Notes on the combinatorial fundamentals of algebra*

Darij Grinberg

May 6, 2016

Contents

1. Introduction 2
   1.1. Prerequisites . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
   1.2. Notations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
   1.3. Sums and products: a synopsis . . . . . . . . . . . . . . . . . . . . . . 4
       1.3.1. Definition of $\sum$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
       1.3.2. Properties of $\sum$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
       1.3.3. Definition of $\prod$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
       1.3.4. Properties of $\prod$ . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29
   1.4. Polynomials: a precise definition . . . . . . . . . . . . . . . . . . . . . 32

2. On acyclic quivers and mutations 40

3. On binomial coefficients 42
   3.1. Definitions and basic properties . . . . . . . . . . . . . . . . . . . . . . 42
   3.2. Binomial coefficients and polynomials . . . . . . . . . . . . . . . . . . 50
   3.3. The Chu-Vandermonde identity . . . . . . . . . . . . . . . . . . . . . . . 53
   3.4. Further results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 69
   3.5. Additional exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 83

4. Recurrent sequences 85
   4.1. Basics . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 85
   4.2. Explicit formulas (à la Binet) . . . . . . . . . . . . . . . . . . . . . . . 89
   4.3. Further results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 90
   4.4. Additional exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 93

*old title: PRIMES 2015 reading project: problems and solutions
5. Permutations

5.1. Permutations and the symmetric group ........................................ 95
5.2. Inversions, lengths and the permutations si ∈ Sn ................................ 101
5.3. The sign of a permutation ................................................................. 104
5.4. Infinite permutations ........................................................................ 106
5.5. More on lengths of permutations ......................................................... 114
5.6. More on signs of permutations ............................................................. 117
5.7. Cycles ............................................................................................... 120
5.8. Additional exercises .......................................................................... 124

6. An introduction to determinants ............................................................. 125

6.1. Commutative rings ........................................................................ 126
6.2. Matrices .......................................................................................... 135
6.3. Determinants ................................................................................... 139
6.4. det(AB) ......................................................................................... 152
6.5. The Cauchy-Binet formula ................................................................. 167
6.6. Prelude to Laplace expansion ............................................................. 179
6.7. The Vandermonde determinant .......................................................... 183
6.8. Invertible elements in commutative rings, and fields ......................... 197
6.9. The Cauchy determinant ................................................................. 201
6.10. Laplace expansion ........................................................................ 203
6.11. Tridiagonal determinants ................................................................. 216
6.12. On block-triangular matrices ......................................................... 223
6.13. The adjugate matrix ..................................................................... 227
6.15. Noncommutative rings ................................................................... 241
6.16. Groups, and the group of units ....................................................... 243
6.17. Cramer’s rule ................................................................................ 245
6.18. Additional exercises ..................................................................... 250

Note

This is the version without solutions. See http://web.mit.edu/~darij/www/primes2015/sols.pdf for the complete version.

1. Introduction

These notes are meant as a detailed introduction to the basic combinatorics that underlies the “explicit” part of abstract algebra (i.e., the theory of determinants, and concrete families of polynomials). They cover permutations and determinants (from a combinatorial viewpoint – no linear algebra is presumed), as well as some basic material on binomial coefficients and recurrent (Fibonacci-like) sequences. The reader is assumed to be familiar with (low-level) “contest mathematics” (i.e.,
have a good proficiency with high-school mathematics) and mature enough to read combinatorial proofs.

These notes were originally written for the PRIMES reading project I have mentored in 2015. The goal of the project was to become familiar with some fundamentals of algebra and combinatorics (particularly the ones needed to understand the literature on cluster algebras).

The notes are unfinished and probably full of misprints. I thank Anya Zhang and Karthik Karnik (the two students taking part in the project) for finding some errors! Thanks also to the PRIMES project at MIT, which gave the impetus for the writing of this notes; and to George Lusztig for the sponsorship of my mentoring position in this project.

1.1. Prerequisites

These notes are still far from their final form, and the exact prerequisites for a reader are subject to change. At the current moment, I assume that the reader

- has a good grasp on basic school-level mathematics (integers, rational numbers, prime numbers, etc.);

- has some experience with proofs (mathematical induction, strong induction, proof by contradiction, the concept of “WLOG”, etc.) and mathematical notation (functions, subscripts, cases, what it means for an object to be “well-defined”, etc.);

- knows what a polynomial is (at least over \( \mathbb{Z} \) and \( \mathbb{Q} \)) and how polynomials differ from polynomial functions;

- knows the most basic properties of binomial coefficients (e.g., how \( \binom{n}{k} \) counts \( k \)-element subsets of an \( n \)-element set);

- knows the basics of modular arithmetic (e.g., if \( a \equiv b \mod n \) and \( c \equiv d \mod n \), then \( ac \equiv bd \mod n \));

- is familiar with the summation sign (\( \sum \)) and the product sign (\( \prod \)) and knows how to transform them (e.g., interchanging summations, and substituting the index).

---

1A great introduction into these matters (and many others!) is the free book [LeLeMe16] by Lehman, Leighton and Meyer. (Practical note: As of 2016, this book is still undergoing frequent revisions, so you may find a newer version of it on the internet by the time you are reading this than what I am citing below. Unfortunately, you will also find many older versions, often as the first google hits. Try searching for the title of the book along with the current year to find something new.)

2See Section [1.4] below for a quick survey of what this means, and which sources to consult for the precise definitions.

3See Section [1.3] below for a quick overview of the notations that we will need.
• has some familiarity with matrices (i.e., knows how to add and to multiply them).

Probably a few more requirements creep in at certain points of the notes, which I have overlooked. Some examples and remarks rely on additional knowledge (such as analysis, graph theory, abstract algebra); however, these can be skipped.

1.2. Notations

• In the following, we use \( \mathbb{N} \) to denote the set \( \{0, 1, 2, \ldots \} \). (Be warned that some other authors use the letter \( \mathbb{N} \) for \( \{1, 2, 3, \ldots \} \) instead.)

• We let \( \mathbb{Q} \) denote the set of all rational numbers; we let \( \mathbb{R} \) be the set of all real numbers; we let \( \mathbb{C} \) be the set of all complex numbers.

• If \( X \) and \( Y \) are two sets, then we shall use the notation “\( X \to Y, \ x \mapsto E \)” (where \( x \) is some symbol which has no specific meaning in the current context, and where \( E \) is some expression which usually involves \( x \)) for “the map from \( X \) to \( Y \) which sends every \( x \in X \) to \( E \)”. For example, “\( \mathbb{N} \to \mathbb{N}, \ x \mapsto x^2 + x + 6 \)” means the map from \( \mathbb{N} \) to \( \mathbb{N} \) which sends every \( x \in \mathbb{N} \) to \( x^2 + x + 6 \). For another example, “\( \mathbb{N} \to \mathbb{Q}, \ x \mapsto \frac{x}{1 + x} \)” denotes the map from \( \mathbb{N} \) to \( \mathbb{Q} \) which sends every \( x \in \mathbb{N} \) to \( \frac{x}{1 + x} \).

Further notations will be defined whenever they arise for the first time.

1.3. Sums and products: a synopsis

In this section, I will recall the definitions of the \( \sum \) and \( \prod \) signs and collect some of their basic properties (without proofs). When I say “recall”, I am implying that the reader has at least some prior acquaintance (and, ideally, experience) with these

\[ A \text{ word of warning: Of course, the notation “} \mathbb{N} \to \mathbb{Q}, \ x \mapsto \frac{x}{1 + x} \text{” does not always make sense; indeed, the map that it stands for might sometimes not exist. For instance, the notation “} \mathbb{N} \to \mathbb{Q}, \ x \mapsto \frac{x}{1 - x} \text{” does not actually define a map, because the map that it is supposed to define (i.e., the map from } \mathbb{N} \text{ to } \mathbb{Q} \text{ which sends every } x \in \mathbb{N} \text{ to } \frac{x}{1 - x} \text{) does not exist (since } \frac{x}{1 - x} \text{ is not defined for } x = 1 \text{). For another example, the notation “} \mathbb{N} \to \mathbb{Z}, \ x \mapsto \frac{x}{1 + x} \text{” does not define a map, because the map that it is supposed to define (i.e., the map from } \mathbb{N} \text{ to } \mathbb{Z} \text{ which sends every } x \in \mathbb{N} \text{ to } \frac{x}{1 + x} \text{) does not exist (for } x = 2 \text{, we have } \frac{x}{1 + x} = \frac{2}{1 + 2} \notin \mathbb{Z}, \text{ which shows that a map from } \mathbb{N} \text{ to } \mathbb{Z} \text{ cannot send this } x \text{ to this } \frac{x}{1 + x} \text{). Thus, when defining a map from } X \text{ to } Y \text{ (using whatever notation), do not forget to check that it is well-defined (i.e., that your definition specifies precisely one image for each } x \in X, \text{ and that these images all lie in } Y \text{). In many cases, this is obvious or very easy to check (I will usually not even mention this check), but in some cases, this is a difficult task.} \]
signs; for a first introduction, this section is probably too brief and too abstract. Ideally, you should use this section to familiarize yourself with my (sometimes idiosyncratic) notations.

Throughout Section 1.3, we let $A$ be one of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

1.3.1. Definition of $\sum$

Let us first define the $\sum$ sign. There are actually several (slightly different, but still closely related) notations involving the $\sum$ sign; let us define the most important of them:

- If $S$ is a finite set, and if $a_s$ is an element of $A$ for each $s \in S$, then $\sum_{s \in S} a_s$ denotes the sum of all of these elements $a_s$. Formally, this sum is defined by recursion on $|S|$, as follows:
  - If $S = \emptyset$, then $\sum_{s \in S} a_s$ is defined to be 0.
  - Let $n \in \mathbb{N}$. Assume that we have defined $\sum_{s \in S} a_s$ for every finite set $S$ with $|S| = n$ (and every choice of elements $a_s$ of $A$). Now, if $S$ is a finite set with $|S| = n + 1$ and if $a_s \in A$ are chosen for all $s \in S$, then $\sum_{s \in S} a_s$ is defined by picking any $t \in S$ and setting
    \[ \sum_{s \in S} a_s = a_t + \sum_{s \in S \setminus \{t\}} a_s. \] (1)

It is not immediately clear why this definition is legitimate: The right hand side of (1) is defined using a choice of $t$, but we want our value of $\sum_{s \in S} a_s$ to depend only on $S$ and on the $a_s$ (not on some arbitrarily chosen $t \in S$). However, it is possible to prove that the right hand side of (1) is actually independent of $t$ (that is, any two choices of $t$ will lead to the same result).

Examples:

- If $S = \{4, 7, 9\}$ and $a_s = \frac{1}{s^2}$ for every $s \in S$, then $\sum_{s \in S} a_s = a_4 + a_7 + a_9 = \frac{1}{4^2} + \frac{1}{7^2} + \frac{1}{9^2} = \frac{6049}{63504}$.
- If $S = \{1, 2, \ldots, n\}$ (for some $n \in \mathbb{N}$) and $a_s = s^2$ for every $s \in S$, then $\sum_{s \in S} a_s = \sum_{s \in S} s^2 = 1^2 + 2^2 + \cdots + n^2$. (There is a formula saying that the right hand side of this equality is $\frac{1}{6} n (2n + 1) (n + 1)$.)

\[ \text{This is possible, because } S \text{ is nonempty (in fact, } |S| = n + 1 > n \geq 0). \]
Remarks:

- The sum $\sum_{s \in S} a_s$ is usually pronounced “sum of the $a_s$ over all $s \in S$” or “sum of the $a_s$ with $s$ ranging over $S$” or “sum of the $a_s$ with $s$ running through all elements of $S$”. The letter “$s$” in the sum is called the “summation index” and its exact choice is immaterial (for example, you can rewrite $\sum_{s \in S} a_s$ as $\sum_{t \in S} a_t$ or as $\sum_{\Phi \in S} a_{\Phi}$ or as $\sum_{\spadesuit \in S} a_{\spadesuit}$), as long as it does not already have a different meaning outside of the sum. (Ultimately, a summation index is the same kind of placeholder variable as the “$s$” in the statement “for all $s \in S$, we have $a_s + 2a_s = 3a_s$”, or as a loop variable in a for-loop in programming.) The sign $\sum$ itself is called “the summation sign” or “the $\sum$ sign”. The numbers $a_s$ are called the addends (or summands) of the sum $\sum_{s \in S} a_s$. More precisely, for any given $t \in S$, we can refer to the number $a_t$ as the “addend corresponding to the index $t$” (or as the “addend for $s = t$”, or as the “addend for $t$”) of the sum $\sum_{s \in S} a_s$.

- When the set $S$ is empty, the sum $\sum_{s \in S} a_s$ is called an empty sum. Our definition implies that any empty sum is 0. This convention is used throughout mathematics, except in rare occasions where a slightly subtler version of it is used. If someone tells you that empty sums are undefined, you should not be listening!

- The summation index does not always have to be a single letter. For instance, if $S$ is a set of pairs, then we can write $\sum_{(x,y) \in S} a(x,y)$ (meaning the

---

6The plural of the word “index” here is “indices”, not “indexes”.
7If it already has a different meaning, then it must not be used as a summation index! For example, you must not write “every $n \in \mathbb{N}$ satisfies $\sum_{n \in \{0,1,\ldots,n\}} n = \frac{n(n+1)}{2}$, because here the summation index $n$ clashes with a different meaning of the letter $n$.
8Do not worry about this subtler version for the time being. If you really want to know what it is: Our above definition is tailored to the cases when the $a_i$ are numbers (i.e., elements of one of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$). In more advanced settings, one tends to take sums of the form $\sum_{a_s \in S} a_s$ where the $a_s$ are not numbers but (for example) elements of a commutative ring $\mathbb{K}$. (See Definition 6.2 for the definition of a commutative ring.) In such cases, one wants the sum $\sum_{a_s \in S} a_s$ for an empty set $S$ to be not the integer 0, but the zero of the commutative ring $\mathbb{K}$ (which is sometimes distinct from the integer 0). This has the slightly confusing consequence that the meaning of the sum $\sum_{a_s \in S}$ for an empty set $S$ depends on what ring $\mathbb{K}$ the $a_s$ belong to, even if (for an empty set $S$) there are no $a_s$ to begin with! But in practice, the choice of $\mathbb{K}$ is always clear from context, so this is not ambiguous.

A similar caveat applies to the other versions of the $\sum$ sign, as well as to the $\prod$ sign defined further below; I shall not elaborate on it further.
same as $\sum_{s \in S} a_s$). Here is an example of this notation:

$$\sum_{(x,y) \in \{1,2,3\}^2} \frac{x}{y} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{2}{1} + \frac{2}{2} + \frac{2}{3} + \frac{3}{1} + \frac{3}{2} + \frac{3}{3}$$

(here, we are using the notation $\sum_{(x,y) \in S} a_{(x,y)}$ with $S = \{1,2,3\}^2$ and $a_{(x,y)} = \frac{x}{y}$). Note that we could not have rewritten this sum in the form $\sum_{s \in S} a_s$ with a single-letter variable $s$ without introducing an extra notation such as $a_{(x,y)}$ for the quotients $\frac{x}{y}$.

- Mathematicians don’t seem to have reached an agreement on the operator precedence of the $\sum$ sign. By this I mean the following question: Does $\sum_{s \in S} a_s + b$ (where $b$ is some other element of $A$) mean $\sum_{s \in S} (a_s + b)$ or $\left(\sum_{s \in S} a_s\right) + b$? In my experience, the second interpretation (i.e., reading it as $\left(\sum_{s \in S} a_s\right) + b$) is more widespread, and this is the interpretation that I will follow. Nevertheless, be on the watch for possible misunderstandings, as someone might be using the first interpretation when you expect it the least!

However, the situation is different for products and nested sums. For instance, the expression $\sum_{s \in S} ba_s c$ is understood to mean $\sum_{s \in S} (ba_s c)$, and a nested sum like $\sum_{s \in S} \sum_{t \in T} a_{s,t}$ (where $S$ and $T$ are two sets, and where $a_{s,t}$ is an element of $A$ for each pair $(s, t) \in S \times T$) is to be read as $\sum_{s \in S} \left(\sum_{t \in T} a_{s,t}\right)$.

- Speaking of nested sums: they mean exactly what they seem to mean. For instance, $\sum_{s \in S} \sum_{t \in T} a_{s,t}$ is what you get if you compute the sum $\sum_{t \in T} a_{s,t}$ for each $s \in S$, and then sum up all of these sums together. In a nested sum $\sum_{s \in S} \sum_{t \in T} a_{s,t}$, the first summation sign ($\sum_{s \in S}$) is called the “outer summation”, and the second summation sign ($\sum_{t \in T}$) is called the “inner summation”.

- We have required the set $S$ to be finite when defining $\sum_{s \in S} a_s$. Of course, this requirement was necessary for our definition, and there is no way to make sense of infinite sums such as $\sum_{s \in \mathbb{Z}} s^2$. However, some infinite sums can be made sense of. The simplest case is when the set $S$ might be

---

9This is similar to the notorious disagreement about whether $a/bc$ means $(a/b) \cdot c$ or $a/(bc)$.
infinite, but only finitely many among the \( a_s \) are nonzero. In this case, we can define \( \sum_{s \in S} a_s \) simply by discarding the zero addends and summing the finitely many remaining addends. Other situations in which infinite sums make sense appear in analysis and in topological algebra (e.g., power series).

- The sum \( \sum_{s \in S} a_s \) always belongs to \( A \).  

\[ \sum_{s \in S} a_s = \sum_{s \in \{ t \in S \mid A(t) \}} a_s. \]

In other words, \( \sum_{s \in S; A(s)} a_s \) is the sum of the \( a_s \) for all \( s \in S \) which satisfy \( A(s) \).

Examples:

- If \( S = \{1,2,3,4,5\} \), then \( \sum_{s \in S; s \text{ is even}} a_s = a_2 + a_4 \). (Of course, \( \sum_{s \in S; s \text{ is even}} a_s \) when \( A(s) \) is defined to be the statement “\( s \) is even”.)

- If \( S = \{1,2,\ldots,n\} \) (for some \( n \in \mathbb{N} \)) and \( a_s = s^2 \) for every \( s \in S \), then \( \sum_{s \in S; s \text{ is even}} a_s = a_2 + a_4 + \cdots + a_k \), where \( k \) is the largest even number among \( 1,2,\ldots,n \) (that is, \( k = n \) if \( n \) is even, and \( k = n - 1 \) otherwise).

Remarks:

- The sum \( \sum_{s \in S; A(s)} a_s \) is usually pronounced “sum of the \( a_s \) over all \( s \in S \)” satisfying \( A(s) \). The semicolon after “\( s \in S \)” is often omitted or replaced by a colon or a comma. Many authors often omit the “\( s \in S \)” part (so they

\[ ^{10}\text{Recall that we have assumed } A \text{ to be one of the sets } \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \text{ and } \mathbb{C}, \text{ and that we have assumed the } a_s \text{ to belong to } A. \]

\[ ^{11}\text{Formally speaking, this means that } A \text{ is a map from } S \text{ to the set of all logical statements. Such a map is called a predicate.} \]
simply write $\sum_{A(s)} a_s$ when it is clear enough what the $S$ is. (For instance, they would write $\sum_{1 \leq s \leq 5} s^2$ instead of $\sum_{s \in \mathbb{N}; 1 \leq s \leq 5} s^2$.)

- The set $S$ needs not be finite in order for $\sum_{s \in S \cap \mathcal{A}(s)} a_s$ to be defined; it suffices that the set $\{ t \in S \mid \mathcal{A}(t) \}$ be finite (i.e., that only finitely many $s \in S$ satisfy $\mathcal{A}(s)$).

- The sum $\sum_{s \in S \cap \mathcal{A}(s)} a_s$ is said to be empty whenever the set $\{ t \in S \mid \mathcal{A}(t) \}$ is empty (i.e., whenever no $s \in S$ satisfies $\mathcal{A}(s)$).

- Finally, here is the simplest version of the summation sign: Let $u$ and $v$ be two integers. We agree to understand the set $\{u, u+1, \ldots, v\}$ to be empty when $u > v$. Let $a_s$ be an element of $\mathcal{A}$ for each $s \in \{u, u+1, \ldots, v\}$. Then, $\sum_{s=u}^{v} a_s$ is defined by

$$\sum_{s=u}^{v} a_s = \sum_{s\in\{u,u+1,\ldots,v\}} a_s.$$ 

Examples:

- We have $\sum_{s=3}^{8} \frac{1}{s} = \sum_{s \in \{3,4,\ldots,8\}} \frac{1}{s} = \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} = \frac{341}{280}$.

- We have $\sum_{s=3}^{3} \frac{1}{s} = \sum_{s \in \{3\}} \frac{1}{s} = \frac{1}{3}$.

- We have $\sum_{s=3}^{2} \frac{1}{s} = \sum_{s \in \emptyset} \frac{1}{s} = 0$.

Remarks:

- The sum $\sum_{s=u}^{v} a_s$ is usually pronounced “sum of the $a_s$ for all $s$ from $u$ to $v$ (inclusive)””. It is often written $a_u + a_{u+1} + \cdots + a_v$, but this latter notation has its drawbacks: In order to understand an expression like $a_u + a_{u+1} + \cdots + a_v$, one needs to correctly guess the pattern (which can be unintuitive when the $a_s$ themselves are complicated: for example, it takes a while to find the “moving parts” in the expression $\frac{2 \cdot 7}{3+2} + \frac{3 \cdot 7}{3+3} + \cdots + \frac{7 \cdot 7}{3+7}$, whereas the notation $\sum_{s=2}^{7} \frac{s \cdot 7}{3+s}$ for the same sum is perfectly clear).
In the sum \( \sum_{s=u}^{v} a_s \), the integer \( u \) is called the lower limit (of the sum), whereas the integer \( v \) is called the upper limit (of the sum). The sum is said to start (or begin) at \( u \) and end at \( v \).

The sum \( \sum_{s=u}^{v} a_s \) is said to be empty whenever \( u > v \). In other words, a sum of the form \( \sum_{s=u}^{v} a_s \) is empty whenever it “ends before it has begun”. However, a sum which “ends right after it begins” (i.e., a sum \( \sum_{s=u}^{v} a_s \) with \( u = v \)) is not empty; it just has one addend only. (This is unlike integrals, which are 0 whenever their lower and upper limit are equal.)

Let me stress once again that a sum \( \sum_{s=u}^{v} a_s \) with \( u > v \) is empty and equals 0. It does not matter how much greater \( u \) is than \( v \). So, for example, \( \sum_{s=1}^{-5} s = 0 \). The fact that the upper bound \((-5)\) is much smaller than the lower bound \((1)\) does not mean that you have to subtract rather than add.

Thus we have introduced the main three forms of the summation sign. Some mild variations on them appear in the literature (e.g., there is a slightly awkward notation \( \sum_{s=u}^{v} a_s\text{ for } s \in \mathcal{A}(s) \)).

### 1.3.2. Properties of \( \sum \)

Let me now show some basic properties of summation signs that are important in making them useful:

- **Splitting-off:** Let \( S \) be a finite set. Let \( t \in S \). Let \( a_s \) be an element of \( \mathcal{A}(s) \) for each \( s \in S \). Then,
  \[
  \sum_{s \in S} a_s = a_t + \sum_{s \in S \setminus \{t\}} a_s.
  \]  
  (This is precisely the equality (1).) This formula allows us to “split off” an addend from a sum.

**Example:** If \( n \in \mathbb{N} \), then
\[
\sum_{s \in \{1,2,\ldots,n+1\}} a_s = a_{n+1} + \sum_{s \in \{1,2,\ldots,n\}} a_s
\]
(by (2), applied to \( S = \{1,2,\ldots,n+1\} \) and \( t = n + 1 \)), but also
\[
\sum_{s \in \{1,2,\ldots,n\}} a_s = a_1 + \sum_{s \in \{2,3,\ldots,n+1\}} a_s
\]
• **Splitting**: Let $S$ be a finite set. Let $X$ and $Y$ be two subsets of $S$ such that $X \cap Y = \emptyset$ and $X \cup Y = S$. (Equivalently, $X$ and $Y$ are two subsets of $S$ such that each element of $S$ lies in exactly one of $X$ and $Y$.) Let $a_s$ be an element of $A$ for each $s \in S$. Then,

\[
\sum_{s \in S} a_s = \sum_{s \in X} a_s + \sum_{s \in Y} a_s.
\]

(3)

(Here, as we explained, $\sum_{s \in X} a_s + \sum_{s \in Y} a_s$ stands for $\left(\sum_{s \in X} a_s\right) + \left(\sum_{s \in Y} a_s\right)$.) The idea behind (3) is that if we want to add a bunch of numbers (the $a_s$ for $s \in S$), we can proceed by splitting it into two “sub-bunches” (one “sub-bunch” consisting of the $a_s$ for $s \in X$, and the other consisting of the $a_s$ for $s \in Y$), then take the sum of each of these two sub-bunches, and finally add together the two sums.

**Examples:**

– If $n \in \mathbb{N}$, then

\[
\sum_{s \in \{1,2,\ldots,2n\}} a_s = \sum_{s \in \{1,3,\ldots,2n-1\}} a_s + \sum_{s \in \{2,4,\ldots,2n\}} a_s.
\]

(by (3), applied to $S = \{1,2,\ldots,2n\}$, $X = \{1,3,\ldots,2n-1\}$ and $Y = \{2,4,\ldots,2n\}$.)

– If $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then

\[
\sum_{s \in \{-m,-m+1,\ldots,n\}} a_s = \sum_{s \in \{-m,-m+1,\ldots,0\}} a_s + \sum_{s \in \{1,2,\ldots,n\}} a_s
\]

(by (3), applied to $S = \{-m,-m+1,\ldots,n\}$, $X = \{-m,-m+1,\ldots,0\}$ and $Y = \{1,2,\ldots,n\}$.)

– If $u$, $v$ and $w$ are three integers such that $u - 1 \leq v \leq w$, and if $a_s$ is an element of $A$ for each $s \in \{u,u+1,\ldots,w\}$, then

\[
\sum_{s=u}^{w} a_s = \sum_{s=u}^{v} a_s + \sum_{s=v+1}^{w} a_s.
\]

(4)

This follows from (3), applied to $S = \{u,u+1,\ldots,w\}$, $X = \{u,u+1,\ldots,v\}$ and $Y = \{v+1,v+2,\ldots,w\}$. Notice that the requirement $u - 1 \leq v \leq w$ is important; otherwise, the $X \cap Y = \emptyset$ and $X \cup Y = S$ condition would not hold!
• **Splitting using a predicate:** Let $S$ be a finite set. Let $\mathcal{A}(s)$ be a logical statement for each $s \in S$. Let $a_s$ be an element of $\mathcal{A}$ for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{s \in S; \mathcal{A}(s)} a_s + \sum_{s \in S; \neg \mathcal{A}(s)} a_s$$  \hspace{1cm} (5)

(where “not $\mathcal{A}(s)$” means the negation of $\mathcal{A}(s)$). This simply follows from (3), applied to $X = \{ s \in S \mid \mathcal{A}(s) \}$ and $Y = \{ s \in S \mid \neg \mathcal{A}(s) \}$.

**Example:** If $S \subseteq \mathbb{Z}$, then

$$\sum_{s \in S} a_s = \sum_{s \in S; \text{s is even}} a_s + \sum_{s \in S; \text{s is odd}} a_s$$

(because “s is odd” is the negation of “s is even”).

• **Summing equal values:** Let $S$ be a finite set. Let $a$ be an element of $\mathcal{A}$. Then,

$$\sum_{s \in S} a = |S| \cdot a.$$ \hspace{1cm} (6)

In other words, if all addends of a sum are equal to one and the same element $a$, then the sum is just the number of its addends times $a$. In particular,

$$\sum_{s \in S} 1 = |S| \cdot 1 = |S|.$$  

• **Splitting an addend:** Let $S$ be a finite set. For every $s \in S$, let $a_s$ and $b_s$ be elements of $\mathcal{A}$. Then,

$$\sum_{s \in S} (a_s + b_s) = \sum_{s \in S} a_s + \sum_{s \in S} b_s.$$  \hspace{1cm} (7)

**Remark:** Of course, similar rules hold for other forms of summations: If $\mathcal{A}(s)$ is a logical statement for each $s \in S$, then

$$\sum_{s \in S; \mathcal{A}(s)} (a_s + b_s) = \sum_{s \in S; \mathcal{A}(s)} a_s + \sum_{s \in S; \mathcal{A}(s)} b_s.$$  

If $u$ and $v$ are two integers, then

$$\sum_{s = u}^{v} (a_s + b_s) = \sum_{s = u}^{v} a_s + \sum_{s = u}^{v} b_s.$$  \hspace{1cm} (8)

• **Factoring out:** Let $S$ be a finite set. For every $s \in S$, let $a_s$ be an element of $\mathcal{A}$. Also, let $\lambda$ be an element of $\mathcal{A}$. Then,

$$\sum_{s \in S} \lambda a_s = \lambda \sum_{s \in S} a_s.$$ \hspace{1cm} (9)

Again, similar rules hold for the other types of summation sign.
• **Zeros sum to zero:** Let $S$ be a finite set. Then,

$$\sum_{s \in S} 0 = 0.$$ 

That is, any sum of zeroes is zero.

