisfies the associativity law (that is, $A(BC) = (AB)C$). The general associativity law then shows that a product $A_1 A_2 \cdots A_k$ of k matrices is well-defined (i.e., its value does not depend on the order in which you perform the multiplications).[13] Chances are, you have been using this fact long before you realized it needs to be proven.

4.3 Solution

(a) We will solve part **(a)** of the exercise by induction on k.

Induction base: Part **(a)** of the exercise holds for $k = 1$, for fairly stupid reasons[14]. This concludes the induction base.

Induction step: Fix a positive integer $n > 1$. Assume that part **(a)** of the exercise holds for $k = n - 1$. We must now prove that part **(a)** of the exercise holds for $k = n$.

We have assumed that part **(a)** of the exercise holds for $k = n - 1$. In other words, the following claim holds:

> *Claim 1:* Every elements $a_1, a_2, \ldots, a_{n-1} \in S$ and every $i \in \{1, 2, \ldots, n-2\}$ satisfy
>
> $$P(a_1, a_2, \ldots, a_{n-1}) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})).$$

We must prove that part **(a)** of the exercise holds for $k = n$. In other words, we must prove the following claim:

> *Claim 2:* Every elements $a_1, a_2, \ldots, a_n \in S$ and every $i \in \{1, 2, \ldots, n-1\}$ satisfy
>
> $$P(a_1, a_2, \ldots, a_n) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_n)). \tag{29}$$

[*Proof of Claim 2:* Let $a_1, a_2, \ldots, a_n \in S$ and $i \in \{1, 2, \ldots, n-1\}$. We must prove the equality (29).

From $i \in \{1, 2, \ldots, n-1\}$, we obtain $1 \leq i \leq n-1$. Hence, $n - 1 \geq 1$, so that $n \geq 2$.

We are in one of the following two cases:

[13] Strictly speaking, this argument works only for square matrices, because multiplication of non-square matrices is not a binary operation. But a straightforward generalization of the general associativity law can be used to adapt this argument to the case of arbitrary rectangular matrices.

[14] *Proof.* If $k = 1$, then $\{1, 2, \ldots, k-1\} = \{1, 2, \ldots, 1-1\} = \{1, 2, \ldots, 0\} = \varnothing$. Hence, if $k = 1$, then there exists no $i \in \{1, 2, \ldots, k-1\}$. Thus, if $k = 1$, then part **(a)** of the exercise is vacuously true (because it makes a statement about "every $i \in \{1, 2, \ldots, k-1\}$", but no such i exists). And a vacuously true statement is true.

Case 1: We have $i = n-1$.

Case 2: We have $i \neq n-1$.

Let us first consider Case 1. In this case, we have $i = n-1$. Thus, $n-i = 1$; hence, the $(n-i)$-tuple $(a_{i+1}, a_{i+2}, \ldots, a_n)$ is simply the 1-tuple (a_n). Thus,

$$P(a_{i+1}, a_{i+2}, \ldots, a_n) = P(a_n) = a_n \tag{30}$$

(by (25), applied to a_n instead of a_1).

But $n \geq 2 > 1$. Thus, (26) (applied to $k = n$) yields

$$\begin{aligned} P(a_1, a_2, \ldots, a_n) &= (P(a_1, a_2, \ldots, a_{n-1})) * a_n \\ &= (P(a_1, a_2, \ldots, a_i)) * \underbrace{a_n}_{\substack{=P(a_{i+1}, a_{i+2}, \ldots, a_n) \\ \text{(by (30))}}} \qquad \text{(since } n-1 = i\text{)} \\ &= (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_n)). \end{aligned}$$

Thus, (29) is proven in Case 1.