**Remark:** This applies even to infinite sums! Do not be fooled by the infiniteness of a sum: There are no reasonable situations where an infinite sum of zeroes is defined to be anything other than zero. The infinity does not “compensate” for the zero.

• **Dropping zeroes:** Let $S$ be a finite set. Let $a_s$ be an element of $A$ for each $s \in S$. Let $T$ be a subset of $S$ such that every $s \in T$ satisfies $a_s = 0$. Then,

$$\sum_{s \in S} a_s = \sum_{s \in S \setminus T} a_s.$$ 

(That is, any addends which are zero can be removed from a sum without changing the sum’s value.)

• **Renaming the index:** Let $S$ be a finite set. Let $a_s$ be an element of $A$ for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{t \in S} a_t.$$ 

This is just saying that the summation index in a sum can be renamed at will, as long as its name does not clash with other notation.

• **Substituting the index I:** Let $S$ and $T$ be two finite sets. Let $f : S \to T$ be a bijective map. Let $a_t$ be an element of $A$ for each $t \in T$. Then,

$$\sum_{t \in T} a_t = \sum_{s \in S} a_{f(s)}.$$ 

(The idea here is that the sum $\sum_{s \in S} a_{f(s)}$ contains the same addends as the sum $\sum_{t \in T} a_t$.)

**Examples:**

- For any $n \in \mathbb{N}$, we have

$$\sum_{t \in \{1, 2, \ldots, n\}} t^3 = \sum_{s \in \{-n, -n+1, \ldots, -1\}} (-s)^3.$$ 

(This follows from (10), applied to $S = \{-n, -n+1, \ldots, -1\}$, $T = \{1, 2, \ldots, n\}$, $f(s) = -s$, and $a_t = t^3$.)
- The sets $S$ and $T$ in (10) may well be the same. For example, for any $n \in \mathbb{N}$, we have
\[ \sum_{t \in \{1,2,\ldots,n\}} t^3 = \sum_{s \in \{1,2,\ldots,n\}} (n + 1 - s)^3. \]
(This follows from (10), applied to $S = \{1,2,\ldots,n\}$, $T = \{1,2,\ldots,n\}$, $f(s) = n + 1 - s$ and $a_t = t^3$.)

- More generally: Let $u$ and $v$ be two integers. Then, the map
\[ \{u,u+1,\ldots,v\} \rightarrow \{u,u+1,\ldots,v\} \]
sending each $s \in \{u,u+1,\ldots,v\}$ to $u + v - s$ is a bijection. Hence, we can substitute $u + v - s$ for $s$ in the sum $\sum_{s=u}^{v} a_s$ whenever an element $a_s$ of $A$ is given for each $s \in \{u,u+1,\ldots,v\}$. We thus obtain the formula
\[ \sum_{s=u}^{v} a_s = \sum_{s=u}^{v} a_{u+v-s}. \]

**Remark:**

- When I use (10) to rewrite the sum $\sum_{t \in T} a_t$ as $\sum_{s \in S} a_{f(s)}$, I say that I have “substituted $f(s)$ for $t$ in the sum”. Conversely, when I use (10) to rewrite the sum $\sum_{s \in S} a_{f(s)}$ as $\sum_{t \in T} a_t$, I say that I have “substituted $t$ for $f(s)$ in the sum”.

- For convenience, I have chosen $s$ and $t$ as summation indices in (10). But as before, they can be chosen to be any letters not otherwise used. It is perfectly okay to use one and the same letter for both of them, e.g., to write $\sum_{s \in T} a_s = \sum_{s \in S} a_{f(s)}$.

- Here is the probably most famous example of substitution in a sum: Fix a nonnegative integer $n$. Then, we can substitute $n - i$ for $i$ in the sum $\sum_{i=0}^{n} i$ (since the map $\{0,1,\ldots,n\} \rightarrow \{0,1,\ldots,n\}$, $i \mapsto n - i$ is a bijection). Thus, we obtain
\[ \sum_{i=0}^{n} i = \sum_{i=0}^{n} (n - i). \]

\[\text{Check this!}\]
Now,
\[2 \sum_{i=0}^{n} i = \sum_{i=0}^{n} i + \sum_{i=0}^{n} i = \sum_{i=0}^{n} (n-i)\]
\[= \sum_{i=0}^{n} i + \sum_{i=0}^{n} (n-i)\]
\[= \sum_{i=0}^{n} (i + (n - i)) = n\]
\[= n \sum_{i=0}^{n} (n+1)\]
\[= n (n+1),\]
and therefore
\[\sum_{i=0}^{n} i = \frac{n (n+1)}{2}. \quad (11)\]

Since \[\sum_{i=0}^{n} i = 0 + \sum_{i=1}^{n} i = \sum_{i=1}^{n} i,\] this rewrites as
\[\sum_{i=1}^{n} i = \frac{n (n+1)}{2}. \quad (12)\]

• **Substituting the index II:** Let \(S\) and \(T\) be two finite sets. Let \(f : S \rightarrow T\) be a bijective map. Let \(a_s\) be an element of \(A\) for each \(s \in S\). Then,
\[\sum_{s \in S} a_s = \sum_{t \in f} a_{f^{-1}(t)}. \quad (13)\]
This is, of course, just (10) but applied to \(T, S\) and \(f^{-1}\) instead of \(S, T\) and \(f\). (Nevertheless, I prefer to mention (13) separately because it often is used in this very form.)

• **Telescoping sums:** Let \(u\) and \(v\) be two integers such that \(u - 1 \leq v\). Let \(a_s\) be an element of \(A\) for each \(s \in \{u - 1, u, \ldots, v\}\). Then,
\[\sum_{s=u}^{v} (a_s - a_{s-1}) = a_v - a_{u-1}. \quad (14)\]

Examples:
Let us give a new proof of (12). Indeed, fix a nonnegative integer $n$. An easy computation reveals that

$$s = \frac{s(s+1)}{2} - \frac{(s-1)((s-1)+1)}{2}$$

(15)

for each $s \in \mathbb{Z}$. Thus,

$$\sum_{i=1}^{n} i = \sum_{s=1}^{n} s = \sum_{s=1}^{n} \left( \frac{s(s+1)}{2} - \frac{(s-1)((s-1)+1)}{2} \right) \quad \text{(by (15))}$$

$$= \frac{n(n+1)}{2} - \frac{(1-1)((1-1)+1)}{2}$$

(by (14), applied to $u = 1$, $v = n$ and $a_s = \frac{s(s+1)}{2}$)

$$= \frac{n(n+1)}{2}.$$  

Thus, (12) is proven again. This kind of proof works often when we need to prove a formula like (12); the only tricky part was to “guess” the right value of $a_s$, which is straightforward if you know what you are looking for (you want $a_n - a_1$ to be $\frac{n(n+1)}{2}$), but rather tricky if you don’t.

- Other examples for the use of (14) can be found on the Wikipedia page for “telescoping series”. Let me add just one more example: Given $n \in \mathbb{N}$, we want to compute $\sum_{i=1}^{n} \frac{1}{\sqrt{i} + \sqrt{i+1}}$. (Here, of course, we need to take $A = \mathbb{R}$ or $A = \mathbb{C}$.) We proceed as follows: For every positive integer $i$, we have

$$\frac{1}{\sqrt{i} + \sqrt{i+1}} = \frac{\sqrt{i+1} - \sqrt{i}}{\sqrt{i} + \sqrt{i+1}(\sqrt{i+1} - \sqrt{i})} = \sqrt{i+1} - \sqrt{i}$$

(since $\left(\sqrt{i} + \sqrt{i+1}\right) \left(\sqrt{i+1} - \sqrt{i}\right) = \left(\sqrt{i+1}\right)^2 - \left(\sqrt{i}\right)^2 = (i+1) -$...
Thus, 
\[ \sum_{i=1}^{n} \frac{1}{\sqrt{i + \sqrt{i + 1}}} = \sum_{s=2}^{n+1} \left( \sqrt{s - \sqrt{s - 1}} \right) \]

here, we have substituted \( s - 1 \) for \( i \) in the sum, since the map \( \{2, 3, \ldots, n + 1\} \to \{1, 2, \ldots, n\}, s \mapsto s - 1 \) is a bijection

\[ = \sqrt{n + 1} - \frac{\sqrt{2} - 1}{\sqrt{1}} = \sqrt{n + 1} - 1. \]

**Remark:** When we use the equality (14) to rewrite the sum \( \sum_{s=0}^{v} (a_s - a_{s-1}) \) as \( a_v - a_{u-1} \), we can say that the sum \( \sum_{s=0}^{u} (a_s - a_{s-1}) \) “telescopes” to \( a_v - a_{u-1} \).

A sum like \( \sum_{s=0}^{v} (a_s - a_{s-1}) \) is said to be a “telescoping sum”. This terminology references the idea that the sum \( \sum_{s=0}^{v} (a_s - a_{s-1}) \) “shrink” to the simple difference \( a_v - a_{u-1} \) like a telescope does when it is collapsed.

**Splitting a sum by a value of a function:** Let \( S \) be a finite set. Let \( W \) be a set. Let \( f : S \to W \) be a map. Then,

\[ \sum_{s \in S} a_s = \sum_{w \in W} \sum_{s \in S; f(s)=w} a_s. \quad (16) \]

The idea behind this formula is the following: The left hand side is the sum of all \( a_s \) for \( s \in S \). The right hand side is the same sum, but split in a particular way: First, for each \( w \in W \), we sum the \( a_s \) for all \( s \in S \) satisfying \( f(s) = w \), and then we take the sum of all these “partial sums”.

**Examples:**
- Let \( n \in \mathbb{N} \). Then,

\[ \sum_{s \in \{-n, -(n-1), \ldots, n\}} s^3 = \sum_{w \in \{0, 1, \ldots, n\}} \sum_{s \in \{-n, -(n-1), \ldots, n\}; |s|=w} s^3. \quad (17) \]

(This follows from (16), applied to \( S = \{-n, -(n-1), \ldots, n\}, W = \{0, 1, \ldots, n\} \) and \( f(s) = |s|. \) You might wonder what you gain by this
observation. But actually, it allows you to compute the sum: For any $w \in \{0, 1, \ldots, n\}$, the sum $\sum_{s \in \{-n, -(n-1), \ldots, n\}; |s| = w} s^3$ is 0, and therefore (17) becomes

$$\sum_{s \in \{-n, -(n-1), \ldots, n\}} s^3 = \sum_{w \in \{0, 1, \ldots, n\}} \sum_{s \in \{-n, -(n-1), \ldots, n\}; |s| = w} s^3 = \sum_{w \in \{0, 1, \ldots, n\}} 0 = 0.$$ 

Thus, a strategic application of (16) can help in evaluating a sum.

- Let $S$ be a finite set. Let $W$ be a set. Let $f: S \rightarrow W$ be a map. If we apply (16) to $a_s = 1$, then we obtain

$$\sum_{s \in S} 1 = \sum_{w \in W} \sum_{s \in S; f(s) = w} 1 = \sum_{w \in W} |\{s \in S \mid f(s) = w\}|.$$

Since $\sum_{s \in S} 1 = |S| \cdot 1 = |S|$, this rewrites as follows:

$$|S| = \sum_{w \in W} |\{s \in S \mid f(s) = w\}|. \quad (18)$$

This equality is often called the shepherd’s principle, because it is connected to the joke that “in order to count a flock of sheep, just count the legs and divide by 4”. The connection is somewhat weak, actually; the equality (18) is better regarded as a formalization of the (less funny) idea that in order to count all legs of a flock of sheep, you can count the legs of every single sheep, and then sum the resulting numbers over all sheep in the flock. Think of the $S$ in (18) as the set of all legs of all sheep in the flock; think of $W$ as the set of all sheep in the flock; and think of $f$ as the function which sends every leg to the (hopefully uniquely determined) sheep it belongs to.

Remarks:

- If $f: S \rightarrow W$ is a map between two sets $S$ and $W$, and if $w$ is an element of $W$, then it is common to denote the set $\{s \in S \mid f(s) = w\}$ by $f^{-1}(w)$. (Formally speaking, this notation might clash with the notation $f^{-1}(w)$)

13Proof. If $w = 0$, then this sum $\sum_{s \in \{-n, -(n-1), \ldots, n\}; |s| = w} s^3$ consists of one addend only, and this addend is $0^3$. If $w > 0$, then this sum has two addends, namely $(-w)^3$ and $w^3$. In either case, the sum is 0 (because $0^3 = 0$ and $(-w)^3 + w^3 = -w^3 + w^3 = 0$).
for the actual preimage of \( w \) when \( f \) happens to be bijective; but in practice, this causes far less confusion than it might seem to.) Using this notation, we can rewrite (16) as follows:

\[
\sum_{s \in S} a_s = \sum_{w \in W} \sum_{s \in S; f(s) = w} a_s = \sum_{w \in W} \sum_{s \in f^{-1}(w)} a_s. \tag{19}
\]

- When I rewrite a sum \( \sum_{s \in S} a_s \) as \( \sum_{w \in W} \sum_{s \in S; f(s) = w} a_s \) (or as \( \sum_{w \in W} \sum_{s \in f^{-1}(w)} a_s \)), I say that I am “splitting the sum according to the value of \( f(s) \)”.

(Though, most of the time, I shall be doing such manipulations without explicit mention.)

• **Splitting a sum into subsums:** Let \( S \) be a finite set. Let \( S_1, S_2, \ldots, S_n \) be finitely many subsets of \( S \). Assume that these subsets \( S_1, S_2, \ldots, S_n \) are pairwise disjoint (i.e., we have \( S_i \cap S_j = \emptyset \) for any two distinct elements \( i \) and \( j \) of \( \{1, 2, \ldots, n\} \)) and their union is \( S \). (Thus, every element of \( S \) lies in precisely one of the subsets \( S_1, S_2, \ldots, S_n \).) Let \( a_s \) be an element of \( A \) for each \( s \in S \). Then,

\[
\sum_{s \in S} a_s = \sum_{w=1}^{n} \sum_{s \in S_w} a_s. \tag{20}
\]

This is a generalization of (3) (indeed, (3) is obtained from (20) by setting \( n = 2, S_1 = X \) and \( S_2 = Y \)). It is also a consequence of (16): Indeed, set \( W = \{1, 2, \ldots, n\} \), and define a map \( f : S \to W \) to send each \( s \in S \) to the unique \( w \in \{1, 2, \ldots, n\} \) for which \( s \in S_w \). Then, every \( w \in W \) satisfies \( \sum_{s \in S; f(s) = w} a_s = \sum_{s \in S_w} a_s \); therefore, (16) becomes (20).

**Example:** If we set \( a_s = 1 \) for each \( s \in S \), then (20) becomes

\[
\sum_{s \in S} 1 = \sum_{w=1}^{n} \sum_{s \in S_w} 1 = \sum_{w=1}^{n} |S_w|. \]

Hence,

\[
\sum_{w=1}^{n} |S_w| = \sum_{s \in S} 1 = |S|. \]

• **Fubini’s theorem (interchanging the order of summation):** Let \( X \) and \( Y \) be two finite sets. Let \( a_{(x,y)} \) be an element of \( A \) for each \( (x,y) \in X \times Y \). Then,

\[
\sum_{x \in X} \sum_{y \in Y} a_{(x,y)} = \sum_{(x,y) \in X \times Y} a_{(x,y)} = \sum_{y \in Y} \sum_{x \in X} a_{(x,y)}. \tag{21}
\]
This is called *Fubini's theorem for finite sums*, and is a lot easier to prove than what analysts tend to call Fubini’s theorem. I shall sketch a proof shortly (in the Remark below); but first, let me give some intuition for the statement. Imagine that you have a rectangular table filled with numbers. If you want to sum the numbers in the table, you can proceed in several ways. One way is to sum the numbers in each row, and then sum all the sums you have obtained. Another way is to sum the numbers in each column, and then sum all the obtained sums. Either way, you get the same result – namely, the sum of all numbers in the table. This is essentially what (21) says, at least when $X = \{1, 2, \ldots, n\}$ and $Y = \{1, 2, \ldots, m\}$ for some integers $n$ and $m$. In this case, the numbers $a_{(x,y)}$ can be viewed as forming a table, where $a_{(x,y)}$ is placed in the cell at the intersection of row $x$ with column $y$. When $X$ and $Y$ are arbitrary finite sets (not necessarily $\{1, 2, \ldots, n\}$ and $\{1, 2, \ldots, m\}$), then you need to slightly stretch your imagination in order to see the $a_{(x,y)}$ as “forming a table”; in fact, there is no obvious order in which the numbers appear in a row or column, but there is still a notion of rows and columns.

**Examples:**

- Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $a_{(x,y)}$ be an element of $A$ for each $(x,y) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$. Then,
  \[
  \sum_{x=1}^{n} \sum_{y=1}^{m} a_{(x,y)} = \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} a_{(x,y)} = \sum_{y=1}^{m} \sum_{x=1}^{n} a_{(x,y)}. \quad (22)
  \]
  (This follows from (21), applied to $X = \{1, 2, \ldots, n\}$ and $Y = \{1, 2, \ldots, m\}$.) We can rewrite the equality (22) without using $\sum$ signs; it then takes the following form:

  \[
  \left( a_{(1,1)} + a_{(1,2)} + \cdots + a_{(1,m)} \right) \\
  \quad + \left( a_{(2,1)} + a_{(2,2)} + \cdots + a_{(2,m)} \right) \\
  \quad + \cdots \\
  \quad + \left( a_{(n,1)} + a_{(n,2)} + \cdots + a_{(n,m)} \right) \\
  = a_{(1,1)} + a_{(1,2)} + \cdots + a_{(n,m)} \quad \text{(this is the sum of all $nm$ numbers $a_{(x,y)}$)}
  \]

  \[
  = \left( a_{(1,1)} + a_{(2,1)} + \cdots + a_{(n,1)} \right) \\
  \quad + \left( a_{(1,2)} + a_{(2,2)} + \cdots + a_{(n,2)} \right) \\
  \quad + \cdots \\
  \quad + \left( a_{(1,m)} + a_{(2,m)} + \cdots + a_{(n,m)} \right) .
  \]

- Here is a concrete application of (22): Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. We want to compute

  \[
  \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} xy. \quad \text{(This is the sum of all entries of the}
  \]


\( n \times m \) multiplication table.) Applying (22) to \( a_{(x,y)} = xy \), we obtain

\[
\sum_{x=1}^{n} \sum_{y=1}^{m} xy = \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} xy = \sum_{y=1}^{m} \sum_{x=1}^{n} xy.
\]

Hence,

\[
\sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} xy
= \sum_{x=1}^{n} \sum_{y=1}^{m} xy
= \sum_{x=1}^{n} x \sum_{s=1}^{m} s
= \sum_{s=1}^{m} s \sum_{x=1}^{n} x
= \sum_{s=1}^{m} m (m + 1) s / 2
= \frac{m (m + 1)}{2} \sum_{s=1}^{n} s
= \frac{m (m + 1)}{2} \frac{n (n + 1)}{2}
= \frac{m (m + 1)}{2} \cdot \frac{n (n + 1)}{2}.
\]

Remarks:

- I have promised to outline a proof of (21). Here it comes: Let \( S = X \times Y \) and \( W = Y \), and let \( f : S \to W \) be the map which sends every pair \((x,y)\) to its second entry \( y \). Then, (19) shows that

\[
\sum_{s \in X \times Y} a_s = \sum_{w \in Y} \sum_{s \in f^{-1}(w)} a_s.
\]

But for every given \( w \in Y \), the set \( f^{-1}(w) \) is simply the set of all pairs \((x,w)\) with \( x \in X \). Thus, for every given \( w \in Y \), there is a bijection \( g_w : X \to f^{-1}(w) \) given by

\[
g_w(x) = (x,w) \quad \text{for all } x \in X.
\]
Hence, for every given \( w \in Y \), we can substitute \( g_w(x) \) for \( s \) in the sum \( \sum_{s \in f^{-1}(w)} a_s \), and thus obtain

\[
\sum_{s \in f^{-1}(w)} a_s = \sum_{x \in X} a_{g_w(x)} = \sum_{x \in X} a_{(x,w)}.
\]

(since \( g_w(x) = (x,w) \))

Hence, (23) becomes

\[
\sum_{s \in X \times Y} a_s = \sum_{w \in Y} \sum_{s \in f^{-1}(w)} a_s = \sum_{w \in Y} \sum_{x \in X} a_{(x,w)} = \sum_{x \in X} \sum_{w \in Y} a_{(x,w)}.
\]

(here, we have renamed the summation index \( w \) as \( y \) in the outer sum). Therefore,

\[
\sum_{y \in Y} \sum_{x \in X} a_{(x,y)} = \sum_{s \in X \times Y} a_s = \sum_{(x,y) \in X \times Y} a_{(x,y)}
\]

(here, we have renamed the summation index \( s \) as \( (x,y) \)). Thus, we have proven the second part of the equality (21). The first part can be proven similarly.

- I like to abbreviate the equality (22) as follows:

\[
\sum_{x=1}^{n} \sum_{y=1}^{m} a_{(x,y)} = \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} a_{(x,y)} = \sum_{y=1}^{m} \sum_{x=1}^{n} a_{(x,y)}.
\]

(24)

This is an “equality between summation signs”; it should be understood as follows: Every time you see an “\( \sum_{x=1}^{n} \sum_{y=1}^{m} \)” in an expression, you can replace it by a “\( \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}} \)” or by a “\( \sum_{y=1}^{m} \sum_{x=1}^{n} \)”, and similarly the other ways round.

- **Triangular Fubini’s theorem I**: The equality (22) formalizes the idea that we can sum the entries of a rectangular table by first tallying each row and then adding together, or first tallying each column and adding together. The same holds for triangular tables. More precisely: Let \( n \in \mathbb{N} \). Let \( T_n \) be the set \( \{(x,y) \in \{1,2,3,\ldots\}^2 \mid x + y \leq n\} \). (For instance, if \( n = 3 \), then \( T_3 = \{(1,1),(1,2),(2,1)\}\).) Let \( a_{(x,y)} \) be an element of \( \mathcal{A} \) for each \( (x,y) \in T_n \). Then,

\[
\sum_{x=1}^{n} \sum_{y=1}^{n-x} a_{(x,y)} = \sum_{(x,y) \in T_n} a_{(x,y)} = \sum_{y=1}^{n} \sum_{x=1}^{n-y} a_{(x,y)}.
\]

(25)

Examples:
In the case when \( n = 4 \), the formula (25) (rewritten without the use of \( \sum \) signs) looks as follows:

\[
(a_{(1,1)} + a_{(2,1)} + a_{(3,1)}) + (a_{(2,1)} + a_{(2,2)}) + a_{(3,1)}
\]

\[
= \text{(the sum of the } a_{(x,y)} \text{ for all } (x,y) \in T_4) \]

\[
= (a_{(1,1)} + a_{(2,1)} + a_{(3,1)}) + (a_{(2,1)} + a_{(2,2)}) + a_{(1,3)}.
\]

Let us use (25) to compute \( |T_n| \). Indeed, we can apply (25) to \( a_{(x,y)} = 1 \). Thus, we obtain

\[
\sum_{x=1}^{n} \sum_{y=1}^{n-x} 1 = \sum_{(x,y) \in T_n} 1 = \sum_{y=1}^{n} \sum_{x=1}^{n-y} 1.
\]

Hence,

\[
\sum_{x=1}^{n} \sum_{y=1}^{n-x} 1 = \sum_{(x,y) \in T_n} 1 = |T_n|,
\]

so that

\[
|T_n| = \sum_{x=1}^{n} \sum_{y=1}^{n-x} 1 = \sum_{x=1}^{n} (n - x) = \sum_{i=0}^{n-1} i
\]

\[
= \frac{(n - 1)(n - 1) + 1}{2} \quad \text{(by (11), applied to } n - 1 \text{ instead of } n) \]

\[
= \frac{(n - 1)n}{2}.
\]

Remarks:

- The sum \( \sum_{(x,y) \in T_n} a_{(x,y)} \) in (25) can also be rewritten as \( \sum_{x+y \leq n} a_{(x,y)} \).

- Let us prove (25). Indeed, the proof will be very similar to our proof of (21) above. Let \( S = T_n \) and \( W = \{1,2,\ldots,n\} \), and let \( f : S \to W \) be the map which sends every pair \( (x,y) \) to its second entry \( y \). Then, (19) shows that

\[
\sum_{s \in T_n} a_s = \sum_{w \in W} \sum_{s \in f^{-1}(w)} a_s.
\]

(26)
But for every given \( w \in W \), the set \( f^{-1}(w) \) is simply the set of all pairs \((x, w)\) with \( x \in \{1, 2, \ldots, n - w\}\). Thus, for every given \( w \in W \), there is a bijection \( g_w : \{1, 2, \ldots, n - w\} \to f^{-1}(w) \) given by

\[
g_w(x) = (x, w) \quad \text{for all } x \in \{1, 2, \ldots, n - w\}.
\]

Hence, for every given \( w \in W \), we can substitute \( g_w(x) \) for \( s \) in the sum \( \sum_{s \in f^{-1}(w)} a_s \), and thus obtain

\[
\sum_{s \in f^{-1}(w)} a_s = \sum_{x \in \{1, 2, \ldots, n - w\}} \sum_{s = g_w(x)} a_{g_w(x)} = \sum_{x = 1}^{n - w} a_{(x, w)}\]

(here, we have renamed the summation index \( w \) as \( y \) in the outer sum). Therefore,

\[
\sum_{y = 1}^{n} \sum_{x = 1}^{n - y} a_{(x, y)} = \sum_{s \in T_n} a_s = \sum_{(x, y) \in T_n} a_{(x, y)}.
\]

Thus, we have proven the second part of the equality (25). The first part can be proven similarly.

- **Triangular Fubini’s theorem II**: Here is another equality similar to (25). Let \( n \in \mathbb{N} \). Let \( Q_n \) be the set \( \{(x, y) \in \{1, 2, \ldots, n\}^2 \mid x \leq y\} \). (For instance, if \( n = 3 \), then \( Q_n = Q_3 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}.\) Let \( a_{(x, y)} \) be an element of \( \mathbb{A} \) for each \((x, y) \in Q_n\). Then,

\[
\sum_{x = 1}^{n} \sum_{y = x}^{n} a_{(x, y)} = \sum_{(x, y) \in Q_n} a_{(x, y)} = \sum_{y = 1}^{n} \sum_{x = 1}^{y} a_{(x, y)}.
\]

**Examples:**

- Let us use (27) to compute \(|Q_n|\). Indeed, we can apply (27) to \( a_{(x, y)} = 1 \). Thus, we obtain

\[
\sum_{x = 1}^{n} \sum_{y = x}^{n} 1 = \sum_{(x, y) \in Q_n} 1 = \sum_{y = 1}^{n} \sum_{x = 1}^{y} 1.
\]
Hence,
\[
\sum_{y=1}^{n} \sum_{x=1}^{y} \frac{1}{y^2} = \sum_{y=1}^{n} \frac{1}{y^2} = |Q_n|,
\]
so that
\[
|Q_n| = \sum_{y=1}^{n} \sum_{x=1}^{y} 1 = \sum_{y=1}^{n} y = \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \text{(by (12)).}
\]

Remarks:
- The sum \( \sum_{(x,y) \in Q_n} a(x,y) \) in (27) can also be rewritten as \( \sum_{x \leq y} a(x,y) \).

It is also often written as \( \sum_{1 \leq x \leq y \leq n} a(x,y) \).
- The proof of (27) is similar to that of (25).

\begin{itemize}
  \item **Fubini’s theorem with a predicate:** Let \( X \) and \( Y \) be two finite sets. For every pair \((x, y) \in X \times Y\), let \( A(x, y) \) be a logical statement. For each \((x, y) \in X \times Y\) satisfying \( A(x, y) \), let \( a(x,y) \) be an element of \( A \). Then,
    \[
    \sum_{x \in X} \sum_{y \in Y; A(x,y)} a(x,y) = \sum_{(x,y) \in X \times Y; A(x,y)} a(x,y) = \sum_{y \in Y} \sum_{x \in X; A(x,y)} a(x,y). \tag{28}
    \]

    Examples:
    - For any \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \), we have
      \[
      \sum_{x \in \{1,2,\ldots,n\}; y \in \{1,2,\ldots,m\}; x+y \text{ is even}} xy = \sum_{(x,y) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}; x+y \text{ is even}} xy = \sum_{y \in \{1,2,\ldots,m\}} \sum_{x \in \{1,2,\ldots,n\}; x+y \text{ is even}} xy.
      \]

      (This follows from (28), applied to \( X = \{1,2,\ldots,n\}, Y = \{1,2,\ldots,m\} \) and \( A(x, y) = (\text{“}x+\text{y is even”}) \).)
  \end{itemize}

- **Interchange of predicates:** Let \( S \) be a finite set. For every \( s \in S \), let \( A(s) \) and \( B(s) \) be two equivalent logical statements. (“Equivalent” means that \( A(s) \) holds if and only if \( B(s) \) holds.) Let \( a_s \) be an element of \( A \) for each \( s \in S \). Then,
    \[
    \sum_{s \in S; A(s)} a_s = \sum_{s \in S; B(s)} a_s.
    \]

    (If you regard equivalent logical statements as identical, then you will see this as a tautology. If not, it is still completely obvious, since the equivalence of \( A(s) \) with \( B(s) \) shows that \( \{t \in S \mid A(t)\} = \{t \in S \mid B(t)\} \).)
1.3.3. Definition of $\prod$

We shall now define the $\prod$ sign. Since the $\prod$ sign is (in many aspects) analogous to the $\sum$ sign, we shall be brief and confine ourselves to the bare necessities; we trust the reader to transfer most of what we said about $\sum$ to the case of $\prod$. In particular, we shall give very few examples and no proofs.

- If $S$ is a finite set, and if $a_s$ is an element of $A$ for each $s \in S$, then $\prod_{s \in S} a_s$ denotes the product of all of these elements $a_s$. Formally, this product is defined by recursion on $|S|$, as follows:

  - If $S = \emptyset$, then $\prod_{s \in S} a_s$ is defined to be 1.

  - Let $n \in \mathbb{N}$. Assume that we have defined $\prod_{s \in S} a_s$ for every finite set $S$ with $|S| = n$ (and every choice of elements $a_s$ of $A$). Now, if $S$ is a finite set with $|S| = n + 1$ (and if $a_s \in A$ are chosen for all $s \in S$), then $\prod_{s \in S} a_s$ is defined by picking any $t \in S$ and setting

    $\prod_{s \in S} a_s = a_t \cdot \prod_{s \in S \setminus \{t\}} a_s.$  

(29)

As for $\sum a_s$, this definition is not obviously legitimate, but it can be proven to be legitimate nevertheless.

Examples:

- If $S = \{1, 2, \ldots, n\}$ (for some $n \in \mathbb{N}$) and $a_s = s$ for every $s \in S$, then $\prod_{s \in S} s = 1 \cdot 2 \cdot \cdots \cdot n$. This number $1 \cdot 2 \cdot \cdots \cdot n$ is denoted by $n!$ and called the factorial of $n$.

Remarks:

- The product $\prod_{s \in S} a_s$ is usually pronounced “product of the $a_s$ over all $s \in S$” or “product of the $a_s$ with $s$ ranging over $S$” or “product of the $a_s$ with $s$ running through all elements of $S$”. The letter “$s$” in the product is called the “product index”, and its exact choice is immaterial, as long as it does not already have a different meaning outside of the product. The sign $\prod$ itself is called “the product sign” or “the $\prod$ sign”. The numbers $a_s$ are called the factors of the product $\prod_{s \in S} a_s$. More precisely, for any given $t \in S$, we can refer to the number $a_t$ as the “factor corresponding to the index $t$” (or as the “factor for $s = t$”, or as the “factor for $t$”) of the product $\prod_{s \in S} a_s$. 


When the set $S$ is empty, the product $\prod_{s \in S} a_s$ is called an **empty product**. Our definition implies that any empty product is 1. This convention is used throughout mathematics, except in rare occasions where a slightly subtler version of it is used.\(^{14}\)

If $a \in A$ and $n \in \mathbb{N}$, then the $n$-th power of $a$ (written $a^n$) is defined by

$$a^n = a \cdot a \cdots a = \prod_{i \in \{1,2,\ldots,n\}} a.$$  

Thus, $a^0$ is an empty product, and therefore equal to 1. This holds for any $a \in A$, including 0; thus, $0^0 = 1$. **There is nothing controversial about the equality $0^0 = 1$;** it is a consequence of the only reasonable definition of the $n$-th power of a number. If anyone tells you that $0^0$ is “undefined” or “indeterminate” or “can be 0 or 1 or anything, depending on the context”, do not listen to them.\(^{15}\)

The product index (just like a summation index) needs not be a single letter; it can be a pair or a triple, for example.

Mathematicians don’t seem to have reached an agreement on the operator precedence of the $\prod$ sign. My convention is that the product sign has higher precedence than the plus sign (so an expression like $\prod_{s \in S} a_s + b$ must be read as $\left(\prod_{s \in S} a_s\right) + b$, and not as $\prod_{s \in S} \left(a_s + b\right)$); this is, of course, in line with the standard convention that multiplication-like operations have higher precedence than addition-like operations (“PEMDAS”). Be warned that some authors disagree even with this convention. I strongly advise against writing things like $\prod_{s \in S} a_s b$, since it might mean both $\left(\prod_{s \in S} a_s\right) b$ and $\prod_{s \in S} \left(a_s b\right)$ depending on the weather. In particular, I advise against writing things like $\prod_{s \in S} a_s \cdot \prod_{s \in S} b_s$ without parentheses (although I do use a similar convention for sums, namely $\sum_{s \in S} a_s + \sum_{s \in S} b_s$, and I find it to be fairly harmless). These rules are not carved in stone, and you should use whatever conventions make you safe from ambiguity; either way, you should keep in mind that other authors make different choices.

We have required the set $S$ to be finite when defining $\prod_{s \in S} a_s$. Such products are not generally defined when $S$ is infinite. However, **some** infinite

\(^{14}\)Just as with sums, the subtlety lies in the fact that mathematicians sometimes want an empty product to be not the integer 1 but the unity of some ring. As before, this does not matter for us right now.

\(^{15}\)I am talking about the **number** $0^0$ here. There is also something called “the indeterminate form $0^0$”, which is a much different story.
products can be made sense of. The simplest case is when the set $S$ might be infinite, but only finitely many among the $a_s$ are distinct from 1. In this case, we can define $\prod_{s \in S} a_s$ simply by discarding the factors which equal 1 and multiplying the finitely many remaining factors. Other situations in which infinite products make sense appear in analysis and in topological algebra.

- The product $\prod_{s \in S} a_s$ always belongs to $A$.

- A slightly more complicated version of the product sign is the following: Let $S$ be a finite set, and let $A(s)$ be a logical statement defined for every $s \in S$. For each $s \in S$ satisfying $A(s)$, let $a_s$ be an element of $A$. Then, the product $\prod_{s \in S, A(s)} a_s$ is defined by

$$\prod_{s \in S, A(s)} a_s = \prod_{s \in \{t \in S \mid A(t)\}} a_s.$$

- Finally, here is the simplest version of the product sign: Let $u$ and $v$ be two integers. As before, we understand the set $\{u, u+1, \ldots, v\}$ to be empty when $u > v$. Let $a_s$ be an element of $A$ for each $s \in \{u, u+1, \ldots, v\}$. Then, $\prod_{s=u}^{v} a_s$ is defined by

$$\prod_{s=u}^{v} a_s = \prod_{s \in \{u, u+1, \ldots, v\}} a_s.$$

Examples:

- We have $\prod_{s=1}^{n} s = 1 \cdot 2 \cdots n = n!$ for each $n \in \mathbb{N}$.

Remarks:

- The product $\prod_{s=u}^{v} a_s$ is usually pronounced “product of the $a_s$ for all $s$ from $u$ to $v$ (inclusive)”. It is often written $a_u \cdot a_{u+1} \cdots a_v$ (or just $a_u a_{u+1} \cdots a_v$), but this latter notation has the same drawbacks as the similar notation $a_u + a_{u+1} + \cdots + a_v$ for $\sum_{s=u}^{v} a_s$.

- The product $\prod_{s=u}^{v} a_s$ is said to be empty whenever $u > v$. As with sums, it does not matter how much smaller $v$ is than $u$; as long as $v$ is smaller than $u$, the product is empty and equals 1.

Thus we have introduced the main three forms of the product sign.
1.3.4. Properties of $\prod$

Now, let me summarize the most important properties of the $\prod$ sign. These properties mirror the properties of $\sum$ discussed before; thus, I will again be brief.

- **Splitting-off**: Let $S$ be a finite set. Let $t \in S$. Let $a_s$ be an element of $A$ for each $s \in S$. Then,
  \[
  \prod_{s \in S} a_s = a_t \cdot \prod_{s \in S \setminus \{t\}} a_s.
  \]

- **Splitting**: Let $S$ be a finite set. Let $X$ and $Y$ be two subsets of $S$ such that $X \cap Y = \emptyset$ and $X \cup Y = S$. (Equivalently, $X$ and $Y$ are two subsets of $S$ such that each element of $S$ lies in exactly one of $X$ and $Y$.) Let $a_s$ be an element of $A$ for each $s \in S$. Then,
  \[
  \prod_{s \in S} a_s = \left( \prod_{s \in X} a_s \right) \cdot \left( \prod_{s \in Y} a_s \right).
  \]

- **Splitting using a predicate**: Let $S$ be a finite set. Let $A(s)$ be a logical statement for each $s \in S$. Let $a_s$ be an element of $A$ for each $s \in S$. Then,
  \[
  \prod_{s \in S} a_s = \left( \prod_{s \in S; A(s)} a_s \right) \cdot \left( \prod_{s \in S; \text{not } A(s)} a_s \right).
  \]

- **Multiplying equal values**: Let $S$ be a finite set. Let $a$ be an element of $A$. Then,
  \[
  \prod_{s \in S} a = a^{|S|}.
  \]

- **Splitting a factor**: Let $S$ be a finite set. For every $s \in S$, let $a_s$ and $b_s$ be elements of $A$. Then,
  \[
  \prod_{s \in S} (a_s b_s) = \left( \prod_{s \in S} a_s \right) \cdot \left( \prod_{s \in S} b_s \right).
  \] (30)

**Examples:**

- Here is a frequently used particular case of (30): Let $S$ be a finite set. For every $s \in S$, let $b_s$ be an element of $A$. Let $a$ be an element of $A$. Then, (30) (applied to $a_s = a$) yields
  \[
  \prod_{s \in S} (a b_s) = \left( \prod_{s \in S} a \right) \cdot \left( \prod_{s \in S} b_s \right) = a^{|S|} \cdot \left( \prod_{s \in S} b_s \right).
  \] (31)
Here is an even further particular case: Let $S$ be a finite set. For every $s \in S$, let $b_s$ be an element of $\mathbb{A}$. Then,

$$\prod_{s \in S} (-b_s) = \prod_{s \in S} ((-1) b_s) = (-1)^{|S|} \cdot \left( \prod_{s \in S} b_s \right)$$

(by (31), applied to $a = -1$).

- **Factoring out an exponent:** Let $S$ be a finite set. For every $s \in S$, let $a_s$ be an element of $\mathbb{A}$. Also, let $\lambda \in \mathbb{N}$. Then,

$$\prod_{s \in S} a_s^\lambda = \left( \prod_{s \in S} a_s \right)^\lambda.$$

- **Ones multiply to one:** Let $S$ be a finite set. Then,

$$\prod_{s \in S} 1 = 1.$$

- **Dropping ones:** Let $S$ be a finite set. Let $a_s$ be an element of $\mathbb{A}$ for each $s \in S$. Let $T$ be a subset of $S$ such that every $s \in T$ satisfies $a_s = 1$. Then,

$$\prod_{s \in S} a_s = \prod_{s \in S \setminus T} a_s.$$

- **Renaming the index:** Let $S$ be a finite set. Let $a_s$ be an element of $\mathbb{A}$ for each $s \in S$. Then,

$$\prod_{s \in S} a_s = \prod_{t \in T} a_t.$$

- **Substituting the index I:** Let $S$ and $T$ be two finite sets. Let $f : S \to T$ be a bijective map. Let $a_t$ be an element of $\mathbb{A}$ for each $t \in T$. Then,

$$\prod_{t \in T} a_t = \prod_{s \in S} a_{f(s)}.$$

- **Substituting the index II:** Let $S$ and $T$ be two finite sets. Let $f : S \to T$ be a bijective map. Let $a_s$ be an element of $\mathbb{A}$ for each $s \in S$. Then,

$$\prod_{s \in S} a_s = \prod_{t \in T} a_{f^{-1}(t)}.$$

- **Telescoping products:** Let $u$ and $v$ be two integers such that $u - 1 \leq v$. Let $a_s$ be an element of $\mathbb{A}$ for each $s \in \{u - 1, u, \ldots, v\}$. Then,

$$\prod_{s = u}^{v} \frac{a_s}{a_{s-1}} = \frac{a_{v}}{a_{u-1}} \quad \text{(32)}$$

(provided that $a_{s-1} \neq 0$ for all $s \in \{u, u + 1, \ldots, v\}$).

Examples:
– Let $n$ be a positive integer. Then,
\[
\prod_{s=2}^{n} \left(1 - \frac{1}{s}\right) = \prod_{s=2}^{n} \frac{1/s}{1/ (s-1)} = \frac{s-1}{s} \frac{1/ (s-1)}{1/ (2-1)}
\]
(by (32), applied to $u = 2, v = n$ and $a_s = 1/s$)
\[= \frac{1}{n}.
\]

- **Splitting a product by a value of a function:** Let $S$ be a finite set. Let $W$ be a
set. Let $f : S \to W$ be a map. Then,
\[
\prod_{s \in S} a_s = \prod_{w \in W} \prod_{\substack{s \in S; \quad f(s) = w}} a_s.
\]
(The right hand side is to be read as $\prod_{w \in W} \left(\prod_{\substack{s \in S; \quad f(s) = w}} a_s\right)$.)

- **Splitting a product into subproducts:** Let $S$ be a finite set. Let $S_1, S_2, \ldots, S_n$
be finitely many subsets of $S$. Assume that these subsets $S_1, S_2, \ldots, S_n$ are
pairwise disjoint (i.e., we have $S_i \cap S_j = \emptyset$ for any two distinct elements $i$
and $j$ of $\{1,2,\ldots, n\}$) and their union is $S$. (Thus, every element of $S$ lies in
precisely one of the subsets $S_1, S_2, \ldots, S_n$.) Let $a_s$ be an element of $A$ for each
$s \in S$. Then,
\[
\prod_{s \in S} a_s = \prod_{w=1}^{n} \prod_{s \in S_w} a_s.
\]

- **Fubini’s theorem (interchanging the order of multiplication):** Let $X$ and $Y$
be two finite sets. Let $a(x,y)$ be an element of $A$ for each $(x,y) \in X \times Y$. Then,
\[
\prod_{x \in X} \prod_{y \in Y} a(x,y) = \prod_{(x,y) \in X \times Y} a(x,y) = \prod_{y \in Y} \prod_{x \in X} a(x,y).
\]

In particular, if $n$ and $m$ are two elements of $\mathbb{N}$, and if $a(x,y)$ is an element of
$A$ for each $(x,y) \in \{1,2,\ldots, n\} \times \{1,2,\ldots, m\}$, then
\[
\prod_{x=1}^{n} \prod_{y=1}^{m} a(x,y) = \prod_{(x,y) \in \{1,2,\ldots, n\} \times \{1,2,\ldots, m\}} a(x,y) = \prod_{y=1}^{m} \prod_{x=1}^{n} a(x,y).
\]
• **Triangular Fubini’s theorem I:** Let \( n \in \mathbb{N} \). Let \( T_n \) be the set \( \left\{ (x, y) \in \{1, 2, 3, \ldots \}^2 \mid x + y \leq n \right\} \). Let \( a_{(x,y)} \) be an element of \( \mathcal{A} \) for each \((x, y) \in T_n \). Then,
\[
\prod_{x=1}^{n} \prod_{y=1}^{n-x} a_{(x,y)} = \prod_{(x,y) \in T_n} a_{(x,y)} = \prod_{y=1}^{n} \prod_{x=1}^{n-y} a_{(x,y)}.
\]

• **Triangular Fubini’s theorem II:** Let \( n \in \mathbb{N} \). Let \( Q_n \) be the set \( \left\{ (x, y) \in \{1, 2, 3, \ldots , n \}^2 \mid x \leq y \right\} \). Let \( a_{(x,y)} \) be an element of \( \mathcal{A} \) for each \((x, y) \in Q_n \). Then,
\[
\prod_{x=1}^{n} \prod_{y=x}^{n} a_{(x,y)} = \prod_{(x,y) \in Q_n} a_{(x,y)} = \prod_{y=1}^{n} \prod_{x=1}^{n-y} a_{(x,y)}.
\]

• **Fubini’s theorem with a predicate:** Let \( X \) and \( Y \) be two finite sets. For every pair \((x, y) \in X \times Y\), let \( A(x, y) \) be a logical statement. For each \((x, y) \in X \times Y\) satisfying \( A(x, y) \), let \( a_{(x,y)} \) be an element of \( \mathcal{A} \). Then,
\[
\prod_{x \in X} \prod_{y \in Y; \ A(x,y)} a_{(x,y)} = \prod_{(x,y) \in X \times Y; \ A(x,y)} a_{(x,y)} = \prod_{y \in Y} \prod_{x \in X; \ A(x,y)} a_{(x,y)}.
\]

• **Interchange of predicates:** Let \( S \) be a finite set. For every \( s \in S \), let \( A(s) \) and \( B(s) \) be two equivalent logical statements. (“Equivalent” means that \( A(s) \) holds if and only if \( B(s) \) holds.) Let \( a_s \) be an element of \( \mathcal{A} \) for each \( s \in S \). Then,
\[
\prod_{s \in S; \ A(s)} a_s = \prod_{s \in S; \ B(s)} a_s.
\]

### 1.4. Polynomials: a precise definition

As I have already mentioned in the above list of prerequisites, the notion of polynomials (in one and in several indeterminates) will be used in these notes. Most likely, the reader already has at least a vague understanding of this notion (e.g., from high school); this vague understanding is probably sufficient for reading most of these notes. But polynomials are one of the most important notions in algebra (if not to say in mathematics), and the reader will likely encounter them over and over; sooner or later, it will happen that the vague understanding is not sufficient and some subtleties do matter. For that reason, anyone serious about doing abstract algebra should know a complete and correct definition of polynomials and have some experience working with it. I shall not give a complete definition of the most general notion of polynomials in these notes, but I will comment on some of the subtleties and define an important special case (that of polynomials in one variable
with rational coefficients) in the present section. A reader is probably best advised to skip this section on their first read.

It is not easy to find a good (formal and sufficiently general) treatment of polynomials in textbooks. Various authors tend to skimp on subtleties and technical points such as the notion of an “indeterminate”, or the precise meaning of “formal expression” in the slogan “a polynomial is a formal expression” (the best texts do not use this vague slogan at all), or the definition of the degree of the zero polynomial, or the difference between regarding polynomials as sequences (which is the classical viewpoint and particularly useful for polynomials in one variable) and regarding polynomials as elements of a monoid ring (which is important in the case of several variables, since it allows us to regard the polynomial rings \( \mathbb{Q}[X] \) and \( \mathbb{Q}[Y] \) as two distinct subrings of \( \mathbb{Q}[X,Y] \)). They also tend to take some questionable shortcuts, such as defining polynomials in \( n \) variables (by induction over \( n \)) as one-variable polynomials over the ring of \( (n-1) \)-variable polynomials (this shortcut has several shortcomings, such as making the symmetric role of the \( n \) variables opaque, and functioning only for finitely many variables).

More often than not, the polynomials we will be using will be polynomials in one variable. These are usually handled well in good books on abstract algebra – e.g., in [Walker87, §4.5], in [Hunger14, Appendix G], in [Hunger03, Chapter III, §5], in [Rotman15, Chapter A-3], in [HoffKun, §4.1, §4.2] (although in [HoffKun, §4.1, §4.2], only polynomials over fields are studied, but the definition applies to commutative rings mutatis mutandis), in [AmaEsc05, §8], and in [BirMac99, Chapter III, §6]. Most of these treatments rely on the notion of a \textit{commutative ring}, which is not difficult but somewhat abstract (I shall introduce it below in Section 6.1).

Let me give a brief survey of the notion of univariate polynomials (i.e., polynomials in one variable). I shall define them as sequences. For the sake of simplicity, I shall only talk of polynomials with rational coefficients. Similarly, one can define polynomials with integer coefficients, with real coefficients, or with complex coefficients; of course, one then has to replace each “\( \mathbb{Q} \)” by a “\( \mathbb{Z} \)”, an “\( \mathbb{R} \)” or a “\( \mathbb{C} \)”.

The rough idea behind the definition of a polynomial is that a polynomial with rational coefficients should be a “formal expression” which is built out of rational numbers, an “indeterminate” \( X \) as well as addition, subtraction and multiplication signs, such as \( X^4 - 27X + \frac{3}{2} \) or \(-X^3 + 2X + 1\) or \( \frac{1}{3} (X - 3) \cdot X^2 \) or \( X^4 + 7X^3 (X - 2) \) or \(-15\). We have not explicitly allowed powers, but we understand \( X^n \) to mean the product \( X \cdots X \) (or 1 when \( n = 0 \)). Notice that division is not allowed, so we cannot get \( \frac{X}{X+1} \) (but we can get \( \frac{3}{2} X \), because \( \frac{3}{2} \) is a rational number). Notice also that a polynomial can be a single rational number, since we never said that \( X \) must necessarily be used; for instance, \(-15\) and 0 are polynomials.

This is, of course, not a valid definition. One problem with it that it does not explain what a “formal expression” is. For starters, we want an expression that is well-defined – i.e., into that we can substitute a rational number for \( X \) and obtain
a valid term. For example, $X - + \cdot 5$ is not well-defined, so it does not fit our bill; neither is the “empty expression”. Furthermore, when do we want two “formal expressions” to be viewed as one and the same polynomial? Do we want to equate $X (X + 2)$ with $X^2 + 2X$? Do we want to equate $0X^3 + 2X + 1$ with $2X + 1$? The answer is “yes” both times, but a general rule is not easy to give if we keep talking of “formal expressions”.

We could define two polynomials $p (X)$ and $q (X)$ to be equal if and only if, for every number $\alpha \in \mathbb{Q}$, the values $p (\alpha)$ and $q (\alpha)$ (obtained by substituting $\alpha$ for $X$ in $p$ and in $q$, respectively) are equal. This would be tantamount to treating polynomials as functions: it would mean that we identify a polynomial $p (X)$ with the function $\mathbb{Q} \rightarrow \mathbb{Q}$, $\alpha \mapsto p (\alpha)$. Such a definition would work well as long as we would do only rather basic things with it, but as soon as we would try to go deeper, we would encounter technical issues which would make it inadequate and painful. Also, if we equated polynomials with the functions they describe, then

---

16 And some authors, such as Axler in [Axler, Chapter 4], do use this definition.
17 Here are the three most important among these issues:

- One of the strengths of polynomials is that we can evaluate them not only at numbers, but also at many other things, e.g., at square matrices: Evaluating the polynomial $X^2 - 3X$ at the square matrix $\begin{pmatrix} 1 & 3 \\ -1 & 2 \end{pmatrix}$ gives $\begin{pmatrix} 1 & 3 \\ -1 & 2 \end{pmatrix}^2 - 3 \begin{pmatrix} 1 & 3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix}$. However, a function must have a well-defined domain, and does not make sense outside of this domain. So, if the polynomial $X^2 - 3X$ is regarded as the function $\mathbb{Q} \rightarrow \mathbb{Q}$, $\alpha \mapsto \alpha^2 - 3\alpha$, then it makes no sense to evaluate this polynomial at the matrix $\begin{pmatrix} 1 & 3 \\ -1 & 2 \end{pmatrix}$, just because this matrix does not lie in the domain $\mathbb{Q}$ of the function. We could, of course, extend the domain of the function to (say) the set of square matrices over $\mathbb{Q}$, but then we would still have the same problem with other things that we want to evaluate polynomials at. At some point we want to be able to evaluate polynomials at functions and at other polynomials, and if we would try to achieve this by extending the domain, we would have to do this over and over, because each time we extend the domain, we get even more polynomials to evaluate our polynomials at; thus, the definition would be eternally “hunting its own tail”! (We could resolve this difficulty by defining polynomials as natural transformations in the sense of category theory. I do not want to even go into this definition here, as it would take several pages to properly introduce. At this point, it is not worth the hassle.)

- Let $p (X)$ be a polynomial with real coefficients. Then, it should be obvious that $p (X)$ can also be viewed as a polynomial with complex coefficients: For instance, if $p (X)$ was defined as $3X + \frac{7}{2}X (X - 1)$, then we can view the numbers $3$, $\frac{7}{2}$ and $-1$ appearing in its definition as complex numbers, and thus get a polynomial with complex coefficients. But wait! What if two polynomials $p (X)$ and $q (X)$ are equal when viewed as polynomials with real coefficients, but when viewed as polynomials with complex coefficients become distinct (because when we view them as polynomials with complex coefficients, their domains become extended, and a new complex $\alpha$ might perhaps no longer satisfy $p (\alpha) = q (\alpha)$)? This does not actually happen, but ruling this out is not obvious if you regard polynomials as functions.

- (This requires some familiarity with finite fields:) Treating polynomials as functions works reasonably well for polynomials with integer, rational, real and complex coefficients (as long as one is not too demanding). But we will eventually want to consider polynomials with coefficients in any arbitrary commutative ring $\mathbb{K}$. An example for a commutative ring $\mathbb{K}$ is...
we would waste the word “polynomial” on a concept (a function described by a polynomial) that already has a word for it (namely, polynomial function).

The preceding paragraphs should have convinced you that it is worth defining “polynomials” in a way that, on the one hand, conveys the concept that they are more “formal expressions” than “functions”, but on the other hand, is less nebulous than “formal expression”. Here is one such definition:

**Definition 1.1. (a)** A univariate polynomial with rational coefficients means a sequence \((p_0, p_1, p_2, \ldots) \in \mathbb{Q}^\infty\) of elements of \(\mathbb{Q}\) such that all but finitely many \(k \in \mathbb{N}\) satisfy \(p_k = 0\). \(\tag{33}\)

Here, the phrase “all but finitely many \(k \in \mathbb{N}\) satisfy \(p_k = 0\)” means “there exists some finite subset \(J\) of \(\mathbb{N}\) such that every \(k \in \mathbb{N} \setminus J\) satisfies \(p_k = 0\).” (See Definition 5.14 for the general definition of “all but finitely many”, and Section 5.4 for some practice with this concept.) More concretely, the condition (33) can be rewritten as follows: The sequence \((p_0, p_1, p_2, \ldots)\) contains only zeroes from some point on (i.e., there exists some \(N \in \mathbb{N}\) such that \(p_N = p_{N+1} = p_{N+2} = \cdots = 0\)).

For the remainder of this definition, “univariate polynomial with rational coefficients” will be abbreviated as “polynomial”.

For example, the sequences \((0, 0, 0, \ldots)\), \((1, 3, 5, 0, 0, 0, \ldots)\), \((4, 0, -\frac{2}{3}, 5, 0, 0, 0, \ldots)\), \((0, -1, \frac{1}{2}, 0, 0, 0, \ldots)\) (where the “…” stand for infinitely many zeroes) are polynomials, but the sequence \((1, 1, 1, \ldots)\) (where the “…” stands for infinitely many 1’s) is not (since it does not satisfy (33)).

So we have defined a polynomial as an infinite sequence of rational numbers with a certain property. So far, this does not seem to reflect any intuition of polynomials as “formal expressions”. However, we shall soon (namely, in **Definition 1.1** (j)) identify the polynomial \((p_0, p_1, p_2, \ldots) \in \mathbb{Q}^\infty\) with the “formal expression” \(p_0 + p_1X + p_2X^2 + \cdots\) (this is an infinite sum, but due to (33) all but its first few terms are 0 and thus can be neglected). For instance, the polynomial \((1, 3, 5, 0, 0, 0, \ldots)\) will be identified with the “formal expression” \(1 + 3X + 5X^2 + 0X^3 + 0X^4 + 0X^5 + \cdots = 1 + 3X + 5X^2\). Of course, we cannot do this identification right now, since we do not have a reasonable definition of \(X\).

(b) We let \(\mathbb{Q}[X]\) denote the set of all univariate polynomials with rational coefficients. Given a polynomial \(p = (p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X]\), we denote the numbers \(p_0, p_1, p_2, \ldots\) as the coefficients of \(p\). More precisely, for every \(i \in \mathbb{N}\), we shall refer to \(p_i\) as the \(i\)-th coefficient of \(p\). (Do not forget that we are counting from the finite field \(\mathbb{F}_p\) with \(p\) elements, where \(p\) is a prime. (This finite field \(\mathbb{F}_p\) is better known as the ring of integers modulo \(p\).) If we define polynomials with coefficients in \(\mathbb{F}_p\) as functions \(\mathbb{F}_p \to \mathbb{F}_p\), then we really run into problems; for example, the polynomials \(X\) and \(X^p\) over this field become identical as functions!
0 here: any polynomial “begins” with its 0-th coefficient.) The 0-th coefficient of p is also known as the constant term of p.