Let us now consider Case 2. In this case, we have $i \neq n-1$. Thus, $i < n-1$ (since $i \leq n-1$). Hence, $n-i > 1$. Thus, (26) (applied to $n-i$ and $a_{i+1}, a_{i+2}, \ldots, a_n$ instead of k and $a_1, a_2, \ldots, a_k$) yields

$$P(a_{i+1}, a_{i+2}, \ldots, a_n) = (P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})) * a_n.$$

Hence,

$$\begin{aligned} &(P(a_1, a_2, \ldots, a_i)) * \underbrace{(P(a_{i+1}, a_{i+2}, \ldots, a_n))}_{=(P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})) * a_n} \\ &= (P(a_1, a_2, \ldots, a_i)) * ((P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})) * a_n) \\ &= ((P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_{n-1}))) * a_n \end{aligned} \tag{31}$$

(by (24), applied to $a = P(a_1, a_2, \ldots, a_i)$, $b = P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})$ and $c = a_n$).

Furthermore, $i < n-1$. Since i and $n-1$ are integers, this entails $i \leq (n-1)-1 = n-2$. Thus, $i \in \{1, 2, \ldots, n-2\}$ (since $i \geq 1$). Hence, Claim 1 yields

$$P(a_1, a_2, \ldots, a_{n-1}) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_{n-1})). \tag{32}$$

On the other hand, $n \geq 2 > 1$. Thus, (26) (applied to $k = n$) yields

$$\begin{aligned} P(a_1, a_2, \ldots, a_n) &= (P(a_1, a_2, \ldots, a_{n-1})) * a_n \\ &= ((P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_{n-1}))) * a_n \qquad \text{(by (32))} \\ &= (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_n)) \qquad \text{(by (31))}. \end{aligned}$$

Thus, (29) is proven in Case 2.

We have now proven (29) in both Cases 1 and 2. Since these two Cases cover all possibilities, we thus conclude that (29) always holds. Thus, Claim 2 is proven.]

By proving Claim 2, we have shown that part **(a)** of the exercise holds for $k = n$. This completes the induction step. Thus, part **(a)** of the exercise is proven by induction.

(b) Let k be a nonnegative integer. Let $a_1, a_2, \ldots, a_k \in S$ and $i \in \{0, 1, \ldots, k\}$. We must prove the equality

$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_k)). \tag{33}$$

We are in one of the following three cases:

Case 1: We have $i = 0$.

Case 2: We have $i = k$.

Case 3: We have $i \neq 0$ and $i \neq k$.

Let us first consider Case 1. In this case, we have $i = 0$. Hence, the i-tuple $(a_1, a_2, \ldots, a_i)$ is actually the 0-tuple $()$. Therefore, $P(a_1, a_2, \ldots, a_i) = P() = e$ (by our definition of $P()$). But the equality (28) yields that $e * a = a$ for each $a \in S$. Applying this to $a = P(a_{i+1}, a_{i+2}, \ldots, a_k)$, we obtain

$$e * P(a_{i+1}, a_{i+2}, \ldots, a_k) = P(a_{i+1}, a_{i+2}, \ldots, a_k) = P(a_1, a_2, \ldots, a_k)$$

(since $i = 0$). Hence,

$$\underbrace{(P(a_1, a_2, \ldots, a_i))}_{=e} * (P(a_{i+1}, a_{i+2}, \ldots, a_k)) = e * P(a_{i+1}, a_{i+2}, \ldots, a_k) = P(a_1, a_2, \ldots, a_k).$$

Thus, (33) is proven in Case 1.

Let us next consider Case 2. In this case, we have $i = k$. Hence, the $(k-i)$-tuple $(a_{i+1}, a_{i+2}, \ldots, a_k)$ is actually the 0-tuple $()$. Therefore, $P(a_{i+1}, a_{i+2}, \ldots, a_k) = P() = e$ (by our definition of $P()$). But the equality (28) yields that $a * e = a$ for each $a \in S$. Applying this to $a = P(a_1, a_2, \ldots, a_i)$, we obtain

$$P(a_1, a_2, \ldots, a_i) * e = P(a_1, a_2, \ldots, a_i) = P(a_1, a_2, \ldots, a_k)$$

(since $i = k$). Hence,

$$(P(a_1, a_2, \ldots, a_i)) * \underbrace{(P(a_{i+1}, a_{i+2}, \ldots, a_k))}_{=e} = P(a_1, a_2, \ldots, a_i) * e = P(a_1, a_2, \ldots, a_k).$$

Thus, (33) is proven in Case 2.