Instead of “the i-th coefficient of p”, we often also say “the coefficient before X^i of p” or “the coefficient of X^i in p”.

Thus, any polynomial p ∈ Q[X] is the sequence of its coefficients.

(c) We denote the polynomial (0, 0, 0, . . .) ∈ Q[X] by 0. We will also write 0 for it when no confusion with the number 0 is possible. The polynomial 0 is called the zero polynomial. A polynomial p ∈ Q[X] is said to be nonzero if p ̸= 0.

(d) We denote the polynomial (1, 0, 0, 0, . . .) ∈ Q[X] by 1. We will also write 1 for it when no confusion with the number 1 is possible.

(e) For any λ ∈ Q, we denote the polynomial (λ, 0, 0, 0, . . .) ∈ Q[X] by const λ. We call it the constant polynomial with value λ. It is often useful to identify λ ∈ Q with const λ ∈ Q[X]. Notice that 0 = const 0 and 1 = const 1.

(f) Now, let us define the sum, the difference and the product of two polynomials. Indeed, let a = (a_0, a_1, a_2, . . .) ∈ Q[X] and b = (b_0, b_1, b_2, . . .) ∈ Q[X] be two polynomials. Then, we define three polynomials a + b, a − b and a · b in Q[X] by

\[
a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots);
\]
\[
a − b = (a_0 − b_0, a_1 − b_1, a_2 − b_2, \ldots);
\]
\[
a · b = (c_0, c_1, c_2, \ldots),
\]

where

\[
c_k = \sum_{i=0}^{k} a_i b_{k−i} \quad \text{for every } k ∈ \mathbb{N}.
\]

We call a + b the sum of a and b; we call a − b the difference of a and b; we call a · b the product of a and b. We abbreviate a · b by ab.

For example,

\[
(1,2,2,0,0,\ldots) + (3,0,−1,0,0,0,\ldots) = (4,2,1,0,0,0,\ldots);
\]
\[
(1,2,2,0,0,\ldots) − (3,0,−1,0,0,0,\ldots) = (−2,2,3,0,0,0,\ldots);
\]
\[
(1,2,2,0,0,\ldots) · (3,0,−1,0,0,0,\ldots) = (3,6,5,−2,−2,0,0,0,\ldots).
\]

The definition of a + b essentially says that “polynomials are added coefficientwise” (i.e., in order to obtain the sum of two polynomials a and b, it suffices to add each coefficient of a to the corresponding coefficient of b). Similarly, the definition of a − b says the same thing about subtraction. The definition of a · b is more surprising. However, it loses its mystique when we identify the polynomials a and b with the “formal expressions” a_0 + a_1 X + a_2 X^2 + · · · and b_0 + b_1 X + b_2 X^2 + · · · (although, at this point, we do not know what these expressions really mean); indeed, it simply says that

\[
(a_0 + a_1 X + a_2 X^2 + · · ·)(b_0 + b_1 X + b_2 X^2 + · · ·) = c_0 + c_1 X + c_2 X^2 + · · ·,
\]
where \( c_k = \sum_{i=0}^{k} a_i b_{k-i} \) for every \( k \in \mathbb{N} \). This is precisely what one would expect, because if you expand \( \left(a_0 + a_1 X + a_2 X^2 + \cdots\right) \left(b_0 + b_1 X + b_2 X^2 + \cdots\right) \) using the distributive law and collect equal powers of \( X \), then you get precisely \( c_0 + c_1 X + c_2 X^2 + \cdots \). Thus, the definition of \( a \cdot b \) has been tailored to make the distributive law hold.

(By the way, why is \( a \cdot b \) a polynomial? That is, why does it satisfy (33)? The proof is easy, but we omit it.)

Addition, subtraction and multiplication of polynomials satisfy some of the same rules as addition, subtraction and multiplication of numbers. For example, the commutative laws \( a + b = b + a \) and \( ab = ba \) are valid for polynomials just as they are for numbers; same holds for the associative laws \( (a + b) + c = a + (b + c) \) and \( (ab)c = a(bc) \) and the distributive laws \( (a + b)c = ac + bc \) and \( a(b + c) = ab + ac \).

The set \( \mathbb{Q}[X] \), endowed with the operations + and \( \cdot \) just defined, and with the elements 0 and 1, is a commutative ring (where we are using the notations of Definition 6.2). It is called the (univariate) polynomial ring over \( \mathbb{Q} \).

(g) Let \( a = (a_0, a_1, a_2, \ldots) \in \mathbb{Q}[X] \) and \( \lambda \in \mathbb{Q} \). Then, \( \lambda a \) denotes the polynomial \( (\lambda a_0, \lambda a_1, \lambda a_2, \ldots) \in \mathbb{Q}[X] \). (This equals the polynomial \( (\text{const } \lambda) \cdot a \); thus, identifying \( \lambda \) with \( \text{const } \lambda \) does not cause any inconsistencies here.)

(h) If \( p = (p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X] \) is a nonzero polynomial, then the degree of \( p \) is defined to be the maximum \( i \in \mathbb{N} \) satisfying \( p_i \neq 0 \). If \( p \in \mathbb{Q}[X] \) is the zero polynomial, then the degree of \( p \) is defined to be \(-\infty \). (Here, \(-\infty \) is just a fancy symbol, not a number.) For example, \( \deg (1, 4, 0, -1, 0, 0, 0, \ldots) = 3 \).

(i) If \( a = (a_0, a_1, a_2, \ldots) \in \mathbb{Q}[X] \) and \( n \in \mathbb{N} \), then a polynomial \( a^n \in \mathbb{Q}[X] \) is defined to be the product \( aa \cdots a \). (This is understood to be 1 when \( n = 0 \). In general, an empty product of polynomials is always understood to be 1.)

(j) We let \( X \) denote the polynomial \((0, 1, 0, 0, 0, \ldots) \in \mathbb{Q}[X]\). (This is the polynomial whose 1-st coefficient is 1 and whose other coefficients are 0.) This polynomial is called the indeterminate of \( \mathbb{Q}[X] \). It is easy to see that, for any \( n \in \mathbb{N} \), we have

\[
X^n = \left(\underbrace{0, 0, \ldots, 0}_{n \text{ zeroes}}, 1, 0, 0, 0, \ldots\right).
\]

This polynomial \( X \) finally provides an answer to the questions “what is an indeterminate” and “what is a formal expression”. Namely, let \((p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X]\) be any polynomial. Then, the sum \( p_0 + p_1 X + p_2 X^2 + \cdots \) is well-defined (it is an infinite sum, but due to (33) it has only finitely many nonzero addends), and it is easy to see that this sum equals \((p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X]\). This finally allows us to write a polynomial \((p_0, p_1, p_2, \ldots) \) as a sum \( p_0 + p_1 X + p_2 X^2 + \cdots \) while remaining honest; the sum \( p_0 + p_1 X + p_2 X^2 + \cdots \) is no longer
a “formal expression” of unclear meaning, nor a function, but it is just an alternative way to write the sequence \((p_0, p_1, p_2, \ldots)\). So, at last, our notion of a polynomial resembles the intuitive notion of a polynomial!

Of course, we can write polynomials as finite sums as well. Indeed, if \((p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X]\) is a polynomial and \(N\) is a nonnegative integer such that every \(n > N\) satisfies \(p_n = 0\), then

\[
(p_0, p_1, p_2, \ldots) = p_0 + p_1X + p_2X^2 + \cdots = p_0 + p_1X + \cdots + p_NX^N
\]

(because addends can be discarded when they are 0). For example,

\[
(4, 1, 0, 0, 0, \ldots) = 4 + 1X = 4 + X \text{ and } \left(\frac{1}{2}, 0, \frac{1}{3}, 0, 0, 0, \ldots\right) = \frac{1}{2} + 0X + \frac{1}{3}X^2 = \frac{1}{2} + \frac{1}{3}X^2.
\]

\textbf{(k)} For our definition of polynomials to be fully compatible with our intuition, we are missing only one more thing: a way to evaluate a polynomial at a number, or some other object (e.g., another polynomial or a function). This is easy: Let \(p = (p_0, p_1, p_2, \ldots) \in \mathbb{Q}[X]\) be a polynomial, and let \(\alpha \in \mathbb{Q}\). Then, \(p(\alpha)\) means the number \(p_0 + p_1\alpha + p_2\alpha^2 + \cdots \in \mathbb{Q}\). (Again, the infinite sum \(p_0 + p_1\alpha + p_2\alpha^2 + \cdots\) makes sense because of (33).) Similarly, we can define \(p(\alpha)\) when \(\alpha \in \mathbb{R}\) (but in this case, \(p(\alpha)\) will be an element of \(\mathbb{R}\)) or when \(\alpha \in \mathbb{C}\) (in this case, \(p(\alpha) \in \mathbb{C}\)) or when \(\alpha\) is a square matrix with rational entries (in this case, \(p(\alpha)\) will also be such a matrix) or when \(\alpha\) is another polynomial (in this case, \(p(\alpha)\) is such a polynomial as well).

For example, if \(p = (1, -2, 0, 3, 0, 0, 0, \ldots) = 1 - 2X + 3X^3\), then \(p(\alpha) = 1 - 2\alpha + 3\alpha^3\) for every \(\alpha\).

The map \(\mathbb{Q} \to \mathbb{Q}, \alpha \mapsto p(\alpha)\) is called the polynomial function described by \(p\). As we said above, this function is not \(p\), and it is not a good idea to equate it with \(p\).

If \(\alpha\) is a number (or a square matrix, or another polynomial), then \(p(\alpha)\) is called the result of evaluating \(p\) at \(X = \alpha\) (or, simply, evaluating \(p\) at \(\alpha\)), or the result of substituting \(\alpha\) for \(X\) in \(p\). This notation, of course, reminds of functions; nevertheless, (as we already said a few times) \(p\) is not a function.

Probably the simplest three cases of evaluation are the following ones:

- We have \(p(0) = p_0 + p_10^1 + p_20^2 + \cdots = p_0\). In other words, evaluating \(p\) at \(X = 0\) yields the constant term of \(p\).

- We have \(p(1) = p_0 + p_11^1 + p_21^2 + \cdots = p_0 + p_1 + p_2 + \cdots\). In other words, evaluating \(p\) at \(X = 1\) yields the sum of all coefficients of \(p\).

- We have \(p(X) = p_0 + p_1X^1 + p_2X^2 + \cdots = p_0 + p_1X + p_2X^2 + \cdots = p\). In other words, evaluating \(p\) at \(X = X\) yields \(p\) itself. This allows us to write \(p(X)\) for \(p\). Many authors do so, just in order to stress that \(p\) is a polynomial and that the indeterminate is called \(X\). It should be kept in
mind that $X$ is not a variable (just as $p$ is not a function); it is the (fixed!) sequence $(0,1,0,0,0,\ldots) \in \mathbb{Q}[X]$ which serves as the indeterminate for polynomials in $\mathbb{Q}[X]$.

(l) Often, one wants (or is required) to give an indeterminate a name other than $X$. (For instance, instead of polynomials with rational coefficients, we could be considering polynomials whose coefficients themselves are polynomials in $\mathbb{Q}[X]$; and then, we would not be allowed to use the letter $X$ for the “new” indeterminate anymore, as it already means the indeterminate of $\mathbb{Q}[X]$ !) This can be done, and the rules are the following: Any letter (that does not already have a meaning) can be used to denote the indeterminate; but then, the set of all polynomials has to be renamed as $\mathbb{Q}[^\eta]$, where $^\eta$ is this letter. For instance, if we want to denote the indeterminate as $x$, then we have to denote the set by $\mathbb{Q}[x]$.

It is furthermore convenient to regard the sets $\mathbb{Q}[^\eta]$ for different letters $^\eta$ as distinct. Thus, for example, the polynomial $3X^2 + 1$ is not the same as the polynomial $3Y^2 + 1$. (The reason for doing so is that one sometimes wishes to view both of these polynomials as polynomials in the two variables $X$ and $Y$.) Formally speaking, this means that we should define a polynomial in $\mathbb{Q}[^\eta]$ to be not just a sequence $(p_0, p_1, p_2, \ldots)$ of rational numbers, but actually a pair $((p_0, p_1, p_2, \ldots), "^\eta")$ of a sequence of rational numbers and the letter $^\eta$. (Here, "$^\eta$" really means the letter $^\eta$, not the sequence $(0,1,0,0,0,\ldots)$.) This is, of course, a very technical point which is of little relevance to most of mathematics; it becomes important when one tries to implement polynomials in a programming language.

(m) As already explained, we can replace $\mathbb{Q}$ by $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ or any other commutative ring $\mathbb{K}$ in the above definition. (See Definition 6.2 for the definition of a commutative ring.) When $\mathbb{Q}$ is replaced by a commutative ring $\mathbb{K}$, the notion of “univariate polynomials with rational coefficients” becomes “univariate polynomials with coefficients in $\mathbb{K}$” (also known as “univariate polynomials over $\mathbb{K}$”), and the set of such polynomials is denoted by $\mathbb{K}[X]$ rather than $\mathbb{Q}[X]$.

So much for univariate polynomials.

Polynomials in multiple variables are (in my opinion) treated the best in [Lang02, Chapter II, §3], where they are introduced as elements of a monoid ring. However, this treatment is rather abstract and uses a good deal of algebraic language.[18] The treatments in [Walker87, §4.5], in [Rotman15 Chapter A-3] and in [BirMac99 Chapter IV, §4] use the above-mentioned recursive shortcut that makes them inferior (in my opinion). A neat (and rather elementary) treatment of polynomials in $n$ variables (for finite $n$) can be found in [Hünger03 Chapter III, §5] and in [AmaEsc05 §8]; it generalizes the viewpoint we used in Definition 1.1 for univariate polynomials above.[19]

[18] Also, the book [Lang02] is notorious for its unpolished writing; it is best read with Bergman’s companion [Bergma15] at hand.

[19] You are reading right: The analysis textbook [AmaEsc05] is one of the few sources I am aware of
2. On acyclic quivers and mutations

**Remark 2.1.** Chapter 2 is rough and will probably be rewritten at some point (as well as moved to a more appropriate place somewhere near the end of the notes). Since the rest of these notes does not depend on this chapter, I recommend to skip it when reading the notes.

In this chapter, we will use the following notations (which come from [Lampe, §2.1.1]):

- A quiver means a tuple $Q = (Q_0, Q_1, s, t)$, where $Q_0$ and $Q_1$ are two finite sets and where $s$ and $t$ are two maps from $Q_1$ to $Q_0$. We call the elements of $Q_0$ the vertices of the quiver $Q$, and we call the elements of $Q_1$ the arrows of the quiver $Q$. For every $e \in Q_1$, we call $s(e)$ the starting point of $e$ (and we say that $e$ starts at $s(e)$), and we call $t(e)$ the terminal point of $e$ (and we say that $e$ ends at $t(e)$). Furthermore, if $e \in Q_1$, then we say that $e$ is an arrow from $s(e)$ to $t(e)$.

So the notion of a quiver is one of many different versions of the notion of a finite directed graph. (Notice that it is a version which allows multiple arrows, and which distinguishes between them – i.e., the quiver stores not just the information of how many arrows there are from a vertex to another, but it actually has them all as distinguishable objects in $Q_1$. Lampe himself seems to later tacitly switch to a different notion of quivers, where edges from a given to vertex to another are indistinguishable and only exist as a number. This does not matter for the next exercise, which works just as well with either notion of a quiver; but I just wanted to have it mentioned.)

- The underlying undirected graph of a quiver $Q = (Q_0, Q_1, s, t)$ is defined as the undirected multigraph with vertex set $Q_0$ and edge multiset

$$\bigl\{\{s(e), t(e)\} \mid e \in Q_1\bigr\}_{\text{multiset}}.$$  

(“Multigraph” means that multiple edges are allowed, but we do not make them distinguishable.)

- A quiver $Q = (Q_0, Q_1, s, t)$ is said to be acyclic if there is no sequence $(a_0, a_1, \ldots, a_n)$ of elements of $Q_0$ such that $n > 0$ and $a_0 = a_n$ and such that $Q$ has an arrow from $a_i$ to $a_{i+1}$ for every $i \in \{0, 1, \ldots, n - 1\}$. (This is equivalent to [Lampe, Definition 2.1.7].) Notice that this does not mean that the undirected version of $Q$ has no cycles.

- Let $Q = (Q_0, Q_1, s, t)$. Then, a sink of $Q$ means a vertex $v \in Q_0$ such that no $e \in Q_1$ starts at $v$ (in other words, no arrow of $Q$ starts at $v$). A source of $Q$ means a vertex $v \in Q_0$ such that no $e \in Q_1$ ends at $v$ (in other words, no arrow of $Q$ ends at $v$).

---

to define the (algebraic!) notion of polynomials precisely and well.
Let \( Q = (Q_0, Q_1, s,t) \). If \( i \in Q_0 \) is a sink of \( Q \), then the mutation \( \mu_i (Q) \) of \( Q \) at \( i \) is the quiver obtained from \( Q \) simply by turning all arrows ending at \( i \). (To be really pedantic: We define \( \mu_i (Q) \) as the quiver \((Q_0, Q_1, s', t')\), where

\[
\begin{align*}
s'(e) &= \begin{cases} t(e), & \text{if } t(e) = i; \\ s(e), & \text{if } t(e) \neq i \end{cases} \quad \text{for each } e \in Q_1, \\
t'(e) &= \begin{cases} s(e), & \text{if } t(e) = i; \\ t(e), & \text{if } t(e) \neq i \end{cases} \quad \text{for each } e \in Q_1.
\end{align*}
\]

If \( i \in Q_0 \) is a source of \( Q \), then the mutation \( \mu_i (Q) \) of \( Q \) at \( i \) is the quiver obtained from \( Q \) by turning all arrows starting at \( i \). (Notice that if \( i \) is both a source and a sink of \( Q \), then these two definitions give the same result; namely, \( \mu_i (Q) = Q \) in this case.)

If \( Q \) is an acyclic quiver, then \( \mu_i (Q) \) is acyclic as well (whenever \( i \in Q_0 \) is a sink or a source of \( Q \)).

We use the word “mutation” not only for the quiver \( \mu_i (Q) \), but also for the operation that transforms \( Q \) into \( \mu_i (Q) \). (We have defined this operation only if \( i \) is a sink or a source of \( Q \). It can be viewed as a particular case of the more general definition of mutation given in [Lampe, Definition 2.2.1], at least if one gives up the ability to distinguish different arrows from one vertex to another.)

**Exercise 1.** Let \( Q = (Q_0, Q_1, s,t) \) be an acyclic quiver.

(a) Let \( A \) and \( B \) be two subsets of \( Q_0 \) such that \( A \cap B = \emptyset \) and \( A \cup B = Q_0 \). Assume that there exists no arrow of \( Q \) that starts at a vertex in \( B \) and ends at a vertex in \( A \). Then, by turning all arrows of \( Q \) which start at a vertex in \( A \) and end at a vertex in \( B \), we obtain a new acyclic quiver \( \text{mut}_{A,B} Q \).

(When we say “turning all arrows of \( Q \) which start at a vertex in \( A \) and end at a vertex in \( B' \)”, we mean “turning all arrows \( e \) of \( Q \) which satisfy \( s(e) \in A \) and \( t(e) \in B' \). We do not mean that we fix a vertex \( a \) in \( A \) and a vertex \( b \) in \( B \), and only turn the arrows from \( a \) to \( b \).)

For example, if \( Q = \begin{array}{c} 3 \\ 1 \end{array} \rightarrow \begin{array}{c} 4 \\ \ \end{array} \) and \( A = \{1,3\} \) and \( B = \{2,4\} \), then

\[
\text{mut}_{A,B} Q = \begin{array}{c} 3 \\ 1 \end{array} \rightarrow \begin{array}{c} 4 \\ 2 \end{array}.
\]

Prove that \( \text{mut}_{A,B} Q \) can be obtained from \( Q \) by a sequence of mutations at sinks. (More precisely, there exists a sequence \( (Q^{(0)}, Q^{(1)}, \ldots, Q^{(\ell)}) \) of acyclic

---

\( ^{20} \)To *turn* an arrow \( e \) means to reverse its direction, i.e., to switch the values of \( s(e) \) and \( t(e) \). We model this as a change to the functions \( s \) and \( t \), not as a change to the arrow itself.
quivers such that \( Q^{(0)} = Q \), \( Q^{(\ell)} = \text{mut}_{A,B} Q \), and for every \( i \in \{1,2,\ldots,\ell\} \), the quiver \( Q^{(i)} \) is obtained from \( Q^{(i-1)} \) by mutation at a sink of \( Q^{(i-1)} \).

[In our above example, we can mutate at 4 first and then at 2.]

(b) If \( i \in Q_0 \) is a source of \( Q \), then show that the mutation \( \mu_i(Q) \) can be obtained from \( Q \) by a sequence of mutations at sinks.

(c) Assume now that the underlying undirected graph of \( Q \) is a tree. (In particular, \( Q \) cannot have more than one edge between two vertices, as these would form a cycle in the underlying undirected graph!) Show that any acyclic quiver which can be obtained from \( Q \) by turning some of its arrows can also be obtained from \( Q \) by a sequence of mutations at sinks.

Remark 2.2. More general results than those of Exercise 1 are stated (for directed graphs rather than quivers, but it is easy to translate from one language into another) in [Pretzel].

3. On binomial coefficients

Let me now switch to a different subject. The present chapter is about binomial coefficients and some of their properties. This subject has little to do with cluster algebras, but it proves two lemmas in the long Lee–Schiffler paper [LeeSch2] (specifically, our Exercise 3 is [LeeSch2, Lemma 5.11], and our Proposition 3.7 is [LeeSch2, Lemma 5.12]); besides, it is highly useful in many fields of mathematics and provides good opportunities to practice the arts of mathematical induction and of finding bijections.

Identities involving binomial coefficients are legion, and books have been written about them (let me mention [GrKnPa, Chapter 5] as a highly readable introduction; but, e.g., Henry W. Gould’s website goes far further down the rabbit hole). We shall only study a few of these identities.

3.1. Definitions and basic properties

Recall that for every \( n \in \mathbb{N} \), the binomial coefficient \( \binom{X}{n} \) is a polynomial in \( X \) of degree \( n \), with rational coefficients. It is defined by

\[
\binom{X}{n} = \frac{X (X-1) \cdots (X-n+1)}{n!}.
\]

This polynomial can be evaluated at every integer or rational number or even complex number (i.e., we can substitute any such number for \( X \), or at any other

\[\text{When } n = 0, \text{ then the numerator of this fraction (i.e., the product } X (X-1) \cdots (X-n+1) \text{) is an empty product. By convention, an empty product is always defined to be 1.}\]
polynomial (for example, we can substitute $X^2 + 2$ for $X$ to obtain $\binom{X^2 + 2}{n}$, which is again a polynomial). Whenever $m$ is an integer (or rational number, or complex number), we denote by $\binom{m}{n}$ the result of evaluating the polynomial $\binom{X}{n}$ at $X = m$. These numbers $\binom{m}{n}$ are the so-called binomial coefficients, and form the so-called Pascal’s triangle. Let us state a few basic properties of these numbers:

- We have
  \[
  \binom{m}{n} = \frac{m (m-1) \cdots (m-n+1)}{n!}
  \]
  for every $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. (This follows by evaluating both sides of the identity $\binom{X}{n} = \frac{X (X-1) \cdots (X-n+1)}{n!}$ at $X = m$.)

The equality (34) is how the binomial coefficients $\binom{m}{n}$ are usually defined in textbooks. Thus, our detour through polynomials was not necessary. (But this detour will reveal to be useful soon, when we will prove some properties of binomial coefficients.)

- We have
  \[
  \binom{X}{0} = 1
  \]
  \[23\] Thus,
  \[
  \binom{m}{0} = 1
  \]
  for every $m \in \mathbb{Z}$. (This follows by substituting 0 for $m$ in (35).)

- We have
  \[
  \binom{m}{n} = \frac{m!}{n! (m-n)!}
  \]

\[22\]More precisely, the numbers $\binom{m}{n}$ for $m \in \mathbb{N}$ and $n \in \{0, 1, \ldots, m\}$ form Pascal’s triangle. Nevertheless, the “other” binomial coefficients (particularly the ones where $m$ is a negative integer) are highly useful.

\[23\]Proof. The definition of $\binom{X}{0}$ yields $\binom{X}{0} = \frac{X (X-1) \cdots (X-0+1)}{0!}$. Since $X (X-1) \cdots (X-0+1) = (a \text{ product of } 0 \text{ integers}) = 1$, this rewrites as $\binom{X}{0} = \frac{1}{0!} = 1$ (since $0! = 1$), qed.
for any \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m \geq n \).

\[ \binom{m}{n} = 0 \quad (38) \]

for every \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m < n \).  

\[ \binom{-3}{2} \text{ nor } \binom{1/3}{3} \text{ nor } \binom{2}{5} \text{ nor the polynomial } \binom{X}{3} \text{ can be evaluated using this formula! The \footnote{Caution: This formula holds only for } m \in \mathbb{N} \text{ and } n \in \mathbb{N} \text{ satisfying } m \geq n. \text{ Thus, neither } \binom{-3}{2} \text{ nor } \binom{1/3}{3} \text{ nor } \binom{2}{5} \text{ nor the polynomial } \binom{X}{3} \text{ can be evaluated using this formula! The definition } \binom{X}{n} = \frac{X(X-1) \cdots (X-n+1)}{n!} \text{ of binomial coefficients is a lot more general than (37).} \]

For the sake of completeness, let us give a proof of (37): Let \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) be such that \( m \geq n \). Then, evaluating both sides of the identity \( \binom{X}{n} = \frac{X(X-1) \cdots (X-n+1)}{n!} \) at \( X = m \), we obtain

\[ \binom{m}{n} = \frac{m(m-1) \cdots (m-n+1)}{n!}, \]

so that \( n! \cdot \binom{m}{n} = m(m-1) \cdots (m-n+1) \). But

\[
\begin{align*}
  m! &= m(m-1) \cdots 1 = (m(m-1) \cdots (m-n+1)) \cdot ((m-n)(m-n-1) \cdots 1) \\
  &= (m(m-1) \cdots (m-n+1)) \cdot (m-n)!
\end{align*}
\]

so that \( \frac{m!}{(m-n)!} = m(m-1) \cdots (m-n+1) \). Comparing this with \( n! \cdot \binom{m}{n} = m(m-1) \cdots (m-n+1) \), we obtain \( n! \cdot \binom{m}{n} = \frac{m!}{(m-n)!} \). Dividing this equality by \( n! \), we obtain \( \binom{m}{n} = \frac{m!}{n!(m-n)!} \). Thus, (37) is proven.

\[ \binom{-3}{2} \text{ nor } \binom{1/3}{3} \text{ nor } \binom{2}{5} \text{ nor the polynomial } \binom{X}{3} \text{ can be evaluated using this formula! The \footnote{Caution: This is not true if we drop the condition } m \in \mathbb{N}. \]

For the sake of completeness, let us give a proof of (38): Let \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) be such that \( m < n \). Evaluating both sides of the identity \( \binom{X}{n} = \frac{X(X-1) \cdots (X-n+1)}{n!} \) at \( X = m \), we obtain

\[ \binom{m}{n} = \frac{m(m-1) \cdots (m-n+1)}{n!}. \]

But \( m \geq 0 \) (since \( m \in \mathbb{N} \)) and \( m < n \). Hence, \( m-m \) is one of the \( n \) integers \( m, m-1, \ldots, m-n+1 \). Thus, one of the \( n \) factors of the product \( m(m-1) \cdots (m-n+1) \) is \( m-m = 0 \). Therefore, the whole product \( m(m-1) \cdots (m-n+1) \) is 0 (because if one of the factors of a product is 0, then the whole product must be 0). Thus, \( m(m-1) \cdots (m-n+1) = 0 \). Hence,

\[
\binom{m}{n} = \frac{m(m-1) \cdots (m-n+1)}{n!} = \frac{0}{n!} = 0
\]

(since \( m(m-1) \cdots (m-n+1) = 0 \))

qed.
• We have
\[
\binom{m}{n} = \binom{m}{m-n}
\]
for any \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m \geq n \) \(^{26}\).

• We have
\[
\binom{m}{m} = 1
\]
for every \( m \in \mathbb{N} \)^{27}.

• If \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \), and if \( S \) is an \( m \)-element set, then
\[
\binom{m}{n}
\]
is the number of all \( n \)-element subsets of \( S \). \(^{41}\)

In less formal terms, this says that \( \binom{m}{n} \) is the number of ways to pick out \( n \) among \( m \) given objects, without replacement\(^{28}\) and without regard for the order in which they are picked out. (Probabilists call this “unordered samples without replacement”.)

Notice that this does not hold for negative \( m! \) ! Indeed, when \( m \in \mathbb{Z} \) is negative, then \( \binom{m}{n} \) is positive for \( n \) even and negative for \( n \) odd (easy exercise), and so an interpretation of \( \binom{m}{n} \) as a number of ways to do something is rather unlikely. (On the other hand, \((-1)^n \binom{m}{n}\) does have such an interpretation.)

• We have
\[
\binom{m}{n} = (-1)^n \binom{n-m-1}{n}
\]
for any \( m \in \mathbb{Z} \) and \( n \in \mathbb{N} \)^{29}. This formula is known as the upper negation formula and holds more generally for any \( m \) for which it makes sense (in

\(^{26}\)Proof of (39): Let \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) be such that \( m \geq n \). Then, \( m - n \in \mathbb{N} \) (since \( m \geq n \) and \( m \geq m - n \) (since \( n \geq 0 \) (since \( n \in \mathbb{N} \)). Hence, (37) (applied to \( m - n \) instead of \( n \)) yields
\[
\binom{m-n}{m-n} = \frac{m!}{(m-n)! (m-(m-n))!} = \frac{m!}{(m-(m-n))! (m-n)!} = \frac{m!}{n! (m-n)!}
\]
(since \( m - (m - n) = n \)). Compared with (37), this yields \( \binom{m}{n} = \binom{m}{m-n} \), qed.

\(^{27}\)Proof of (40): Let \( m \in \mathbb{N} \). Then, (39) (applied to \( n = m \)) yields
\[
\binom{m}{m} = \binom{m}{m-m} = \binom{m}{0} = 1
\]
(according to (36)). This proves (40).

\(^{28}\)That is, one must not pick out the same object twice.

\(^{29}\)Proof of (42): Let \( m \in \mathbb{Z} \) and \( n \in \mathbb{N} \).
particular, \( m \) can be a polynomial or a complex number. In particular, we have
\[
\binom{X}{n} = (-1)^n \binom{n - X - 1}{n}
\]  
(43)

(an identity between polynomials in \( X \)) for every \( n \in \mathbb{N} \).

• We have
\[
\binom{X}{n} = \binom{X - 1}{n} + \binom{X - 1}{n - 1}
\]  
(44)

Evaluating both sides of the identity \( \binom{X}{n} = \frac{X(X - 1) \cdots (X - n + 1)}{n!} \) at \( X = n - m - 1 \), we obtain
\[
\binom{n - m - 1}{n} = \frac{(n - m - 1) ((n - m - 1) - 1) \cdots ((n - m - 1) - n + 1)}{n!}
\]
\[
= \frac{1}{n!} (n - m - 1) ((n - m - 1) - 1) \cdots ((n - m - 1) - n + 1)
\]
\[
= \frac{1}{n!} \frac{(-m)(-m+1) \cdots (-m-n+1)}{(-1)^{n-m-n+1}}
\]
\[
= \frac{1}{n!} ((-1)^m ((-1)(m-1)) \cdots ((-1)(m-n+1))
\]
\[
= \frac{1}{n!} (-1)^n (m - 1) \cdots (m - n + 1),
\]
so that
\[
(-1)^n \binom{n - m - 1}{n} = (-1)^n \frac{1}{n!} (-1)^n (m - 1) \cdots (m - n + 1)
\]
\[
= \frac{1}{n!} (-1)^n (m - 1) \cdots (m - n + 1)
\]
\[
= \frac{1}{n!} m (m - 1) \cdots (m - n + 1)
\]
\[
\text{since } 2n \text{ is even}
\]
\[
= \frac{m (m - 1) \cdots (m - n + 1)}{n!}.
\]

Compared with \( \binom{m}{n} = \frac{m (m - 1) \cdots (m - n + 1)}{n!} \) (which is obtained by evaluating both sides of the identity \( \binom{X}{n} = \frac{X(X - 1) \cdots (X - n + 1)}{n!} \) at \( X = m \)), this yields \( \binom{m}{n} = (-1)^n \binom{n - m - 1}{n} \), qed.

\text{Proof of (43): To prove (43), just replace every appearance of “m” by “X” in our proof of (42).}
for any \( n \in \{1, 2, 3, \ldots\} \)\(^{31}\) Thus,

\[
\binom{m}{n} = \binom{m - 1}{n - 1} + \binom{m - 1}{n}
\]

(46)

\(^{31}\)Proof of (44): Let \( n \in \{1, 2, 3, \ldots\} \). We have \( n! = n \cdot (n - 1)! \), so that \( (n - 1)! = \frac{n!}{n} \) and thus

\[
\frac{1}{(n - 1)!} = \frac{1}{n!} \cdot \frac{1}{n}
\]

The definition of \( \binom{X}{n - 1} \) yields

\[
\binom{X}{n - 1} = \frac{X(X - 1) \cdots (X - (n - 1) + 1)}{(n - 1)!} = \frac{1}{(n - 1)!} (X(X - 1) \cdots (X - (n - 1) + 1)).
\]

Substituting \( X - 1 \) for \( X \) in this equality, we obtain

\[
\binom{X - 1}{n - 1} = \frac{1}{(n - 1)!} \binom{X - 1}{X - 2} \cdots \binom{X - (n - 1) + 1}{X - n + 1} = \frac{1}{n!} \cdot n ((X - 1) (X - 2) \cdots (X - n + 1)).
\]

(45)

On the other hand,

\[
\binom{X}{n} = \frac{X(X - 1) \cdots (X - n + 1)}{n!} = \frac{1}{n!} (X(X - 1) \cdots (X - n + 1)).
\]

Substituting \( X - 1 \) for \( X \) in this equality, we find

\[
\binom{X - 1}{n} = \frac{1}{n!} \binom{X - 1}{X - 2} \cdots \binom{X - (n - 1) + 1}{X - n + 1} = \frac{1}{n!} ((X - 1) (X - 2) \cdots (X - n + 1)) \cdot (X - n)
\]

\[
= \frac{1}{n!} (X - n) \cdot ((X - 1) (X - 2) \cdots (X - n + 1)).
\]

Adding (45) to this equality, we obtain

\[
\binom{X - 1}{n} + \binom{X - 1}{n - 1} = \frac{1}{n!} (X - n) \cdot ((X - 1) (X - 2) \cdots (X - n + 1)) + \frac{1}{n!} \cdot n ((X - 1) (X - 2) \cdots (X - n + 1))
\]

\[
= \frac{1}{n!} ([X - n] + n) \cdot ((X - 1) (X - 2) \cdots (X - n + 1)) = \frac{1}{n!} X \cdot ((X - 1) (X - 2) \cdots (X - n + 1)) = \frac{1}{n!} (X(X - 1) \cdots (X - n + 1)) = \binom{X}{n},
\]

qed.
for any $m \in \mathbb{Z}$ and $n \in \{1, 2, 3, \ldots\}$. (This is the result of substituting $m$ for $X$ in (44).) The formula (46) is known as the recurrence relation of the binomial coefficients.

- We have
  \[
  \binom{m}{n} \in \mathbb{Z}
  \] (47)
  for any $m \in \mathbb{Z}$ and $n \in \mathbb{N}$.

- We have
  \[
  (X + Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^k Y^{n-k}
  \] (48)

Often it is extended to the case $n = 0$ by setting $\left(\begin{array}{c}X \\ -1\end{array}\right) = 0$. It then follows from (36) in this case.

The formula (46) is responsible for the fact that “every number in Pascal’s triangle is the sum of the two numbers above it”. (Of course, if you use this fact as a definition of Pascal’s triangle, then (46) is conversely responsible for the fact that the numbers in this triangle are the binomial coefficients.)

Proof of (47): Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. We need to show that $\binom{m}{n} \in \mathbb{Z}$. We are in one of the following two cases:

Case 1: We have $m \geq 0$.

Case 2: We have $m < 0$.

Let us first consider Case 1. In this case, we have $m \geq 0$. Hence, $m \in \mathbb{N}$. Thus, there exists an $m$-element set $S$ (for example, $S = \{1, 2, \ldots, m\}$). Consider such $S$. Then, $\binom{m}{n}$ is the number of all $n$-element subsets of $S$ (because of (41)). Hence, $\binom{m}{n}$ is a nonnegative integer, so that $\binom{m}{n} \in \mathbb{N} \subseteq \mathbb{Z}$. This proves (47) in Case 1.

Let us now consider Case 2. In this case, we have $m < 0$. Thus, $m + 1 \leq 0$, so that $n - (m + 1) \geq 0$. Hence, $n - m - 1 \in \mathbb{N}$. Therefore, there exists an $(n - m - 1)$-element set $S$ (for example, $S = \{1, 2, \ldots, n - m - 1\}$). Consider such $S$. Then, $\binom{n - m - 1}{n}$ is the number of all $n$-element subsets of $S$ (because of (41), applied to $n - m - 1$ instead of $m$). Hence, $\binom{n - m - 1}{n} \in \mathbb{N} \subseteq \mathbb{Z}$. Now, (42) shows that $\binom{m}{n} = (-1)^n \binom{n - m - 1}{n} \in (-1)^n \mathbb{Z} \subseteq \mathbb{Z}$ (where $(-1)^n \mathbb{Z}$ means $\{(-1)^n z \mid z \in \mathbb{Z}\}$). This proves (47) in Case 2.

We thus have proven (47) in each of the two Cases 1 and 2, and can therefore conclude that (47) always holds.

This is the simplest proof of (47) that I am aware of. There is another which proceeds by induction on $m$ (using (44)), but this induction needs two induction steps ($m \to m + 1$ and $m \to m - 1$) in order to reach all integers (positive and negative). There is yet another proof using basic number theory (specifically, checking how often a prime $p$ appears in the numerator and the denominator of $\binom{m}{n} = \frac{m(m-1) \cdots (m-n+1)}{n!}$), but this is not quite easy.
(as an equality between two polynomials in \(X\) and \(Y\)) for every \(n \in \mathbb{N}\). This is the famous binomial formula and has a well-known standard proof by induction over \(n\) (using (46) and (36)). Some versions of it hold for negative \(n\) as well (but not in the exact form (48), and not without restrictions).

• We have

\[
\binom{X}{n} = \frac{X}{n} \binom{X-1}{n-1}
\]

for any \(n \in \{1, 2, 3, \ldots\}\). \(\square\)

• If \(a \in \mathbb{N}\) and \(i \in \mathbb{N}\) are such that \(i \geq a\), then

\[
\binom{X}{i} \binom{i}{a} = \binom{X}{a} \binom{X-a}{i-a}
\]

(50)

34

Proof of (49): Let \(n \in \{1, 2, 3, \ldots\}\). The definition of \(\binom{X}{n-1}\) yields

\[
\frac{X (X-1) \cdots (X-(n-1)+1)}{(n-1)!} = \binom{X-1}{n-1}.
\]

Substituting \(X-1\) for \(X\) in this equality, we obtain

\[
\binom{X-1}{n-1} = \frac{(X-1) ((X-1) - 1) \cdots ((X-1) - (n-1) + 1)}{(n-1)!} = \frac{(X-1) (X-2) \cdots (X-n+1)}{(n-1)!}
\]

(since \((X-1) - 1 = X - 2\) and \((X-1) - (n-1) + 1 = X - n + 1\)). Multiplying both sides of this equality by \(\frac{X}{n}\), we obtain

\[
\frac{X}{n} \binom{X-1}{n-1} = \frac{X (X-1) (X-2) \cdots (X-n+1)}{(n-1)!} = \frac{X (X-1) (X-2) \cdots (X-n+1)}{n (n-1)!}
\]

\[
= \frac{X (X-1) \cdots (X-n+1)}{n!}
\]

(since \(X (X-1) (X-2) \cdots (X-n+1) = X (X-1) \cdots (X-n+1)\) and \(n (n-1)! = n!\)). Compared with

\[
\binom{X}{n} = \frac{X (X-1) \cdots (X-n+1)}{n!},
\]

this yields \(\binom{X}{n} = \frac{X}{n} \binom{X-1}{n-1}\). This proves (49).
In particular, if \( m \in \mathbb{Z}, a \in \mathbb{N} \) and \( i \in \mathbb{N} \) are such that \( i \geq a \), then

\[
\binom{m}{i} \binom{i}{a} = \binom{m}{a} \binom{m-a}{i-a}
\]  

(51)

This is a simple and yet highly useful formula, which Graham, Knuth and Patashnik call trinomial revision in [GrKnPa, Table 174].

3.2. Binomial coefficients and polynomials

Recall that any polynomial \( P \in \mathbb{Q}[X] \) (that is, any polynomial in the indeterminate \( X \) with rational coefficients) can be quasi-uniquely written in the form \( P(X) = \sum_{n=0}^{N} a_n X^n \).

Proof of (50): Let \( a \in \mathbb{N} \) and \( i \in \mathbb{N} \) be such that \( i \geq a \). We have

\[
\frac{X}{a!} (X-1) \cdots (X-a+1) = \frac{X-a}{(i-a)!} (X-a-1) \cdots (X-a-(i-a)+1)
\]

(by the definition of \( \binom{X}{a} \))

\[
\frac{X}{a!} (X-1) \cdots (X-a+1) = \frac{X-a}{(i-a)!} (X-a-1) \cdots (X-a-(i-a)+1)
\]

(by the definition of \( \binom{X-a}{i-a} \)).

\[
\frac{1}{a! \cdot (i-a)!} (X-1) \cdots (X-a+1) \cdot ((X-a) \cdots (X-a-(i-a)+1))
\]

= \( X(X-1) \cdots (X-a) \cdots (X-a-(i-a)+1) \)

= \( X(X-1) \cdots (X-a)+1 \)

(since \( X-a-(i-a)=X-a \))

\[
= \frac{1}{a! \cdot (i-a)!} X(X-1) \cdots (X-i+1).
\]

Compared with

\[
\frac{X}{i!} (X-1) \cdots (X-i+1) = \frac{i}{a!} (X-1) \cdots (X-i+1)
\]

(by the definition of \( \binom{X}{i} \))

\[
\frac{X}{i!} (X-1) \cdots (X-i+1) = \frac{i}{a! \cdot (i-a)!} \cdot \frac{i!}{a! \cdot (i-a)!}
\]

= \( 1 \)

(50).

This proves (50).

Notice that we used \( \text{by } (37), \text{ applied to } m=i \) and \( u=a \) to simplify \( \binom{i}{a} \) in this proof. Do not be tempted to use \( \text{by } (37), \text{ applied to } m=i \) and \( u=a \) to simplify \( \binom{X}{i}, \binom{X-a}{i} \) and \( \binom{X-a}{i-a} \): The \( X \) in these expressions is a polynomial indeterminate, and \( \text{by } (37), \text{ applied to } m=i \) and \( u=a \) cannot be applied to it!

This formula is obtained from (50) by substituting \( m \) for \( X \).
\[ \sum_{i=0}^{d} c_i X^i \] with rational \( c_0, c_1, \ldots, c_d \). The word “quasi-uniquely” here means that the coefficients \( c_0, c_1, \ldots, c_d \) are uniquely determined when \( d \in \mathbb{N} \) is specified; they are not literally unique because we can always increase \( d \) by adding new 0 coefficients (for example, the polynomial \((1 + X)^2\) can be written both as \(1 + 2X + X^2\) and as \(1 + 2X + X^2 + 0X^3 + 0X^4\)).

It is not hard to check that an analogue of this statement holds with the \( X^i \) replaced by the \( \binom{X}{i} \):

**Proposition 3.1.** (a) Any polynomial \( P \in \mathbb{Q}[X] \) can be quasi-uniquely written in the form \( P(X) = \sum_{i=0}^{d} c_i \binom{X}{i} \) with rational \( c_0, c_1, \ldots, c_d \). (Again, “quasi-uniquely” means that we can always increase \( d \) by adding new 0 coefficients, but apart from this the \( c_0, c_1, \ldots, c_d \) are uniquely determined.)

(b) The polynomial \( P \) is integer-valued (i.e., its values at integers are integers) if and only if these rationals \( c_0, c_1, \ldots, c_d \) are integers.

(We will not use this fact below, but it gives context to Theorem 3.3 and Exercise 2 further below. The “if” part of Proposition 3.1 (b) follows from (47).)

We shall now prove some facts and give some exercises about binomial coefficients; but let us first prove a fundamental property of polynomials:

**Lemma 3.2.** (a) Let \( P \) be a polynomial in the indeterminate \( X \) with rational coefficients. Assume that \( P(x) = 0 \) for all \( x \in \mathbb{N} \). Then, \( P = 0 \) as polynomials.

(b) Let \( P \) and \( Q \) be two polynomials in the indeterminate \( X \) with rational coefficients. Assume that \( P(x) = Q(x) \) for all \( x \in \mathbb{N} \). Then, \( P = Q \) as polynomials.

(c) Let \( P \) be a polynomial in the indeterminates \( X \) and \( Y \) with rational coefficients. Assume that \( P(x,y) = 0 \) for all \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \). Then, \( P = 0 \) as polynomials.

(d) Let \( P \) and \( Q \) be two polynomials in the indeterminates \( X \) and \( Y \) with rational coefficients. Assume that \( P(x,y) = Q(x,y) \) for all \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \). Then, \( P = Q \) as polynomials.

Probably you have seen this lemma proven at least once in your life, but let me still prove it for the sake of completeness.

*Proof of Lemma 3.2* (a) The polynomial \( P \) satisfies \( P(x) = 0 \) for every \( x \in \mathbb{N} \). Hence, every \( x \in \mathbb{N} \) is a root of \( P \). Thus, the polynomial \( P \) has infinitely many roots. But a nonzero polynomial in one variable (with rational coefficients) can only have finitely many roots.\(^{38}\) If \( P \) was nonzero, this would force a contradiction.

---

\(^{38}\)In fact, a stronger statement holds: A nonzero polynomial in one variable (with rational coefficients) having degree \( n \geq 0 \) has at most \( n \) roots. See, for example, \( \text{[Goodman, Corollary 1.8.24]} \) for a proof.
with the sentence before. So \( P \) must be zero. In other words, \( P = 0 \). Lemma 3.2 (a) is proven.

(b) Every \( x \in \mathbb{N} \) satisfies \((P - Q)(x) = P(x) - Q(x) = 0 \) (since \( P(x) = Q(x) \)). Hence, Lemma 3.2 (a) (applied to \( P - Q \) instead of \( P \)) yields \( P - Q = 0 \). Thus, \( P = Q \). Lemma 3.2 (b) is thus proven.

(c) Every \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \) satisfy
\[
P(x, y) = 0. \tag{52}
\]

We can write the polynomial \( P \) in the form
\[
P = \sum_{k=0}^{d} P_k(X) Y^k,
\]
where \( d \) is an integer and where each \( P_k(X) \) (for \( 0 \leq k \leq d \)) is a polynomial in the single variable \( X \). Consider this \( d \) and these \( P_k(X) \).

Fix \( \alpha \in \mathbb{N} \). Every \( x \in \mathbb{N} \) satisfies \( P(\alpha, x) = 0 \) (by (52), applied to \( \alpha \) and \( x \) instead of \( x \) and \( y \)).

Therefore, Lemma 3.2 (a) (applied to \( \sum_{k=0}^{d} P_k(X) X^k \) instead of \( P \)) yields that
\[
\sum_{k=0}^{d} P_k(\alpha) X^k = 0
\]
as polynomials (in the indeterminate \( X \)). In other words, all coefficients of the polynomial \( \sum_{k=0}^{d} P_k(\alpha) X^k \) are 0. In other words, \( P_k(\alpha) = 0 \) for all \( k \in \{0, 1, \ldots, d\} \).

Now, let us forget that we fixed \( \alpha \). We thus have shown that \( P_k(\alpha) = 0 \) for all \( k \in \{0, 1, \ldots, d\} \) and \( \alpha \in \mathbb{N} \).

Let us now fix \( k \in \{0, 1, \ldots, d\} \). Then, \( P_k(\alpha) = 0 \) for all \( \alpha \in \mathbb{N} \). In other words, \( P_k(x) = 0 \) for all \( x \in \mathbb{N} \). Hence, Lemma 3.2 (a) (applied to \( P = P_k \)) yields that \( P_k = 0 \) as polynomials.

Let us forget that we fixed \( k \). We thus have proven that \( P_k = 0 \) as polynomials for each \( k \in \{0, 1, \ldots, d\} \). Hence, \( P = \sum_{k=0}^{d} P_k(X) Y^k = 0 \). This proves Lemma 3.2 (c).

(d) Every \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \) satisfy
\[
(P - Q)(x, y) = P(x, y) - Q(x, y) = 0 \quad \text{(since } P(x, y) = Q(x, y) \text{).}
\]
Hence, Lemma 3.2 (c) (applied to \( P - Q \) instead of \( P \)) yields \( P - Q = 0 \). Thus, \( P = Q \). Lemma 3.2 (d) is proven.
Of course, Lemma 3.2 can be generalized to polynomials in more than two variables (the proof of Lemma 3.2 (c) essentially suggests how to prove this generalization by induction over the number of variables).

3.3. The Chu-Vandermonde identity

The following fact is known as the Chu-Vandermonde identity:

**Theorem 3.3.** Let \( n \in \mathbb{N} \). Then,

\[
\binom{X + Y}{n} = \sum_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k}
\]

(an equality between polynomials in two variables \( X \) and \( Y \)).

We will give two proofs of this theorem: one combinatorial, and one algebraic.

**First proof of Theorem 3.3.** Let us first show that

\[
\binom{x + y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}
\]

for any \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \).

Keep in mind that (53) and Theorem 3.3 are different claims: The \( x \) and \( y \) in (53) are nonnegative integers, while the \( X \) and \( Y \) in Theorem 3.3 are indeterminates!

**Proof of (53):** For every \( N \in \mathbb{N} \), we let \([N]\) denote the \( N \)-element set \( \{1, 2, \ldots, N\} \).

---

39If you know what a commutative ring is, you might wonder whether Lemma 3.2 can also be generalized to polynomials with coefficients from other commutative rings (e.g., from \( R \) or \( C \)) instead of rational coefficients. In other words, what happens if we replace “rational coefficients” by “coefficients in \( R \)” throughout Lemma 3.2 where \( R \) is some commutative ring? (Of course, we will then have to also replace \( P(x) \) by \( P(x \cdot 1_R) \) and so on.)

The answer is that Lemma 3.2 becomes generally false if we don’t require anything more specific on \( R \). However, there are certain conditions on \( R \) that make Lemma 3.2 remain valid. For instance, Lemma 3.2 remains valid for \( R = \mathbb{Z} \), for \( R = \mathbb{R} \) and for \( R = \mathbb{C} \), as well as for \( R \) being any polynomial ring over \( \mathbb{Z} \), \( \mathbb{Q} \), \( \mathbb{R} \) or \( \mathbb{C} \). More generally, Lemma 3.2 is valid if \( R \) is any field of characteristic 0 (i.e., any field such that the elements \( n \cdot 1_R \) for \( n \) ranging over \( \mathbb{N} \) are pairwise distinct), or any subring of such a field.

40See the Wikipedia page for part of its history. Usually, the equality \( \binom{x + y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \)

for two nonnegative integers \( x \) and \( y \) is called the Vandermonde identity, whereas the name “Chu-Vandermonde identity” is used for the identity \( \binom{X + Y}{n} = \sum_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k} \) in which \( X \) and \( Y \) are indeterminates. However, this seems to be mostly a matter of convention (which isn’t even universally followed); and anyway the two identities are easily derived from one another as we will see in the first proof of Theorem 3.3.

41Note that Theorem 3.3 appears in [GrKnPa, (5.27)], where it is called Vandermonde’s convolution. The first proof of Theorem 3.3 we shall show below is just a more detailed writeup of the proof given there.
Let \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \). Recall that \( \binom{x+y}{n} \) is the number of \( n \)-element subsets of a given \((x+y)\)-element set. Since \([x+y]\) is an \((x+y)\)-element set, we thus conclude that \( \binom{x+y}{n} \) is the number of \( n \)-element subsets of \([x+y]\).

But let us count the \( n \)-element subsets of \([x+y]\) in a different way (i.e., find a different expression for the number of \( n \)-element subsets of \([x+y]\)). Namely, we can choose an \( n \)-element subset \( S \) of \([x+y]\) by means of the following process:

1. We decide how many elements of this subset \( S \) will be among the numbers \( 1, 2, \ldots, x \). Let \( k \) be the number of these elements. Clearly, \( k \) must be an integer between 0 and \( n \) (inclusive).

2. Then, we choose these \( k \) elements of \( S \) among the numbers \( 1, 2, \ldots, x \). This can be done in \( \binom{x}{k} \) different ways (because we are choosing \( k \) out of \( x \) numbers, with no repetitions, and with no regard for their order; in other words, we are choosing a \( k \)-element subset of \( \{1, 2, \ldots, x\} \)).

3. Then, we choose the remaining \( n-k \) elements of \( S \) (because \( S \) should have \( n \) elements in total) among the remaining numbers \( x+1, x+2, \ldots, x+y \). This can be done in \( \binom{y}{n-k} \) ways (because we are choosing \( n-k \) out of \( y \) numbers, with no repetitions, and with no regard for their order).

This process makes it clear that the total number of ways to choose an \( n \)-element subset \( S \) of \([x+y]\) is \( \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \). In other words, the number of \( n \)-element subsets of \([x+y]\) is \( \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \). But earlier, we have shown that the same number is \( \binom{x+y}{n} \). Comparing these two results, we conclude that \( \binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \). Thus, (53) is proven.

Now, we need to prove Theorem 3.3 itself. We define two polynomials \( P \) and \( Q \) in the indeterminates \( X \) and \( Y \) with rational coefficients by setting

\[
P = \binom{X+Y}{n};
\]

\[
Q = \sum_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k}
\]

This follows from (41).

43Because the subset \( S \) will have \( n \) elements in total, and thus at most \( n \) of them can be among the numbers \( 1, 2, \ldots, x \).
The equality \((53)\) (which we have proven) states that \(P(x, y) = Q(x, y)\) for all \(x \in \mathbb{N}\) and \(y \in \mathbb{N}\). Thus, Lemma 3.2(d) yields that \(P = Q\). Recalling how \(P\) and \(Q\) are defined, we can rewrite this as
\[
\binom{X + Y}{n} = \sum_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k}.
\]
This proves Theorem 3.3.

The argument that we used at the end of the above proof to derive Theorem 3.3 from \((53)\) is a very common argument that appears in proofs of equalities for binomial coefficients. Binomial coefficients are polynomials that can be evaluated at many different values, but their combinatorial interpretation (via counting subsets) only makes sense when they are evaluated at nonnegative integers. Thus, if we want to prove an identity of the form \(P = Q\) (where \(P\) and \(Q\) are two polynomials, say, in two indeterminates \(X\) and \(Y\)) using the combinatorial interpretation of binomial coefficients, then a reasonable tactic is to first show that \(P(x, y) = Q(x, y)\) for all \(x \in \mathbb{N}\) and \(y \in \mathbb{N}\) (using combinatorics), and then to use something like Lemma 3.2 in order to conclude that \(P\) and \(Q\) are equal as polynomials. We shall see this tactic used a few more times.

But we promised an algebraic proof of Theorem 3.3 as well; let us show it now:

**Second proof of Theorem 3.3.** We shall prove Theorem 3.3 by induction over \(n\).

**Induction base:** We have \(\binom{X}{0} = 1\). Substituting \(Y\) for \(X\) in this equality, we obtain \(\binom{Y}{0} = 1\). Hence,
\[
\sum_{k=0}^{0} \binom{X}{k} \binom{Y}{0-k} = \binom{X}{0} \binom{Y}{0-0} = 1.
\]
But substituting \(X + Y\) for \(X\) in \(\binom{X}{0} = 1\), we obtain \(\binom{X + Y}{0} = 1\). Compared

---

44These are both polynomials since \(\binom{X + Y}{n}\), \(\binom{X}{k}\) and \(\binom{Y}{n-k}\) are polynomials in \(X\) and \(Y\).

45For example, terms like \(\binom{-1/2}{3}\), \(\binom{2 + \sqrt{3}}{5}\) and \(\binom{-7}{0}\) make perfect sense. Generally, \(\binom{X}{n}\) is a polynomial in \(X\) with rational coefficients, and thus we can substitute any complex number for \(X\). So \(\binom{m}{n}\) is well-defined for all \(m \in \mathbb{C}\) and \(n \in \mathbb{N}\). (But we cannot substitute arbitrary complex numbers for \(n\). So far we have only defined \(\binom{X}{n}\) for \(n \in \mathbb{N}\). It is usual to define \(\binom{X}{n}\) to mean 0 for negative integers \(n\), and using analysis (specifically, the \(\Gamma\) function) it is possible to give a reasonable meaning to \(\binom{m}{n}\) for \(m\) and \(n\) being reals, but this will no longer be a polynomial in \(m\).)