Finally, let us consider Case 3. In this case, we have $i \neq 0$ and $i \neq k$. Hence, $i \notin \{0, k\}$. Combining $i \in \{0, 1, \ldots, k\}$ with $i \notin \{0, k\}$, we obtain $i \in \{0, 1, \ldots, k\} \setminus \{0, k\} = \{1, 2, \ldots, k-1\}$. Thus, $1 \leq i \leq k-1$, so that $k \geq 2$, and therefore k is a positive integer. Hence, part **(a)** of this exercise yields

$$P(a_1, a_2, \ldots, a_k) = (P(a_1, a_2, \ldots, a_i)) * (P(a_{i+1}, a_{i+2}, \ldots, a_k)).$$

Thus, (33) is proven in Case 3.

We have now proven (33) in each of the three Cases 1, 2 and 3. Since these three Cases cover all possibilities, we thus conclude that (33) always holds. This solves part **(b)** of the exercise.

4.4 Remark

1. Assume that there exists an element $e \in S$ that is neutral for the operation $*$ (that is, satisfies (28)). Our definition of $P(a_1, a_2, \ldots, a_k)$ in the exercise treats the cases $k > 0$ and $k = 0$ separately: Namely, in the case $k > 0$, it proceeds recursively (starting with $k = 1$ as a base of the recursion), whereas in the case $k = 0$, it simply defines $P()$ to be e. There is an alternative definition of $P(a_1, a_2, \ldots, a_k)$, which handles all nonnegative integers k at the same time. Namely, we can define $P(a_1, a_2, \ldots, a_k)$ recursively by starting with $k = 0$ as a base (which is handled by setting $P() = e$, as before), and then using (26) as a recursion for all $k > 0$ (not only for $k > 1$). It is easy to see that this alternative definition is equivalent

to the definition that we gave in the exercise[15]. This definition has the advantage of needing fewer cases; but it has the disadvantage that it relies on the existence of a neutral element e more heavily than the definition given in the exercise[16]. This is why we started with the definition given in the exercise.

2. The claim of this exercise is a cornerstone of abstract algebra, often used without mention (and, most likely, without awareness). Here is one obvious-sounding fact that actually relies on this claim: Consider a set A, and n arbitrary maps $f_1, f_2, \ldots, f_n$ from A to A. Then, the composition $f_1 \circ f_2 \circ \cdots \circ f_n$ of all these n maps is well-defined (i.e., it does not matter in which order you perform the $\circ$ operations; the result will always be the same map). This may look completely evident (isn't $f_1 \circ f_2 \circ \cdots \circ f_n$ simply the map that applies f_n first, then f_{n-1}, then f_{n-2}, and so on, until all the n maps have been applied?[17]), but the rigorous proof proceeds by applying the exercise to $S = \{\text{all maps from } A \text{ to } A\}$ and to the binary operation $\circ$ on S. More generally, the same holds if $f_1, f_2, \ldots, f_n$ are maps between different sets (not just maps from A to A), as long as they can be composed (i.e., the codomain of f_{i+1} is the domain of f_i). The proof proceeds in the exact same way as the solution to the exercise above, with the only difference that there is no single S any more in which all our maps lie (but rather different sets, depending on which of our maps we are composing). See also [Grinbe19, §2.13] for this proof, done in greater detail.

References

[18f-hw0s] Darij Grinberg, *Math 5705: Enumerative Combinatorics, Fall 2018: Homework 0*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw-template.pdf` .

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See `https://www-cs-faculty.stanford.edu/~knuth/gkp.html` for errata.

[Grinbe19] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .

[15] The proof is simple: You just need to show that the two definitions agree for $k = 0$ and for $k = 1$; then, an induction on k will reveal that they also agree in all remaining cases.

[16] Namely, the definition given in the exercise uses the neutral element e only in the case $k = 0$; but the alternative definition depends on it entirely (if e was not there, then the recursion would not have a base!).

[17] Yes, it is, but the concept of applying several maps in order needs to be formally defined, too, if you want to be rigorous about it.