46This tactic is called “the polynomial argument” in [GrKnPa §5.1].
with (54), this yields
\[
\binom{X + Y}{0} = \sum_{k=0}^{0} \binom{X}{k} \binom{Y}{0-k}.
\]
In other words, Theorem 3.3 holds for \( n = 0 \). This completes the induction base.

\textit{Induction step:} Let \( N \) be a positive integer. Assume that Theorem 3.3 holds for \( n = N - 1 \). We need to prove that Theorem 3.3 holds for \( n = N \). In other words, we need to prove that
\[
\binom{X + Y}{N} = \sum_{k=0}^{N} \binom{X}{k} \binom{Y}{N-k}.
\] (55)

(Don’t be fooled by the \( N \) being uppercase! The \( X \) and the \( Y \) are indeterminates, while the \( N \) is a fixed positive integer.)

We have assumed that Theorem 3.3 holds for \( n = N - 1 \). In other words, we have
\[
\binom{X + Y}{N-1} = \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y}{(N-1)-k}.
\] (56)

Substituting \( X - 1 \) for \( X \) in this equality, we obtain
\[
\binom{X - 1 + Y}{N - 1} = \sum_{k=0}^{N-1} \binom{X - 1}{k} \binom{Y}{(N-1)-k}
= \sum_{k=1}^{N} \binom{X - 1}{k-1} \binom{Y}{(N-1)-(k-1)}
= \binom{Y}{N-k}
\]
(here, we have substituted \( k - 1 \) for \( k \) in the sum)
\[
= \sum_{k=1}^{N} \binom{X - 1}{k-1} \binom{Y}{N-k}.
\]
Since \( X - 1 + Y = X + Y - 1 \), this rewrites as
\[
\binom{X + Y - 1}{N - 1} = \sum_{k=1}^{N} \binom{X - 1}{k-1} \binom{Y}{N-k}.
\] (57)

On the other hand, we can substitute \( Y - 1 \) for \( Y \) in the equality (56). As a result, we obtain
\[
\binom{X + Y - 1}{N - 1} = \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y - 1}{(N-1)-k} = \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y - 1}{N-k-1}.
\] (58)
Next, we notice a simple consequence of (49): We have

\[
\frac{X}{N} \left( \frac{X - 1}{a - 1} \right) = \frac{a}{N} \left( \frac{X}{a} \right)
\]
for every \(a \in \{1, 2, 3, \ldots\} \) \hspace{1cm} (59)

\[47\]

Also,

\[
\frac{Y}{N} \left( \frac{Y - 1}{a - 1} \right) = \frac{a}{N} \left( \frac{Y}{a} \right)
\]
for every \(a \in \{1, 2, 3, \ldots\} \).

(59) \hspace{1cm} (60)

(This follows by substituting \(Y\) for \(X\) in (59).)

We have

\[
\frac{X}{N} \left( \frac{X + Y - 1}{N - 1} \right) = \frac{X}{N} \sum_{k=1}^{N} \left( \frac{X - 1}{N - k} \right) \left( \frac{Y}{k} \right)
\]

\[= \sum_{k=1}^{N} \frac{X}{N} \left( \frac{X - 1}{N - k} \right) \left( \frac{Y}{k} \right)
\]

\[= \sum_{k=1}^{N} \frac{k}{N} \left( \frac{X}{k} \right) \left( \frac{Y}{N - k} \right)
\]

by (57)

Compared with

\[
\sum_{k=0}^{N} \frac{k}{N} \left( \frac{X}{k} \right) \left( \frac{Y}{N - k} \right)
\]

\[= \frac{0}{N} \left( \frac{X}{0} \right) \left( \frac{Y}{N - 0} \right) + \sum_{k=1}^{N} \frac{k}{N} \left( \frac{X}{k} \right) \left( \frac{Y}{N - k} \right) = \sum_{k=1}^{N} \frac{k}{N} \left( \frac{X}{k} \right) \left( \frac{Y}{N - k} \right),
\]

this yields

\[
\frac{X}{N} \left( \frac{X + Y - 1}{N - 1} \right) = \sum_{k=0}^{N} \frac{k}{N} \left( \frac{X}{k} \right) \left( \frac{Y}{N - k} \right).
\]

(61)

\[47\] Proof of (59): Let \(a \in \{1, 2, 3, \ldots\}\). Then, (49) \hspace{1cm} (applied to \(n = a\)) yields \(\left( \frac{X}{a} \right) = \frac{X}{a} \left( \frac{X - 1}{a - 1} \right)\). Hence,

\[
\frac{a}{N} \left( \frac{X}{a} \right) = \frac{a}{N} \cdot \frac{X}{a} \left( \frac{X - 1}{a - 1} \right) = \frac{X}{N} \left( \frac{X - 1}{a - 1} \right).
\]

This proves (59).
We also have
\[
\frac{Y}{N} \binom{X + Y - 1}{N - 1} = \frac{Y}{N} \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y - 1}{N - k - 1}
\]
\[= \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y - 1}{N - k - 1} \quad \text{(by (58))}
\]
\[= \sum_{k=0}^{N-1} \binom{X}{k} \frac{Y}{N} \binom{Y - 1}{N - k - 1} = \frac{Y}{N} \sum_{k=0}^{N-1} \binom{X}{k} \binom{Y - 1}{N - k - 1}
\]
\[= \sum_{k=0}^{N-1} \binom{X}{k} \frac{N - k}{N} \binom{Y}{N - k} = \sum_{k=0}^{N-1} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N - k} \cdot
\]

Compared with
\[
\sum_{k=0}^{N} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N - k} = \sum_{k=0}^{N-1} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N - k} + \frac{N - N}{N} \binom{X}{N} \binom{Y}{N - N}
\]
\[= \sum_{k=0}^{N-1} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N - k}
\]

this yields
\[
\frac{Y}{N} \binom{X + Y - 1}{N - 1} = \sum_{k=0}^{N} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N - k} \cdot \quad (62)
\]

Now, (49) (applied to \( n = N \)) yields
\[
\binom{X}{N} = \frac{X}{N} \binom{X - 1}{N - 1}.
\]
Substituting $X + Y$ for $X$ in this equality, we obtain

\[
\binom{X + Y}{N} = \frac{X + Y}{N} \binom{X + Y - 1}{N - 1} = \left(\frac{X}{N} + \frac{Y}{N}\right) \binom{X + Y - 1}{N - 1}
\]

\[
= \frac{X}{N} \binom{X + Y - 1}{N - 1} + \frac{Y}{N} \binom{X + Y - 1}{N - 1}
\]

\[
= \sum_{k=0}^{N} \frac{k}{N} \binom{X}{k} \binom{Y}{N-k} = \sum_{k=0}^{N} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N-k} \quad \text{(by (61))}
\]

\[
= \sum_{k=0}^{N} \frac{k}{N} \binom{X}{k} \binom{Y}{N-k} + \sum_{k=0}^{N} \frac{N - k}{N} \binom{X}{k} \binom{Y}{N-k}
\]

\[
= \sum_{k=0}^{N} \left(\frac{k}{N} + \frac{N - k}{N}\right) \binom{X}{k} \binom{Y}{N-k} = \sum_{k=0}^{N} \binom{X}{k} \binom{Y}{N-k}.
\]

This proves (55). In other words, Theorem 3.3 holds for $n = N$. This completes the induction step. Thus, the induction proof of Theorem 3.3 is complete. \qed

Let us give some sample applications of Theorem 3.3.

**Proposition 3.4.** (a) For every $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and $n \in \mathbb{N}$, we have

\[
\binom{x + y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.
\]

(b) For every $x \in \mathbb{N}$ and $y \in \mathbb{Z}$, we have

\[
\binom{x + y}{x} = \sum_{k=0}^{x} \binom{x}{k} \binom{y}{k}.
\]

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

\[
\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.
\]

(d) For every $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and $n \in \mathbb{N}$, we have

\[
\binom{x - y}{n} = \sum_{k=0}^{n} (-1)^k \binom{x}{n-k} \binom{k + y - 1}{k}.
\]

(e) For every $x \in \mathbb{N}$ and $y \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $x \leq n$, we have

\[
\binom{y - x - 1}{n - x} = \sum_{k=0}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}.
\]
(f) For every $x \in \mathbb{N}$ and $y \in \mathbb{N}$ and $n \in \mathbb{N}$, we have
\[
\binom{n + 1}{x + y + 1} = \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y}.
\]

(g) For every $x \in \mathbb{Z}$ and $y \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfying $x + y \geq 0$ and $n \geq x$, we have
\[
\binom{x + y}{n} = \sum_{k=0}^{x+y} \binom{x}{k} \binom{y}{n-k}.
\]

**Remark 3.5.** I have learnt Proposition 3.4 (f) from the AoPS forum. Proposition 3.4 (g) is a generalization of Proposition 3.4 (b).

**Proof of Proposition 3.4.**

(a) Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and $n \in \mathbb{N}$. Theorem 3.3 yields
\[
\binom{X + Y}{n} = \sum_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k}. \quad \text{Substituting } x \text{ and } y \text{ for } X \text{ and } Y \text{ in this equality, we obtain}
\]
\[
\binom{x + y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}. \quad \text{Thus, Proposition 3.4 (a) is proven.}
\]

(b) Let $x \in \mathbb{N}$ and $y \in \mathbb{Z}$. Proposition 3.4 (a) (applied to $y$, $x$ and $x$ instead of $x$, $y$ and $n$) yields
\[
\binom{y + x}{x} = \sum_{k=0}^{x} \binom{y}{k} \binom{x}{x-k}.
\]

Compared with
\[
\sum_{k=0}^{x} \binom{x}{k} \binom{y}{k} = \sum_{k=0}^{x} \binom{x}{x-k} \binom{y}{k} = \sum_{k=0}^{x} \binom{y}{k} \binom{x}{x-k},
\]
(by (39), applied to $m=x$ and $n=k$)

this yields
\[
\binom{y + x}{x} = \sum_{k=0}^{x} \binom{x}{k} \binom{y}{k}. \quad \text{Since } y + x = x + y, \text{ this rewrites as } \binom{x + y}{x} =
\]
\[
\sum_{k=0}^{x} \binom{x}{k} \binom{y}{k}. \quad \text{This proves Proposition 3.4 (b).}
\]

(c) Let $n \in \mathbb{N}$. Applying Proposition 3.4 (b) to $x = n$ and $y = n$, we obtain
\[
\binom{n + n}{n} = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.
\]
\[
= \binom{n}{k}^2
\]
Since \( n + n = 2n \), this rewrites as \( \binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2 \). This proves Proposition 3.4 (c).

(d) Let \( x \in \mathbb{Z} \) and \( y \in \mathbb{Z} \) and \( n \in \mathbb{N} \). Proposition 3.4 (a) (applied to \(-y\) instead of \(y\)) yields

\[
\binom{x + (-y)}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{(-y)}{n-k} = \sum_{k=0}^{n} \binom{x}{k} \binom{-y}{n-(n-k)} = \left(\frac{-y}{k}\right)
\]

(here, we substituted \( n - k \) for \( k \) in the sum)

\[
= \sum_{k=0}^{n} \binom{x}{n-k} \left(\frac{-y}{k}\right) = (-1)^k \binom{k - (-y) - 1}{k}
\]

(by \[42\], applied to \( k \) and \(-y\) instead of \( n \) and \( m \))

\[
= \sum_{k=0}^{n} (-1)^k \binom{x}{n-k} \left(\frac{k + y - 1}{k}\right)
\]

Since \( x + (-y) = x - y \), this rewrites as \( \binom{x - y}{n} = \sum_{k=0}^{n} (-1)^k \binom{x}{n-k} \left(\frac{k + y - 1}{k}\right) \).

This proves Proposition 3.4 (d).

(e) Let \( x \in \mathbb{N} \) and \( y \in \mathbb{Z} \) and \( n \in \mathbb{N} \) be such that \( x \leq n \). From \( x \in \mathbb{N} \), we obtain \( 0 \leq x \) and thus \( 0 \leq x \leq n \). We notice that every integer \( k \geq x \) satisfies

\[
\binom{k}{k-x} = \binom{k}{x}
\]

(63)

Furthermore, \( n - x \in \mathbb{N} \) (since \( x \leq n \)). Hence, we can apply Proposition 3.4 (a)

---

\[48\] Proof of (63): Let \( k \) be an integer such that \( k \geq x \). Thus, \( k - x \in \mathbb{N} \). Recall that \( k \geq x \). Hence, \[39\]

(applied to \( k \) and \( x \) instead of \( m \) and \( n \)) yields \( \binom{k}{x} = \binom{k}{k-x} \). This proves (63).
to \( y, -x - 1 \) and \( n - x \) instead of \( x, y \) and \( n \). As a result, we obtain

\[
\begin{align*}
\binom{y + (-x - 1)}{n - x} &= \sum_{k=0}^{n-x} \binom{y}{k} \binom{-x - 1}{(n - x) - k} \\
&= (-1)^{(n-x)-k} \binom{(n - x) - k - (-x - 1) - 1}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{(n - x) - k - (-x - 1) - 1}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \binom{n - (n - k)}{(n - x) - (n - k)} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \binom{n - (n - k)}{(n - x) - (n - k)} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} \binom{y}{k} (-1)^{(n-x) - k} \binom{n - k}{(n - x) - k} \\
&= \sum_{k=0}^{n-x} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}. 
\end{align*}
\]
Compared with

\[ \sum_{k=0}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k} = \sum_{k=0}^{x-1} (-1)^{k-x} \binom{k}{x} \left( \binom{y}{n-k} + \sum_{k=x}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k} \right) \]

(by (38), applied to \( k \) and \( x \)
instead of \( m \) and \( n \) (since \( k < x \))

\[ (\text{since } 0 \leq x \leq n) \]

\[ = \sum_{k=0}^{x-1} (-1)^{k-x} 0 \binom{y}{n-k} + \sum_{k=x}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k} = \sum_{k=x}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}, \]

this yields

\[ \binom{y + (-x - 1)}{n - x} = \sum_{k=0}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}. \]

In other words,

\[ \binom{y - x - 1}{n - x} = \sum_{k=0}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k} \]

(since \( y + (-x - 1) = y - x - 1 \)). This proves Proposition 3.4(e).

(f) Let \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \) and \( n \in \mathbb{N} \). We must be in one of the following two cases:

Case 1: We have \( n < x + y \).

Case 2: We have \( n \geq x + y \).

Let us first consider Case 1. In this case, we have \( n < x + y \). Thus, \( n + 1 < x + y + 1 \). Therefore, \( \binom{n + 1}{x + y + 1} = 0 \) (by (38), applied to \( n + 1 \) and \( x + y + 1 \)

\[ \text{instead of } m \text{ and } n \). But every \( k \in \{0, 1, \ldots, n\} \) satisfies \( \binom{k}{x} \binom{n-k}{y} = 0 \) 49.

---

49Proof. Let \( k \in \{0, 1, \ldots, n\} \). We need to show that \( \binom{k}{x} \binom{n-k}{y} = 0 \).

If we have \( k < x \), then we have \( \binom{k}{x} = 0 \) (by (38), applied to \( k \) and \( x \) instead of \( m \) and \( n \)). Therefore, if we have \( k < x \), then \( \binom{k}{x} \binom{n-k}{y} = 0 \). Hence, for the rest of this proof of

\[ \binom{k}{x} \binom{n-k}{y} = 0, \text{ we can WLOG assume that we don’t have } k < x \). Assume this.

We have \( k \leq n \) (since \( k \in \{0, 1, \ldots, n\} \)) and thus \( n-k \in \mathbb{N} \).

We have \( k \geq x \) (since we don’t have \( k < x \)), and thus \( n-k \geq x \leq n-x < y \) (since \( n <
Hence, \[ \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y} = 0. \] Compared with \( \binom{n+1}{x+y+1} = 0 \), this yields
\[ \binom{n+1}{x+y+1} = \sum_{k=0}^{n} \frac{n}{k} \binom{n-k}{y}. \] Thus, Proposition 3.4 (f) is proven in Case 1.

Let us now consider Case 2. In this case, we have \( n \geq x + y \). Hence, \( n - y \geq x \) (since \( x \in \mathbb{N} \)), so that \( n - y - x \in \mathbb{N} \). Also, \( n - y \geq 0 \) and thus \( n - y \in \mathbb{N} \). Moreover, \( x \leq n - y \). Therefore, we can apply Proposition 3.4 (e) to \( -y - 1 \) and \( n - y \) instead of \( y \) and \( n \). As a result, we obtain
\[
\begin{align*}
\left( \binom{-y - 1}{n - y - x} \right) &= \sum_{k=0}^{n-y} (-1)^{n-x} \binom{k}{x} \left( \binom{-y - 1}{n-y-k} \right) \\
&= (-1)^{n-y+k} \binom{k}{x} \left( \binom{n-y-k}{n-y-1} \right) \\
&= (-1)^{n-y-k} \binom{n-k}{n-y-k} \\
&= \left( \binom{n-k}{n-y-k} \right) \\
&= \left( \binom{n-k}{n-y-k} \right) \\
&= \left( \binom{n-k}{n-y-k} \right) \\
&= \left( \binom{n-k}{n-y-k} \right) \\
&= \left( \binom{n-k}{n-y-k} \right).
\end{align*}
\]

But every \( k \in \{0,1,\ldots,n-y\} \) satisfies
\[
\binom{n-k}{n-y-k} = \binom{n-k}{y} = 0.
\]

\( x + y \). Hence, \( \binom{n-k}{y} = 0 \) (by 38), applied to \( n-k \) and \( y \) instead of \( m \) and \( n \). Therefore, \( \binom{k}{x} \binom{n-k}{y} = 0 \), qed.
Thus, (64) yields
\[
\begin{align*}
\left(\frac{(-y - 1) - x - 1}{n - y} - x\right) &= (-1)^{n-x-y} \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{(n-y)-k} \\
&= (-1)^{n-x-y} \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y} \\
&= (-1)^{n-x-y} \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y}.
\end{align*}
\]

Compared with
\[
\left(\frac{(-y - 1) - x - 1}{n - y} - x\right) = \frac{(-1)^{(n-y)-x} ((n-y) - x) - ((-y - 1) - x - 1) - 1}{(n-y) - x} = (-1)^{n+1} \frac{n + 1}{n - x - y}.
\]

This yields
\[
(-1)^{n-x-y} \binom{n+1}{n-x-y} = (-1)^{n-x-y} \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y}.
\]

We can cancel \((-1)^{n-x-y}\) from this equality (because \((-1)^{n-x-y} \neq 0\)). As a result, we obtain
\[
\binom{n+1}{n-x-y} = \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y}.
\]

But 0 \(\leq n - y\) (since \(n - y \in \mathbb{N}\)) and \(n - y \leq n\) (since \(y \in \mathbb{N}\)). Also, every \(k \in \{n - y + 1, n - y + 2, \ldots, n\}\) satisfies
\[
\binom{n-k}{y} = 0.
\]

Proof of (64): Let \(k \in \{0, 1, \ldots, n - y\}\). Then, \(k \in \mathbb{N}\) and \(n - y \geq k\). From \(n - y \geq k\), we obtain \(n \geq y + k\), so that \(n - k \geq y\). Thus, \(n - k \geq y \geq 0\), so that \(n - k \in \mathbb{N}\). Hence, (59) (applied to \(n - k\) and \(y\) instead of \(m\) and \(n\)) yields
\[
\binom{n-k}{y} = \binom{n-k}{(n-k)-y} = \binom{n-k}{(n-y)-k}.
\]

Since \((n-k) - y = (n-y) - k\). This proves (65).
Hence,
\[
\sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y} = \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y} + \sum_{k=n-y+1}^{n} \binom{k}{x} \binom{n-k}{y} \quad \text{(since } 0 \leq n - y \leq n) \\
= \sum_{k=0}^{n-y} \binom{k}{x} \binom{n-k}{y} + \sum_{k=n-y+1}^{n} \binom{k}{y} \binom{n-k}{y} = 0 \quad \text{(by } 67) \\
= \binom{n+1}{n-x-y} \quad \text{(by } 66). \tag{68}
\]

Finally, \( n + 1 \in \mathbb{N} \) and \( x + y + 1 \in \mathbb{N} \) (since \( x \in \mathbb{N} \) and \( y \in \mathbb{N} \)) and \( n \geq x + y + 1 \). Hence, \( 39 \) (applied to \( n + 1 \) and \( x + y + 1 \) instead of \( m \) and \( n \)) yields
\[
\binom{n+1}{x+y+1} = \binom{n+1}{n+1-(x+y+1)} = \binom{n+1}{n-x-y}
\]
(since \( (n+1) - (x+y+1) = n-x-y \)). Comparing this with \( 68 \), we obtain
\[
\binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y}.
\]

Thus, Proposition \( 3.4(f) \) is proven in Case 2.
We have now proven Proposition \( 3.4(f) \) in both Cases 1 and 2; thus, Proposition \( 3.4(f) \) always holds.

\( g \) Let \( x \in \mathbb{Z} \) and \( y \in \mathbb{N} \) and \( n \in \mathbb{N} \) be such that \( x + y \geq 0 \) and \( n \geq x \). We have \( x + y \in \mathbb{N} \) (since \( x + y \geq 0 \)). We must be in one of the following two cases:

- **Case 1**: We have \( x + y < n \).
- **Case 2**: We have \( x + y \geq n \).

Let us first consider Case 1. In this case, we have \( x + y < n \). Thus, \( \binom{x+y}{n} = 0 \)
(by \( 38 \), applied to \( m = x+y \)). But every \( k \in \{0,1,\ldots,x+y\} \) satisfies \( \binom{y}{n+k-x} = \)

---

\( ^{51} \) Proof of \( 67 \): Let \( k \in \{n-y+1,n-y+2,\ldots,n\} \). Then, \( k \leq n \) and \( k > n - y \). Hence, \( n-k \in \mathbb{N} \) (since \( k \leq n \)) and \( n - \binom{k}{n-y} < n - (n - y) = y \). Therefore, \( 38 \) (applied to \( n-k \) and \( y \) instead of \( m \) and \( n \)) yields \( \binom{n-k}{y} = 0 \). This proves \( 67 \).
Thus, \( \sum_{k=0}^{\infty} \binom{x+y}{k} \binom{y}{n+k-x} = \sum_{k=0}^{\infty} \binom{x+y}{k} 0 = 0 \). Compared with \( \binom{x+y}{n} = 0 \), this yields \( \binom{x+y}{n} = \sum_{k=0}^{x+y} \binom{x+y}{k} \binom{y}{n+k-x} \). Thus, Proposition 3.4 (g) is proven in Case 1.

Let us now consider Case 2. In this case, we have \( x+y \geq n \). Hence, \( \binom{x+y}{n} = \binom{x+y}{x+y-n} \) (by (39), applied to \( m = x+y \)). Also, \( x+y-n \in \mathbb{N} \) (since \( x+y \geq n \)). Therefore, Proposition 3.4 (a) (applied to \( x+y-n \) instead of \( n \)) yields
\[
\binom{x+y}{x+y-n} = \sum_{k=0}^{x+y-n} \binom{x+y-n}{k} \binom{y}{x+y-n-k}.
\]

Since \( \binom{x+y}{x+y-n} = \binom{x+y}{x+y-n} \), this rewrites as
\[
\binom{x+y}{n} = \sum_{k=0}^{x+y-n} \binom{x+y-n}{k} \binom{y}{x+y-n-k}.
\]

But every \( k \in \{0,1,\ldots,x+y-n\} \) satisfies \( \binom{y}{x+y-n-k} = \binom{n+k-x}{n+k-x} \) \(^{53}\).

Hence, (69) becomes
\[
\binom{x+y}{n} = \sum_{k=0}^{x+y-n} \binom{x+y-n}{k} \binom{y}{x+y-n-k} = \sum_{k=0}^{x+y-n} \binom{x+y-n}{k} \binom{y}{n+k-x}.
\]

On the other hand, we have \( 0 \leq n \leq x+y \) and thus \( 0 \leq x+y-n \leq x+y \). But every \( k \in \mathbb{N} \) satisfying \( k > x+y-n \) satisfies
\[
\binom{y}{n+k-x} = 0
\]
\(^{53}\)Proof. Let \( k \in \{0,1,\ldots,x+y\} \). Then, \( k \geq 0 \), so that \( n+k-x \geq n-x+y \) (since \( n > x+y \) (since \( x+y < n \))). In other words, \( y < n+k-x \). Also, \( n+k-x > y \geq 0 \), so that \( n+k-x \in \mathbb{N} \).

Hence, \( \binom{y}{n+k-x} = 0 \) (by (38), applied to \( y \) and \( n+k-x \) instead of \( m \) and \( n \)). Qed.

Therefore, (39) (applied to \( y \) and \( x+y-n-k \) instead of \( m \) and \( n \)) yields
\[
\binom{y}{y-(x+y-n-k)} = \binom{y}{n+k-x} \text{ (since } y-(x+y-n-k) = n+k-x \text{)}, \text{ qed.}
\]
Hence,
\[
\sum_{k=0}^{x+y} \binom{x}{k} \binom{y}{n+k-x} = \sum_{k=0}^{x+y-n} \binom{x}{k} \binom{y}{n+k-x} + \sum_{k=(x+y-n)+1}^{x+y} \binom{x}{k} \binom{y}{n+k-x} = 0
\]
(by (71) (since \( k > x+y-n \))

(since \( 0 \leq x + y - n \leq x + y \))
\[
= \sum_{k=0}^{x+y-n} \binom{x}{k} \binom{y}{n+k-x} + \sum_{k=(x+y-n)+1}^{x+y} \binom{x}{k} 0 = \sum_{k=0}^{x+y-n} \binom{x}{k} \binom{y}{n+k-x}.
\]

Compared with (70), this yields
\[
\binom{x+y}{n} = \sum_{k=0}^{x+y} \binom{x}{k} \binom{y}{n+k-x}.
\]

This proves Proposition 3.4 (g) in Case 2.

Proposition 3.4 (g) is thus proven in each of the two cases 1 and 2. Therefore, Proposition 3.4 (g) holds in full generality.

**Remark 3.6.** The proof of Proposition 3.4 given above illustrates a useful technique: the use of upper negation (i.e., the equality (42)) to transform one equality into another. In a nutshell,

- we have proven Proposition 3.4 (d) by applying Proposition 3.4 (a) to \(-y\) instead of \(y\), and then rewriting the result using upper negation;
- we have proven Proposition 3.4 (e) by applying Proposition 3.4 (a) to \(y\), \(-x - 1\) and \(n - x\) instead of \(x\), \(y\) and \(n\), and then rewriting the resulting identity using upper negation;
- we have proven Proposition 3.4 (f) by applying Proposition 3.4 (e) to \(-y - 1\) and \(n - y\) instead of \(y\) and \(n\), and rewriting the resulting identity using upper negation.

Thus, by substitution and rewriting using upper negation, one single equality (namely, Proposition 3.4 (a)) has morphed into three other equalities. Note, in particular, that no negative numbers appear in Proposition 3.4 (f), but yet we proved it by substituting negative values for \(x\) and \(y\).

**Proof.** Let \( k \in \mathbb{N} \) be such that \( k > x + y - n \). Then, \( n + k > x + y - n \), hence \( n + k - x > x > n + (x + y - n) - x = y \). In other words, \( y < n + k - x \). Also, \( n + k - x > y \geq 0 \), so that \( n + k - x \in \mathbb{N} \). Hence, (38) (applied to \( y \) and \( n + k - x \) instead of \( m \) and \( n \)) yields \( \binom{y}{n+k-x} = 0 \), qed.
3.4. Further results

Exercise 2. Let \( n \) be a nonnegative integer. Prove that there exist nonnegative integers \( c_{i,j} \) for all \( 0 \leq i \leq n \) and \( 0 \leq j \leq n \) such that

\[
\binom{XY}{n} = \sum_{i=0}^{n} \sum_{j=0}^{n} c_{i,j} \binom{X}{i} \binom{Y}{j}
\]  

(an equality between polynomials in two variables \( X \) and \( Y \)).

Notice that the integers \( c_{i,j} \) in Exercise 2 can depend on the \( n \) (besides depending on \( i \) and \( j \)). We just have not included the \( n \) in the notation because it is fixed.

Exercise 3. Let \( a, b \) and \( c \) be three nonnegative integers. Prove that the polynomial \( (aX + b)^c \) in the variable \( X \) (this is a polynomial in \( X \) of degree \( \leq c \)) can be written as a sum \( \sum_{i=0}^{c} d_i \binom{X}{i} \) with nonnegative \( d_i \).

Proposition 3.7. Let \( a \) and \( b \) be two nonnegative integers. There exist nonnegative integers \( e_0, e_1, \ldots, e_{a+b} \) such that

\[
\binom{X}{a} \binom{X}{b} = \sum_{i=0}^{a+b} e_i \binom{X}{i}
\]  

(an equality between polynomials in \( X \)).

First proof of Proposition [3.7] For every \( N \in \mathbb{N} \), we let \([N]\) denote the \( N \)-element set \( \{1, 2, \ldots, N\} \).

For every set \( S \), we let an \( S \)-junction mean a pair \((A, B)\), where \( A \) is an \( a \)-element subset of \( S \) and where \( B \) is a \( b \)-element subset of \( S \) such that \( A \cup B = S \). (We do not mention \( a \) and \( b \) in our notation, because \( a \) and \( b \) are fixed.)

For example, if \( a = 2 \) and \( b = 3 \), then \( (\{1, 4\}, \{2, 3, 4\}) \) is a \( 4 \)-junction, and \( (\{2, 4\}, \{1, 4, 6\}) \) is a \( \{1, 2, 4, 6\} \)-junction, but \( (\{1, 3\}, \{2, 3, 5\}) \) is not a \( [5] \)-junction (since \( \{1, 3\} \cup \{2, 3, 5\} \neq [5] \)).

For every \( i \in \mathbb{N} \), we let \( e_i \) be the number of all \([i]\)-junctions. Then, if \( S \) is any \( i \)-element set, then

\[ e_i \text{ is the number of all S-junctions} \]  

55 Proof of [73]: Let \( S \) be any \( i \)-element set. We know that \( e_i \) is the number of all \([i]\)-junctions. We want to prove that \( e_i \) is the number of all \( S \)-junctions. Roughly speaking, this is obvious, because we can “relabel the elements of \( S \) as \( 1, 2, \ldots, i \)” (since \( S \) is an \( i \)-element set), and then the \( S \)-junctions become precisely the \([i]\)-junctions.

Here is a formal way to make this argument: The sets \([i] \) and \( S \) have the same number of
Now, let us show that
\[
\binom{x}{a} \binom{x}{b} = \sum_{i=0}^{a+b} e_i \binom{x}{i}
\]  
(74)

for every \( x \in \mathbb{N} \).

**Proof of (74):** Let \( x \in \mathbb{N} \). How many ways are there to choose a pair \((A, B)\) consisting of an \( a \)-element subset \( A \) of \([x]\) and a \( b \)-element subset \( B \) of \([x]\)?

Let us give two different answers to this question. The first answer is the straightforward one: To choose a pair \((A, B)\) consisting of an \( a \)-element subset \( A \) of \([x]\) and a \( b \)-element subset \( B \) of \([x]\), we need to choose an \( a \)-element subset \( A \) of \([x]\) and a \( b \)-element subset \( B \) of \([x]\). There are \( \binom{x}{a} \) total ways to do this (since there are \( \binom{x}{a} \) choices for \( A \) and \( \binom{x}{b} \) choices for \( B \) and these choices are independent). In other words, the number of all pairs \((A, B)\) consisting of an \( a \)-element subset \( A \) of \([x]\) and a \( b \)-element subset \( B \) of \([x]\) equals \( \binom{x}{a} \binom{x}{b} \).

On the other hand, here is a more imaginative procedure to choose a pair \((A, B)\) consisting of an \( a \)-element subset \( A \) of \([x]\) and a \( b \)-element subset \( B \) of \([x]\):

1. We choose how many elements the union \( A \cup B \) will have. In other words, we choose an \( i \in \mathbb{N} \) that will satisfy \( |A \cup B| = i \). This \( i \) must be an integer between 0 and \( a + b \) (inclusive).

2. We choose a subset \( S \) of \([x]\), which will serve as the union \( A \cup B \). This subset \( S \) must be an \( i \)-element subset of \([x]\) (because we will have \( |S| = |A \cup B| = i \)). Thus, there are \( \binom{x}{i} \) ways to choose it (since we need to choose an \( i \)-element subset of \([x]\)).

3. Now, it remains to choose the pair \((A, B)\) itself. This pair must be a pair of subsets of \([x]\) satisfying \( |A| = a \), \( |B| = b \), \( A \cup B = S \) and \( |A \cup B| = i \). We

---

56 This follows from (41).
57 Again, this follows from (41).
58 Proof. Clearly, \( i \) cannot be smaller than 0. But \( i \) also cannot be larger than \( a + b \) (since \( i \) will have to satisfy \( i = |A \cup B| \leq |A| + |B| = a + b \)). Thus, \( i \) must be an integer between 0 and \( a + b \) (inclusive).
can forget about the $|A \cup B| = i$ condition, since it automatically follows from $A \cup B = S$ (because $|S| = i$). So we need to choose a pair $(A, B)$ of subsets of $[x]$ satisfying $|A| = a, |B| = b$ and $A \cup B = S$. In other words, we need to choose a pair $(A, B)$ of subsets of $S$ satisfying $|A| = a, |B| = b$ and $A \cup B = S$.

In other words, we need to choose an $S$-junction (since this is how an $S$-junction was defined). This can be done in exactly $e_i$ ways (according to (73)).

Thus, in total, there are $\sum_{i=0}^{a+b} \binom{x}{i} e_i$ ways to perform this procedure. Hence, the total number of all pairs $(A, B)$ consisting of an $a$-element subset $A$ of $[x]$ and a $b$-element subset $B$ of $[x]$ equals $\sum_{i=0}^{a+b} \binom{x}{i} e_i$. But earlier, we have shown that this number is $\binom{x}{a} \binom{x}{b} e_i$. Comparing these two results, we conclude that $\binom{x}{a} \binom{x}{b} = \sum_{i=0}^{a+b} \binom{x}{i} e_i$. Thus, (74) is proven.

Now, we define two polynomials $P$ and $Q$ in the indeterminate $X$ with rational coefficients by setting

$$P = \binom{X}{a} \binom{X}{b}; \quad Q = \sum_{i=0}^{a+b} e_i \binom{X}{i}.$$

The equality (74) (which we have proven) states that $P(x) = Q(x)$ for all $x \in \mathbb{N}$. Thus, Lemma 3.2 (b) yields that $P = Q$. Recalling how $P$ and $Q$ are defined, we see that this rewrites as $\binom{X}{a} \binom{X}{b} = \sum_{i=0}^{a+b} e_i \binom{X}{i}$. This proves Proposition 3.7.

Second proof of Proposition 3.7. Here is an algebraic proof of Proposition 3.7 (based on a suggestion of math.stackexchange user tcamps in a comment on question #1342384).

Theorem 3.3 (applied to $n = b$) yields

$$\binom{X + Y}{b} = \sum_{k=0}^{b} \binom{X}{k} \binom{Y}{b-k}.$$

This is a polynomial identity in $X$ and $Y$; we can thus substitute $X - a$ and $a$ for $X$ and $Y$. As a result of this substitution, we obtain

$$\binom{(X-a) + a}{b} = \sum_{k=0}^{b} \binom{X-a}{k} \binom{a}{b-k}.$$
Since \((X - a) + a = X\), this rewrites as
\[
\binom{X}{b} = \sum_{k=0}^{b} \binom{X - a}{k} \binom{a}{b - k} = \sum_{i=a}^{a+b} \binom{X - a}{i - a} \binom{a}{b - (i - a)} = \binom{a}{a + b - i}
\]
(here, we substituted \(i - a\) for \(k\) in the sum)
\[
= a + b \sum_{i=a}^{i=a+b} \binom{X - a}{i - a} \binom{a}{a + b - i}.
\]

Multiplying both sides of this identity with \(\binom{X}{a}\), we obtain
\[
\binom{X}{a} \binom{X}{b} = \binom{X}{a} \sum_{i=a}^{a+b} \binom{X - a}{i - a} \binom{a}{a + b - i} = \sum_{i=a}^{a+b} \binom{X}{a} \binom{X - a}{i - a} \binom{a}{a + b - i} = \binom{X}{i} \binom{a}{i}
\]
(by \((50)\))
\[
= a + b \sum_{i=a}^{i=a+b} \binom{X}{i} \binom{a}{a + b - i} = a + b \sum_{i=a}^{i=a+b} \binom{i}{a} \binom{a}{a + b - i} \binom{X}{i}.
\]

Now, let us define \(a + b + 1\) nonnegative integers \(e_0, e_1, \ldots, e_{a+b}\) by
\[
e_i = \begin{cases} 
\binom{i}{a} \binom{a}{a + b - i}, & \text{if } i \geq a; \\
0, & \text{otherwise}
\end{cases}
\]
for all \(i \in \{0, 1, \ldots, a+b\}\). (76)

Then,
\[
\sum_{i=0}^{a+b} e_i \binom{X}{i} = \sum_{i=a}^{i=a+b} \binom{i}{a} \binom{a}{a + b - i} \binom{X}{i} = \binom{X}{a} \binom{X}{b} \quad \text{(by our definition of } e_0, e_1, \ldots, e_{a+b})
\]
(by \((75)\)).

Thus, Proposition 3.7 is proven again.

\[\square\]

**Remark 3.8.** Comparing our two proofs of Proposition 3.7, it is natural to suspect that the \(e_0, e_1, \ldots, e_{a+b}\) defined in the First proof are identical with the \(e_0, e_1, \ldots, e_{a+b}\) defined in the Second proof. This actually follows from general principles (namely, from the word “unique” in Proposition 3.1 (a)), but there is also a simple combinatorial reason. Namely, let \(i \in \{0, 1, \ldots, a+b\}\). We shall show that the \(e_i\) defined in the First proof equals the \(e_i\) defined in the Second proof.
The \( e_i \) defined in the First proof is the number of all \([i]\)-junctions. An \([i]\)-junction is a pair \((A, B)\), where \(A\) is an \(a\)-element subset of \([i]\) and where \(B\) is a \(b\)-element subset of \([i]\) such that \(A \cup B = [i]\). Here is a way to construct an \([i]\)-junction:

- First, we pick the set \(A\). There are \(\binom{i}{a}\) ways to do this, since \(A\) has to be an \(a\)-element subset of the \(i\)-element set \([i]\).
- Then, we pick the set \(B\). This has to be a \(b\)-element subset of the \(i\)-element set \([i]\) satisfying \(A \cup B = [i]\). The equality \(A \cup B = [i]\) means that \(B\) has to contain the \(i - a\) element of \([i] \setminus A\); but the remaining \(b - (i - a) = a + b - i\) elements of \(B\) can be chosen arbitrarily among the \(a\) elements of \(A\). Thus, there are \(\binom{a}{a + b - i}\) ways to choose \(B\) (since we have to choose \(a + b - i\) elements of \(B\) among the \(a\) elements of \(A\)).

Thus, the number of all \([i]\)-junctions is \(\binom{i}{a} \binom{a}{a + b - i}\). This can be rewritten in the form

\[
\begin{cases}
\binom{i}{a} \binom{a}{a + b - i}, & \text{if } i \geq a; \\
0, & \text{otherwise}
\end{cases}
\]

and thus \(\binom{i}{a} \binom{a}{a + b - i} = 0\). Thus, we have shown that the number of all \([i]\)-junctions is \(\begin{cases}
\binom{i}{a} \binom{a}{a + b - i}, & \text{if } i \geq a; \\
0, & \text{otherwise}
\end{cases}\). In other words, the \(e_i\) defined in the First proof equals the \(e_i\) defined in the Second proof.

Here is an assortment of other identities that involve binomial coefficients:

**Proposition 3.9.** (a) Every \(x \in \mathbb{Z}\), \(y \in \mathbb{Z}\) and \(n \in \mathbb{N}\) satisfy \((x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\).

(b) Every \(n \in \mathbb{N}\) satisfies \(\sum_{k=0}^{n} \binom{n}{k} = 2^n\).

(c) Every \(n \in \mathbb{N}\) satisfies \(\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0. \end{cases}\)

(d) Every \(n \in \mathbb{Z}\), \(i \in \mathbb{N}\) and \(a \in \mathbb{N}\) satisfying \(i \geq a\) satisfy \(\binom{n}{i} \binom{i}{a} = \binom{n}{a} \binom{n-a}{i-a}\).

(e) Every \(n \in \mathbb{N}\) and \(m \in \mathbb{Z}\) satisfy \(\sum_{i=0}^{n} \binom{n}{i} \binom{m+i}{n} = \sum_{i=0}^{n} \binom{n}{i} \binom{m}{i} 2^i\).
(f) Every \(a \in \mathbb{N}, b \in \mathbb{N}\) and \(x \in \mathbb{Z}\) satisfy \(\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \frac{x+i}{a+b} = \frac{x}{a} \frac{x}{b}\).

(g) Every \(a \in \mathbb{N}, b \in \mathbb{N}\) and \(x \in \mathbb{Z}\) satisfy \(\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \frac{a+b+x-i}{a+b} = \binom{a+x}{a} \binom{b+x}{b}\).

(Parts (e) and (f) of Proposition 3.9 are from AoPS. Part (g) is a restatement of [Gould10, (6.93)].)

Proof of Proposition 3.9. (a) Let \(x \in \mathbb{Z}, y \in \mathbb{Z}\) and \(n \in \mathbb{N}\). Substituting \(X = x\) and \(Y = y\) into (48), we obtain \((x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\). This proves Proposition 3.9 (a).

(b) Let \(n \in \mathbb{N}\). Applying Proposition 3.9 (a) to \(x = 1\) and \(y = 1\), we obtain \((1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{1} \frac{1}{1} = \sum_{k=0}^{n} \binom{n}{k}, \) thus \(\sum_{k=0}^{n} \binom{n}{k} = \binom{1+1}{2} = 2\). This proves Proposition 3.9 (b).

(c) Let \(n \in \mathbb{N}\). Applying Proposition 3.9 (a) to \(x = -1\) and \(y = 1\), we obtain \((-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \frac{1}{1} \frac{1}{1} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \sum_{k=0}^{n} (-1)^k \binom{n}{k}, \) thus \(\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{-1+1}{0} = 0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0. \end{cases}\). This proves Proposition 3.9 (c).

(d) Let \(n \in \mathbb{Z}, i \in \mathbb{N}\) and \(a \in \mathbb{N}\) be such that \(i \geq a\). Substituting \(n\) for \(X\) in the equality (50), we obtain \(\binom{n}{i} \binom{i}{a} = \binom{n-a}{i-a}\). This proves Proposition 3.9 (d).

(e) Let \(n \in \mathbb{N}\) and \(m \in \mathbb{Z}\). Clearly, every \(p \in \mathbb{N}\) satisfies \(\sum_{i=0}^{p} \binom{p}{i} = \sum_{k=0}^{p} \binom{p}{k}\) (here, we renamed the summation index \(i\) as \(k\))

(by Proposition 3.9 (b), applied to \(p\) instead of \(n\)).

Now, let \(i \in \{0, 1, \ldots, n\}\). Applying Proposition 3.4 (a) to \(x = i\) and \(y = m\), we
obtain
\[
\binom{i+m}{n} = \sum_{k=0}^{n} \binom{i}{k} \binom{m}{n-k}
\]
\[
= \sum_{k=0}^{i} \binom{i}{k} \binom{m}{n-k} + \sum_{k=i+1}^{n} \binom{i}{k} \binom{m}{n-k}
\]
\[
= \sum_{k=0}^{i} \binom{i}{k} \binom{m}{n-k} + \sum_{k=i+1}^{n} 0 \binom{m}{n-k}
\]
\[
= \sum_{k=0}^{i} \binom{i}{k} \binom{m}{n-k}
\]
(78)

(by (38), applied to \(i\) and \(k\) instead of \(m\) and \(n\) (since \(i < k\))

Now, let us forget that we fixed \(i\). We thus have proven (78) for every \(i \in\)
{0, 1, \ldots, n}. Now,

\[
\sum_{i=0}^{n} \binom{n}{i} \binom{m+i}{n} = \sum_{k=0}^{i} \binom{i}{k} \binom{m}{n-k} \tag{by (78)}
\]

\[
= \sum_{i=0}^{n} \sum_{k=0}^{i} \binom{n}{i} \binom{i}{k} \binom{m}{n-k} = \sum_{k=0}^{n} \sum_{i=k}^{n} \binom{n}{k} \binom{i}{i-k} \binom{m}{n-i-k} \tag{by Proposition 3.9(d), applied to a=k (since n\geq k)}
\]

\[
= \sum_{k=0}^{n} \binom{n}{k} \binom{m}{n-k} \sum_{i=0}^{n-k} \binom{n-k}{i} \tag{here, we have substituted i for i-k in the second sum}
\]

\[
= \sum_{k=0}^{n} \binom{n}{k} 2^k = \sum_{i=0}^{n} \binom{n}{i} \binom{m}{i} 2^i \tag{here, we have renamed the summation index k as i). This proves Proposition 3.9(e).}
\]

\[(f) \text{ Let } a \in \mathbb{N}, b \in \mathbb{N} \text{ and } x \in \mathbb{Z}. \text{ Let us first work with polynomials in the indeterminate } X \text{ (rather than functions in the variable } x \in \mathbb{Z}). \text{ Recall that}
\]

\[
\binom{X}{a} \binom{X}{b} = \sum_{i=a}^{a+b} \binom{i}{a} \binom{a}{a+i} \binom{X}{i}. \tag{79}
\]

(Indeed, this is precisely the identity (75) which was proven in the Second proof of Proposition 3.7.)
Clearly, 

\[
\sum_{i=0}^{a+b} \binom{a}{i} \binom{b}{i} \frac{(X+i)}{a+b}
\]

\[
= \sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \frac{(X+i)}{a+b} + \sum_{i=b+1}^{a+b} \binom{a}{i} \binom{b}{i} \frac{(X+i)}{a+b}
\]

(by \(38\), applied to \(b\) and \(i\)

(since \(0 \leq b \leq a + b\))

\[
= \sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \frac{(X+i)}{a+b}.
\]

\[\text{(80)}\]

Theorem 3.3 (applied to \(n = a + b\)) yields

\[
\binom{X+Y}{a+b} = \sum_{k=0}^{a+b} \binom{X}{k} \binom{Y}{a+b-k}.
\]

\[\text{(81)}\]

For every \(i \in \{0, 1, \ldots, b\}\), we have

\[
\binom{X+i}{a+b} = \sum_{k=0}^{a+b} \binom{X}{k} \binom{i}{a+b-k}.
\]

(This follows by substituting \(Y = i\) in \(81\).) Hence,

\[
\sum_{i=0}^{a+b} \binom{a}{i} \binom{b}{i} \frac{(X+i)}{a+b}
\]

\[
= \sum_{k=0}^{a+b} \binom{X}{k} \binom{i}{a+b-k}
\]

\[
= \sum_{i=0}^{a+b} \sum_{k=0}^{b} \binom{a}{i} \binom{b}{i} \binom{X}{k} \binom{i}{a+b-k}
\]

\[
= \sum_{k=0}^{a+b} \sum_{i=0}^{a+b-k} \binom{i}{a+b-k} \binom{b}{i} \binom{X}{k}
\]

\[
= \sum_{k=0}^{a+b} \sum_{i=0}^{a+b-k} \binom{a}{i} \binom{i}{a+b-k} \binom{b}{i} \binom{X}{k}.
\]

\[\text{This follows by substituting } Y = i \text{ in } (81).\]
Compared with (80), this yields
\[
\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} (X+i) = \sum_{k=0}^{a+b} \binom{X}{k} \sum_{i=0}^{a+b} \binom{a}{i} \binom{i}{a+b-k} (b). \tag{82}
\]

But for every \(k \in \{0,1,\ldots,a+b\}\), we have
\[
\sum_{i=0}^{a+b} \binom{a}{i} \binom{i}{a+b-k} (b) = \binom{a}{a+b-k} \sum_{j=0}^{k} (k-b) \binom{b}{a+b-j}
\]
Hence, (82) becomes
\[
\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} (X+i) = \sum_{k=0}^{a+b} \binom{X}{k} \sum_{i=0}^{a+b} \binom{a}{i} \binom{i}{a+b-k} (b)
\]
\[
= \sum_{k=0}^{a+b} \binom{X}{k} \binom{a}{a+b-k} \sum_{j=0}^{k} (k-b) \binom{b}{a+b-j}
\]
\[
= \sum_{i=0}^{a+b} \binom{X}{i} \binom{a}{a+b-i} \sum_{j=0}^{i} (i-b) \binom{b}{a+b-j}
\]
(83)
(here, we renamed the summation index \(k\) as \(i\) in the first sum). Furthermore, every \(i \in \{0,1,\ldots,a+b\}\) satisfies
\[
\sum_{j=0}^{i} (i-b) \binom{b}{a+b-j} = \binom{i}{a}
\]
\[\text{Proof.}\] Let \(k \in \{0,1,\ldots,a+b\}\). Then, \(a+b-k \in \{0,1,\ldots,a+b\}\), so that \(0 \leq a+b-k \leq a+b\).
Now,

\[
\sum_{i=0}^{a+b-k-1} \binom{a}{i} \binom{b}{i} + \sum_{i=a+b-k}^{a+b} \binom{a}{i} \binom{b}{i} = 0
\]

(by \[18\], applied to \(i\) and \(a+b-k\) instead of \(m\) and \(n\) (since \(i \leq a+b-k\))

\[
= \sum_{i=0}^{a+b-k-1} \binom{a}{i} \binom{b}{i} + \sum_{i=a+b-k}^{a+b} \binom{a}{i} \binom{b}{i}
\]

(by Proposition \[17\](d), applied to \(a\) and \(a+b-k\) instead of \(n\) and \(a\) (since \(i \geq a+b-k\))

\[
= \sum_{j=0}^{k} \binom{a}{a+b-k} \binom{b}{a+b-j} = \binom{a}{a+b-k} \sum_{j=0}^{k} \binom{k-b}{k-j} \binom{b}{a+b-j},
\]

(here, we have substituted \(a+b-j\) for \(i\) in the sum)

61 Proof. Let \(i \in \{0, 1, \ldots, a+b\}\). Thus, \(0 \leq i \leq a+b\). We have

\[
\sum_{j=0}^{i} \binom{i-b}{i-j} \binom{b}{a+b-j} = \sum_{k=0}^{i} \binom{i-b}{i-(i-k)} \binom{b}{a+b-(i-k)} = \binom{b}{a+b-(i-k)} \sum_{j=0}^{k-b} \binom{k-b}{k-j} \binom{b}{a+b-j},
\]

(here, we have substituted \(i-k\) for \(j\) in the sum)
On the other hand, we have $b \in \mathbb{N}$, $(i - b) + b = i \geq 0$ and $a \geq i - b$ (since $a + b \geq i$). Therefore, we can apply Proposition 3.14(g) to $i - b$, $b$ and $a$ instead of $x$, $y$ and $n$. As a result, we obtain

\[
\binom{(i - b) + b}{a} = \sum_{k=0}^{(i-b)+b} \binom{i - b}{k} \binom{b}{a + k - (i - b)} = \sum_{k=0}^{(i-b)+b} \binom{i - b}{k} \binom{b}{(a + b) + k - i}.
\]

Since $(i - b) + b = i$, this rewrites as

\[
\binom{i}{a} = \sum_{k=0}^{i} \binom{i - b}{k} \binom{b}{(a + b) + k - i}.
\]

Compared with (84), this yields

\[
\sum_{j=0}^{i} \binom{i-b}{i-j} \binom{b}{a + b - j} = \binom{i}{a},
\]

qed.
Hence, (83) becomes

\[
\sum_{i=0}^{\frac{a+b}{i}} \binom{a}{i} \binom{b}{i} \frac{(X + i)}{a + b} = \sum_{i=0}^{\frac{a+b}{i}} \binom{a}{i} \frac{a}{a + b - i} \binom{a + i}{a + b - i} \left(\frac{X}{a}\right) = \sum_{i=0}^{\frac{a+b}{a}} \binom{a}{a} \frac{a}{a + b - i} \binom{a + i}{a + b - i} \left(\frac{X}{a}\right) + \sum_{i=0}^{\frac{a+b}{i}} \binom{a}{i} \frac{a}{a + b - i} \binom{a + i}{a + b - i} \left(\frac{X}{a}\right)
\]

(by (38), applied to \(i\) and \(a\)
instead of \(m\) and \(n\) (since \(i < a\))

(since \(0 \leq a \leq a + b\))

\[
\sum_{i=0}^{\frac{a+b}{a}} 0 \frac{a}{a + b - i} \binom{X}{i} + \sum_{i=0}^{\frac{a+b}{a}} \binom{a}{a} \frac{a}{a + b - i} \binom{a + i}{a + b - i} \left(\frac{X}{a}\right)
\]

\[
= \sum_{i=0}^{\frac{a+b}{a}} \binom{i}{a} \frac{a}{a + b - i} \binom{X}{i} = \binom{X}{a} \binom{b}{X} = \binom{b}{a} \binom{a + x}{a + b} = \binom{b}{b} \binom{x}{b} \quad \text{(by (79)).}
\]

Substituting \(X = x\) in this equality, we obtain

\[
\sum_{i=0}^{\frac{a+b}{a}} \binom{a}{i} \frac{b}{i} \binom{x + i}{a + b} = \binom{x}{a} \binom{b}{x}.
\]

This proves Proposition 3.9 (f).

\(\textbf{(g)}\) Let \(a \in \mathbb{N}, b \in \mathbb{N}\) and \(x \in \mathbb{Z}\). From (42) (applied to \(m = -x - 1\) and \(n = a\)), we obtain \(\binom{-x - 1}{a} = (-1)^a \binom{a - (-x - 1) - 1}{a} = (-1)^a \binom{a + x}{a}\) (since \(a - (-x - 1) - 1 = a + x\)). The same argument (applied to \(b\) instead of \(a\)) shows that \(\binom{-x - 1}{b} = (-1)^b \binom{b + x}{b}\).
Now, Proposition 3.9(f) (applied to \(-x - 1\) instead of \(x\)) shows that
\[
\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \left(\frac{-x - 1 + i}{a + b}\right) = \frac{(-x - 1)}{a} \left(\frac{-x - 1}{b}\right)
\]
\[= (-1)^a \left(\frac{a + x}{a}\right) (-1)^b \left(\frac{b + x}{b}\right)
\]
\[= (-1)^a \binom{a + x}{a} \left(\frac{-x - 1 + i}{a + b}\right)
\]
\[= (-1)^{a+b} \left(\frac{a + x}{a}\right) \left(\frac{b + x}{b}\right).
\]
(85)

But every \(i \in \{0, 1, \ldots, b\}\) satisfies
\[
\left(\frac{-x - 1 + i}{a + b}\right) = (-1)^{a+b} \left(\frac{a + b - ((-x - 1) + i) - 1}{a + b}\right)
\]
(by [42], applied to \(m = (-x - 1) + i\) and \(n = a + b\))
\[= (-1)^{a+b} \left(\frac{a + b + x - i}{a + b}\right)
\]
(since \(a + b - ((-x - 1) + i) - 1 = a + b + x - i\)).

Hence,
\[
\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \left(\frac{-x - 1 + i}{a + b}\right) = (-1)^{a+b} \binom{a + b + x - i}{a + b}
\]
\[= \sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} (-1)^{a+b} \left(\frac{a + b + x - i}{a + b}\right) = (-1)^{a+b} \sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \left(\frac{a + b + x - i}{a + b}\right).
\]

Comparing this with (85), we obtain
\[
(-1)^{a+b} \sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \left(\frac{a + b + x - i}{a + b}\right) = (-1)^{a+b} \left(\frac{a + x}{a}\right) \left(\frac{b + x}{b}\right).
\]

We can cancel \((-1)^{a+b}\) from this equality (since \((-1)^{a+b} \neq 0\)), and thus obtain
\[
\sum_{i=0}^{b} \binom{a}{i} \binom{b}{i} \left(\frac{a + b + x - i}{a + b}\right) = \left(\frac{a + x}{a}\right) \left(\frac{b + x}{b}\right).
\]
This proves Proposition 3.9(g).

Many more examples of equalities with binomial coefficients, as well as advanced tactics for proving such equalities, can be found in [GrKnPa, Chapter 5].
3.5. Additional exercises

This section contains some further exercises. These will not be used in the rest of the notes, and they can be skipped at will. I am not planning to provide solutions for them.

**Additional exercise 1.** Find a different proof of Proposition 3.4 (f) that uses a double-counting argument (i.e., counting some combinatorial objects in two different ways, and then concluding that the results are equal).

**[Hint]**: How many \((x + y + 1)\)-element subsets does the set \(\{1, 2, \ldots, n + 1\}\) have? Now, for a given \(k \in \{0, 1, \ldots, n\}\), how many \((x + y + 1)\)-element subsets whose \((x + 1)\)-th smallest element is \(k + 1\) does the set \(\{1, 2, \ldots, n + 1\}\) have?

**Additional exercise 2.** Let \(n \in \mathbb{N}\) and \(k \in \mathbb{N}\) be fixed. Show that the number of all \(k\)-tuples \((a_1, a_2, \ldots, a_k) \in \mathbb{N}^k\) satisfying \(a_1 + a_2 + \cdots + a_k = n\) equals \(\binom{n + k - 1}{k}\).

**Remark 3.10.** Additional exercise can be restated in terms of multisets. Namely, let \(n \in \mathbb{N}\) and \(k \in \mathbb{N}\) be fixed. Also, fix a \(k\)-element set \(K\). Then, the number of \(n\)-element multisets whose elements all belong to \(K\) is \(\binom{n + k - 1}{k}\). Indeed, we can WLOG assume that \(K = \{1, 2, \ldots, k\}\) (otherwise, just relabel the elements of \(K\)); then, the multisets whose elements all belong to \(K\) are in bijection with the \(k\)-tuples \((a_1, a_2, \ldots, a_k) \in \mathbb{N}^k\). The bijection sends a multiset \(M\) to the \(k\)-tuple \((m_1(M), m_2(M), \ldots, m_k(M))\), where each \(m_i(M)\) is the multiplicity of the element \(i\) in \(M\). The size of a multiset \(M\) corresponds to the sum \(a_1 + a_2 + \cdots + a_k\) of the entries of the resulting \(k\)-tuple; thus, we get a bijection between

- the \(n\)-element multisets whose elements all belong to \(K\)

and

- the \(k\)-tuples \((a_1, a_2, \ldots, a_k) \in \mathbb{N}^k\) satisfying \(a_1 + a_2 + \cdots + a_k = n\).

As a consequence, Additional exercise shows that the number of the former multisets is \(\binom{n + k - 1}{k}\).

Similarly, we can reinterpret the classical combinatorial interpretation of \(\binom{k}{n}\) (as the number of \(n\)-element subsets of \(\{1, 2, \ldots, k\}\)) as follows: The number of all \(k\)-tuples \((a_1, a_2, \ldots, a_k) \in \{0, 1\}^k\) satisfying \(a_1 + a_2 + \cdots + a_k = n\) equals \(\binom{k}{n}\).

---

62 The same, of course, can be said for many of the standard exercises.
Additional exercise 3. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $n \geq k$. Prove that

$$
\sum_{u=0}^{k} \binom{n+u-1}{u} \binom{n}{k-2u} = \binom{n+k-1}{k}.
$$

Here, $\binom{a}{b}$ is defined to be 0 when $b < 0$.

Additional exercise 4. Let $N \in \mathbb{N}$. The binomial transform of a finite sequence $(f_0, f_1, \ldots, f_N) \in \mathbb{Z}^{N+1}$ is defined to be the sequence $(g_0, g_1, \ldots, g_N)$ defined by

$$
g_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f_i \quad \text{for every } n \in \{0, 1, \ldots, N\}.
$$

(a) Let $(f_0, f_1, \ldots, f_N) \in \mathbb{Z}^{N+1}$ be a finite sequence of integers. Let $(g_0, g_1, \ldots, g_N)$ be the binomial transform of $(f_0, f_1, \ldots, f_N)$. Show that $(f_0, f_1, \ldots, f_N)$ is, in turn, the binomial transform of $(g_0, g_1, \ldots, g_N)$.

(b) Find the binomial transform of the sequence $(1, 1, \ldots, 1)$.

(c) For any given $a \in \mathbb{N}$, find the binomial transform of the sequence $(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a})$.

(d) For any given $q \in \mathbb{Z}$, find the binomial transform of the sequence $(q^0, q^1, \ldots, q^N)$.

(e) Find the binomial transform of the sequence $(1, 0, 1, 0, 1, 0, \ldots)$ (this ends with 1 if $N$ is even, and with 0 if $N$ is odd).

(f) Let $B : \mathbb{Z}^{N+1} \to \mathbb{Z}^{N+1}$ be the map which sends every sequence $(f_0, f_1, \ldots, f_N) \in \mathbb{Z}^{N+1}$ to its binomial transform $(g_0, g_1, \ldots, g_N) \in \mathbb{Z}^{N+1}$. Thus, part (a) of this exercise states that $B^2 = \text{id}$.

On the other hand, let $W : \mathbb{Z}^{N+1} \to \mathbb{Z}^{N+1}$ be the map which sends every sequence $(f_0, f_1, \ldots, f_N) \in \mathbb{Z}^{N+1}$ to $((-1)^N f_N, (-1)^N f_{N-1}, \ldots, (-1)^N f_0) \in \mathbb{Z}^{N+1}$. It is rather clear that $W^2 = \text{id}$.

Show that, furthermore, $B \circ W \circ B = W \circ B \circ W$ and $(B \circ W)^3 = \text{id}$.

Additional exercise 5. For any $n \in \mathbb{N}$ and $m \in \mathbb{N}$, define a polynomial $Z_{m,n} \in \mathbb{Z}[X]$ by

$$
Z_{m,n} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (X^{n-k} - 1)^m.
$$

Show that $Z_{m,n} = Z_{n,m}$ for any $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

Additional exercise 6. Let $n \in \mathbb{N}$. Prove

$$
\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{X}{n-k} = \begin{cases} 
(-1)^{n/2} \binom{X}{n/2}, & \text{if } n \text{ is even;} \\
0, & \text{if } n \text{ is odd}
\end{cases}
$$
(an identity between polynomials in \( \mathbb{Q}[X] \)).

**[Hint]**: It is enough to prove this when \( X \) is replaced by a nonnegative integer \( r \) (why?). Now that you have gotten rid of polynomials, introduce new polynomials. Namely, compute the coefficient of \( X^n \) in \( (1 + X)^r (1 - X)^r \). Compare with the coefficient of \( X^n \) in \( (1 - X^2)^r \).]

The following exercise is a variation on (47):

**Additional exercise 7.** Let \( a \) and \( b \) be two integers such that \( b \neq 0 \). Let \( n \in \mathbb{N} \). Show that there exists some \( N \in \mathbb{N} \) such that \( b^N \binom{a/b}{n} \in \mathbb{Z} \).

**[Hint]**: I am not aware of a combinatorial solution to this exercise! (I.e., I don’t know what the numbers \( b^N \binom{a/b}{n} \) count, even when they are nonnegative.) All solutions that I know use some (elementary) number theory. For the probably slickest (although unmotivated) solution, basic modular arithmetic suffices; here is a roadmap: First, show that if \( b \) and \( c \) are integers such that \( c > 0 \), then there exists an \( s \in \mathbb{Z} \) such that \( b^{c-1} \equiv sb^c \mod c \). Apply this to \( c = n! \) and conclude that \( b^{n!} (a/b - i) \equiv b^{n!} (sa - i) \mod n! \) for every \( i \in \mathbb{Z} \). Now use \( \binom{sa}{n} \in \mathbb{Z} \).]

## 4. Recurrent sequences

### 4.1. Basics

Two of the most famous integer sequences defined recursively are the Fibonacci sequence and the Lucas sequence:

- The **Fibonacci sequence** is the sequence \( (f_0, f_1, f_2, \ldots) \) of integers which is defined recursively by \( f_0 = 0, f_1 = 1, \) and \( f_n = f_{n-1} + f_{n-2} \) for all \( n \geq 2 \). Its first terms are

\[
\begin{align*}
  f_0 &= 0, & f_1 &= 1, & f_2 &= 1, & f_3 &= 2, & f_4 &= 3, & f_5 &= 5, \\
  f_6 &= 8, & f_7 &= 13, & f_8 &= 21, & f_9 &= 34, & f_{10} &= 55, \\
  f_{11} &= 89, & f_{12} &= 144, & f_{13} &= 233.
\end{align*}
\]

(Some authors prefer to start the sequence at \( f_1 \) rather than \( f_0 \); of course, the recursive definition then needs to be modified to require \( f_2 = 1 \) instead of \( f_0 = 0 \).)

---

\(^{63}\)To prove this, argue that at least two of \( b^0, b^1, \ldots, b^c \) are congruent modulo \( c \).
The Lucas sequence is the sequence \((\ell_0, \ell_1, \ell_2, \ldots)\) of integers which is defined recursively by \(\ell_0 = 2, \ell_1 = 1,\) and \(\ell_n = \ell_{n-1} + \ell_{n-2}\) for all \(n \geq 2.\) Its first terms are
\[
\ell_0 = 2, \quad \ell_1 = 1, \quad \ell_2 = 3, \quad \ell_3 = 4, \quad \ell_4 = 7, \quad \ell_5 = 11, \\
\ell_6 = 18, \quad \ell_7 = 29, \quad \ell_8 = 47, \quad \ell_9 = 76, \quad \ell_{10} = 123, \\
\ell_{11} = 199, \quad \ell_{12} = 322, \quad \ell_{13} = 521.
\]

A lot of papers have been written about these two sequences, the relations between them, and the identities that hold for their terms. One of their most striking properties is that they can be computed explicitly, albeit using irrational numbers. In fact, the Binet formula says that the \(n\)-th Fibonacci number \(f_n\) can be computed by
\[
f_n = \frac{1}{\sqrt{5}} \varphi^n - \frac{1}{\sqrt{5}} \psi^n,
\]
where \(\varphi = \frac{1 + \sqrt{5}}{2}\) and \(\psi = \frac{1 - \sqrt{5}}{2}\) are the two solutions of the quadratic equation \(X^2 - X - 1 = 0.\) (The number \(\varphi\) is known as the golden ratio; the number \(\psi\) can be obtained from it by \(\psi = 1 - \varphi = -1/\varphi.\)) A similar formula, using the very same numbers \(\varphi\) and \(\psi,\) exists for the Lucas numbers:
\[
\ell_n = \varphi^n + \psi^n.
\]

Remark 4.1. How easy is it to compute \(f_n\) and \(\ell_n\) using the formulas (86) and (87)?

This is a nontrivial question. Indeed, if you are careless, you may find them rather useless. For instance, if you try to compute \(f_n\) using the formula (86) and using approximate values for the irrational numbers \(\varphi\) and \(\psi,\) then you might end up with a wrong value for \(f_n,\) because the error in the approximate value for \(\varphi\) propagates when you take \(\varphi\) to the \(n\)-th power. (And for high enough \(n,\) the error will become larger than 1, so you will not be able to get the correct value by rounding.) The greater \(n\) is, the more precise you need a value for \(\varphi\) to approximate \(f_n\) this way. Thus, approximating \(\varphi\) is not a good way to compute \(f_n.\) (Actually, the opposite is true: You can use (86) to approximate \(\varphi\) by computing Fibonacci numbers. Namely, it is easy to show that \(\varphi = \lim_{n \to \infty} \frac{f_n}{f_{n-1}}.\))

A better approach to using (86) is to work with the exact values of \(\varphi\) and \(\psi.\) To do so, you need to know how to add, subtract, multiply and divide real numbers of the form \(a + b\sqrt{5}\) with \(a, b \in \mathbb{Q}\) without ever using approximations. (Clearly, \(\varphi, \psi\) and \(\sqrt{5}\) all have this form.) There are rules for this, which are simple to

\[\text{See } \text{https://oeis.org/A000045 and https://oeis.org/A000032 for an overview of their properties.}\]
some further examples of sequences, and generalize (86) and (87) to a broader class of sequences.  

\[
\begin{align*}
(a+b\sqrt{5}) + (c+d\sqrt{5}) &= (a+c) + (b+d)\sqrt{5}; \\
(a+b\sqrt{5}) - (c+d\sqrt{5}) &= (a-c) + (b-d)\sqrt{5}; \\
(a+b\sqrt{5}) \cdot (c+d\sqrt{5}) &= (ac + 5bd) + (bc + ad)\sqrt{5}; \\
\frac{a+b\sqrt{5}}{c+d\sqrt{5}} &= \frac{(ac - 5bd) + (bc - ad)\sqrt{5}}{c^2 - 5d^2} \text{ for } (c,d) \neq (0,0).
\end{align*}
\]

(The last rule is an instance of "rationalizing the denominator"). These rules give you a way to exactly compute things like \(\varphi^n, \frac{1}{\sqrt{5}}\varphi^n, \psi^n\) and \(\frac{1}{\sqrt{5}}\psi^n\), and thus also \(f_n\) and \(\ell_n\). If you use exponentiation by squaring to compute \(n\)-th powers, this actually becomes a fast algorithm (a lot faster than just computing \(f_n\) and \(\ell_n\) using the recurrence). So, yes, (86) and (87) are useful.

We shall now study a generalization of both the Fibonacci and the Lucas sequences, and generalize (86) and (87) to a broader class of sequences.

**Definition 4.2.** If \(a\) and \(b\) are two complex numbers, then a sequence \((x_0, x_1, x_2, \ldots)\) of complex numbers will be called \((a,b)\)-recurrent if every \(n \geq 2\) satisfies

\[x_n = ax_{n-1} + bx_{n-2}.
\]

So, the Fibonacci sequence and the Lucas sequences are \((1,1)\)-recurrent. An \((a,b)\)-recurrent sequence \((x_0, x_1, x_2, \ldots)\) is fully determined by the four values \(a, b, x_0\) and \(x_1\), and can be constructed for any choice of these four values. Here are some further examples of \((a,b)\)-recurrent sequences:

- A sequence \((x_0, x_1, x_2, \ldots)\) is \((2,-1)\)-recurrent if and only if every \(n \geq 2\) satisfies \(x_n = 2x_{n-1} - x_{n-2}\). In other words, a sequence \((x_0, x_1, x_2, \ldots)\) is \((2,-1)\)-recurrent if and only if every \(n \geq 2\) satisfies \(x_n - x_{n-1} = x_{n-1} - x_{n-2}\). In other words, a sequence \((x_0, x_1, x_2, \ldots)\) is \((2,-1)\)-recurrent if and only if \(x_1 - x_0 = x_2 - x_1 = x_3 - x_2 = \cdots\). In other words, the \((2,-1)\)-recurrent sequences are precisely the arithmetic progressions.

- Geometric progressions are also \((a,b)\)-recurrent for appropriate \(a\) and \(b\). Namely, any geometric progression \((u, uq, uq^2, uq^3, \ldots)\) is \((q,0)\)-recurrent, since every \(n \geq 2\) satisfies \(uq^n = q \cdot uq^{n-1} + 0 \cdot uq^{n-2}\). However, not every \((q,0)\)-recurrent sequence \((x_0, x_1, x_2, \ldots)\) is a geometric progression (since the condition \(x_n = qx_{n-1} + 0x_{n-2}\) for all \(n \geq 2\) says nothing about \(x_0\), and thus \(x_0\) can be arbitrary).
• A sequence \((x_0, x_1, x_2, \ldots)\) is \((0,1)\)-recurrent if and only if every \(n \geq 2\) satisfies \(x_n = x_{n-2}\). In other words, a sequence \((x_0, x_1, x_2, \ldots)\) is \((0,1)\)-recurrent if and only if it has the form \((u, v, u, v, u, v, \ldots)\) for two complex numbers \(u\) and \(v\).

• A sequence \((x_0, x_1, x_2, \ldots)\) is \((1,0)\)-recurrent if and only if every \(n \geq 2\) satisfies \(x_n = x_{n-1}\). In other words, a sequence \((x_0, x_1, x_2, \ldots)\) is \((1,0)\)-recurrent if and only if it has the form \((u, v, v, u, v, \ldots)\) for two complex numbers \(u\) and \(v\). Notice that \(u\) is not required to be equal to \(v\), because we never claimed that \(x_n = x_{n-1}\) holds for \(n = 1\).

• A sequence \((x_0, x_1, x_2, \ldots)\) is \((1,-1)\)-recurrent if and only if every \(n \geq 2\) satisfies \(x_n = x_{n-1} - x_{n-2}\). Curiously, it turns out that every such sequence is 6-periodic (i.e., it satisfies \(x_{n+6} = x_n\) for every \(n \in \mathbb{N}\), because every \(n \in \mathbb{N}\) satisfies

\[
x_{n+6} = x_{n+5} - x_{n+4} = (x_{n+4} - x_{n+3}) - x_{n+4} = -x_{n+3} = x_{n+2} - x_{n+1} = -x_{n+1} - x_n = x_n.
\]

More precisely, a sequence \((x_0, x_1, x_2, \ldots)\) is \((1,0)\)-recurrent if and only if it has the form \((u, v, v - u, -u, -v, u - v, \ldots)\) (where the "\(\ldots\)" stands for "repeat the preceding 6 values over and over" here) for two complex numbers \(u\) and \(v\).

• The above three examples notwithstanding, most \((a,b)\)-recurrent sequences of course are not periodic. However, here is another example which provides a great supply of non-periodic \((a,b)\)-recurrent sequences and, at the same time, explains why we get so many periodic ones: If \(\alpha\) is any angle, then the sequences

\[
(sin (0\alpha), sin (1\alpha), sin (2\alpha), \ldots) \quad \text{and} \quad (cos (0\alpha), cos (1\alpha), cos (2\alpha), \ldots)
\]

are \((2 \cos \alpha, -1)\)-recurrent. More generally, if \(\alpha\) and \(\beta\) are two angles, then the sequence

\[
(sin (\beta + 0\alpha), sin (\beta + 1\alpha), sin (\beta + 2\alpha), \ldots)
\]

is \((2 \cos \alpha, -1)\)-recurrent\(^{65}\). When \(\alpha \in 2\pi \mathbb{Q}\) (that is, some integer multiple of \(\alpha\) equals some integer multiple of \(2\pi\)), this sequence is periodic.

\(^{65}\)Proof. Let \(\alpha\) and \(\beta\) be two angles. We need to show that the sequence \((sin (\beta + 0\alpha), sin (\beta + 1\alpha), sin (\beta + 2\alpha), \ldots)\) is \((2 \cos \alpha, -1)\)-recurrent. In other words, we need to prove that

\[
sin (\beta + na) = 2 \cos \alpha \sin (\beta + (n-1)\alpha) + (-1)^n \sin (\beta + (n-2)\alpha)
\]

for every \(n \geq 2\). So fix \(n \geq 2\).
4.2. Explicit formulas (à la Binet)

Now, we can get an explicit formula (similar to (86) and (87)) for every term of an \((a, b)\)-recurrent sequence (in terms of \(a, b, x_0\) and \(x_1\)) in the case when \(a^2 + 4b \neq 0\). Here is how this works:

**Remark 4.3.** Let \(a\) and \(b\) be complex numbers such that \(a^2 + 4b \neq 0\). Let \((x_0, x_1, x_2, \ldots)\) be an \((a, b)\)-recurrent sequence. We want to construct an explicit formula for each \(x_n\) in terms of \(x_0, x_1, a\) and \(b\).

To do so, we let \(q_+\) and \(q_-\) be the two solutions of the quadratic equation \(X^2 - aX - b = 0\), namely

\[
q_+ = \frac{a + \sqrt{a^2 + 4b}}{2} \quad \text{and} \quad q_- = \frac{a - \sqrt{a^2 + 4b}}{2}.
\]

We notice that \(q_+ \neq q_-\) (since \(a^2 + 4b \neq 0\)). It is easy to see that the sequences \((1, q_+, q_+^2, q_+^3, \ldots)\) and \((1, q_-, q_-^2, q_-^3, \ldots)\) are \((a, b)\)-recurrent. As a consequence, for any two complex numbers \(\lambda_+\) and \(\lambda_-\), the sequence

\[
\left(\lambda_+ + \lambda_- q_+ + \lambda_- q_-, \lambda_+ q_+^2 + \lambda_- q_-^2, \ldots\right)
\]

(the \(n\)-th term of this sequence, with \(n\) starting at 0, is \(\lambda_+ q_+^n + \lambda_- q_-^n\)) must also be \((a, b)\)-recurrent (check this!). We denote this sequence by \(L_{\lambda_+, \lambda_-}\).

We now need to find two complex numbers \(\lambda_+\) and \(\lambda_-\) such that this sequence \(L_{\lambda_+, \lambda_-}\) is our sequence \((x_0, x_1, x_2, \ldots)\). In order to do so, we only need to ensure that \(\lambda_+ + \lambda_- = x_0\) and \(\lambda_+ q_+ + \lambda_- q_- = x_1\) (because once this holds, it will follow that the sequences \(L_{\lambda_+, \lambda_-}\) and \((x_0, x_1, x_2, \ldots)\) have the same first two terms; and this will yield that these two sequences are identical, because two \((a, b)\)-recurrent sequences with the same first two terms must be identical). That is, we need to solve the system of linear equations

\[
\begin{align*}
\lambda_+ + \lambda_- &= x_0; \\
\lambda_+ q_+ + \lambda_- q_- &= x_1
\end{align*}
\]

in the unknowns \(\lambda_+\) and \(\lambda_-\).

One of the well-known trigonometric identities states that \(\sin x + \sin y = 2 \sin \frac{x + y}{2} \cos \frac{x - y}{2}\) for any two angles \(x\) and \(y\). Applying this to \(x = \beta + na\) and \(y = \beta + (n - 2) a\), we obtain

\[
\sin (\beta + na) + \sin (\beta + (n - 2) a) = 2 \sin \left(\frac{\beta + na + \beta + (n - 2) a}{2}\right) \cos \left(\frac{\beta + na - (\beta + (n - 2) a)}{2}\right) = 2 \sin (\beta + (n - 1) a) \cos a = 2 \cos a \sin (\beta + (n - 1) a).
\]

Hence,

\[
\begin{align*}
\sin (\beta + na) &= 2 \cos a \sin (\beta + (n - 1) a) - \sin (\beta + (n - 2) a) \\
&= 2 \cos a \sin (\beta + (n - 1) a) + (-1) \sin (\beta + (n - 2) a),
\end{align*}
\]

qed.
Thanks to $q_+ \neq q_-$, this system has a unique solution:

$$\lambda_+ = \frac{x_1 - q_- x_0}{q_+ - q_-}, \quad \lambda_- = \frac{q_+ x_0 - x_1}{q_+ - q_-}.$$

Thus, if we set $(\lambda_+, \lambda_-)$ to be this solution, then $(x_0, x_1, x_2, \ldots) = L_{\lambda_+ \lambda_-}$, so that

$$x_n = \lambda_+ q_+^n + \lambda_- q_-^n$$

for every nonnegative integer $n$. This is an explicit formula, at least if the square roots do not disturb you. When $x_0 = x_1 = a = b = 1$, you get the famous Binet formula (86) for the Fibonacci sequence.

In the next exercise you will see what happens if the $a^2 + 4b \neq 0$ condition does not hold.

**Exercise 4.** Let $a$ and $b$ be complex numbers such that $a^2 + 4b = 0$. Consider an $(a, b)$-recurrent sequence $(x_0, x_1, x_2, \ldots)$. Find an explicit formula for each $x_n$ in terms of $x_0, x_1, a$ and $b$.

[Note: The polynomial $X^2 - aX - b$ has a double root here. Unlike the case of two distinct roots studied above, you won’t see any radicals here. The explicit formula really deserves the name “explicit”.]

Remark 4.3 and Exercise 4 combined, solve the problem of finding an explicit formula for any term of an $(a, b)$-recurrent sequence when $a$ and $b$ are complex numbers, at least if you don’t mind having square roots in your formula. Similar tactics can be used to find explicit forms for the more general case of sequences satisfying “homogeneous linear recurrences with constant coefficients”

although instead of square roots you will now need roots of higher-degree polynomials. (See [LeLeMe16, §22.3.2 (“Solving Homogeneous Linear Recurrences”)] for an outline of this; see also [Hefferon, Topic “Linear Recurrences”] for a linear-algebraic introduction.)

### 4.3. Further results

Here are some more exercises from the theory of recurrent sequences. I am not going particularly deep here, but we may encounter generalizations later.

First, an example: If we “split” the Fibonacci sequence

$$(f_0, f_1, f_2, \ldots) = (1, 1, 2, 3, 5, 8, \ldots)$$

These are sequences $(x_0, x_1, x_2, \ldots)$ which satisfy

$$(x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} \quad \text{for all } n \geq k)$$

for a fixed $k \in \mathbb{N}$ and a fixed $k$-tuple $(c_1, c_2, \ldots, c_k)$ of complex numbers. When $k = 2$, these are the $(c_1, c_2)$-recurrent sequences.
into two subsequences

\[(f_0, f_2, f_4, \ldots) = (1, 2, 5, 13, \ldots) \quad \text{and} \quad (f_1, f_3, f_5, \ldots) = (1, 3, 8, 21, \ldots)\]

(each of which contains every other Fibonacci number), then it turns out that each of these two subsequences is \((3, -1)\)-recurrent\(^{67}\). This is rather easy to prove, but one can always ask for generalizations: What happens if we start with an arbitrary \((a, b)\)-recurrent sequence, instead of the Fibonacci numbers? What happens if we split it into three, four or more subsequences? The answer is rather nice:

**Exercise 5.** Let \(a\) and \(b\) be complex numbers. Let \((x_0, x_1, x_2, \ldots)\) be an \((a, b)\)-recurrent sequence.

(a) Prove that the sequences \((x_0, x_2, x_4, \ldots)\) and \((x_1, x_3, x_5, \ldots)\) are \((c, d)\)-recurrent for some complex numbers \(c\) and \(d\). Find these \(c\) and \(d\).

(b) Prove that the sequences \((x_0, x_3, x_6, \ldots)\), \((x_1, x_4, x_7, \ldots)\) and \((x_2, x_5, x_8, \ldots)\) are \((c, d)\)-recurrent for some (other) complex numbers \(c\) and \(d\).

(c) For every nonnegative integers \(N\) and \(K\), prove that the sequence \((x_K, x_{N+K}, x_{2N+K}, x_{3N+K}, \ldots)\) is \((c, d)\)-recurrent for some complex numbers \(c\) and \(d\) which depend only on \(N\), \(a\) and \(b\) (but not on \(K\) or \(x_0\) or \(x_1\)).

The next exercise gives a combinatorial interpretation of the Fibonacci numbers:

**Exercise 6.** Recall that the Fibonacci numbers \(f_0, f_1, f_2, \ldots\) are defined recursively by \(f_0 = 0\), \(f_1 = 1\) and \(f_n = f_{n-1} + f_{n-2}\) for all \(n \geq 2\). For every positive integer \(n\), show that \(f_n\) is the number of subsets \(I\) of \(\{1, 2, \ldots, n-2\}\) such that no two elements of \(I\) are consecutive (i.e., there exists no \(i \in \mathbb{Z}\) such that both \(i\) and \(i+1\) belong to \(I\)). For instance, for \(n = 5\), these subsets are \(\emptyset\), \(\{1\}\), \(\{2\}\), \(\{3\}\) and \(\{1, 3\}\).

Notice that \(\{1, 2, \ldots, -1\}\) is to be understood as the empty set (since there are no integers \(x\) satisfying \(1 \leq x \leq -1\)). (So Exercise 6 applied to \(n = 1\), says that \(f_1\) is the number of subsets \(I\) of the empty set such that no two elements of \(I\) are consecutive. This is correct, because the empty set has only one subset, which of course is empty and thus has no consecutive elements; and the Fibonacci number \(f_1\) is precisely 1.)

**Remark 4.4.** Exercise 6 is equivalent to another known combinatorial interpretation of the Fibonacci numbers.

Namely, let \(n\) be a positive integer. Consider a rectangular table of dimensions \(2 \times (n-1)\) (that is, with 2 rows and \(n-1\) columns). How many ways are there to subdivide this table into dominos? (A domino means a set of two adjacent boxes.)

\(^{67}\)In other words, we have \(f_{2n} = 3f_{2(n-1)} + (-1)f_{2(n-2)}\) and \(f_{2n+1} = 3f_{2(n-1)+1} + (-1)f_{2(n-2)+1}\) for every \(n \geq 2\).
For $n = 5$, there are 5 ways:

In the general case, there are $f_{n-1}$ ways. Why?

As promised, this result is equivalent to Exercise 6. Let us see why. Let $P$ be a way to subdivide the table into dominos. We say that a horizontal domino is a domino which consists of two adjacent boxes in the same row; similarly, we define a vertical domino. It is easy to see that (in the subdivision $P$) each column of the table is covered either by a single vertical domino, or by two horizontal dominos (in which case either both of them “begin” in this column, or both of them “end” in this column). Let $J(P)$ be the set of all $i \in \{1, 2, \ldots, n - 1\}$ such that the $i$-th column of the table is covered by two horizontal dominos, both of which “begin” in this column. For instance,

$$J\left(\begin{array}{c|c}
\hline
\cdot & \cdot \\
\hline
\cdot & \cdot \\
\hline
\end{array}\right) = \{1, 3\};$$

$$J\left(\begin{array}{c|c|c}
\hline
\cdot & \cdot & \cdot \\
\hline
\cdot & \cdot & \cdot \\
\hline
\end{array}\right) = \{3\};$$

$$J\left(\begin{array}{c|c}
\hline
\cdot & \cdot \\
\hline
\cdot & \cdot \\
\hline
\end{array}\right) = \{1\};$$

$$J\left(\begin{array}{c|c|c|c}
\hline
\cdot & \cdot & \cdot & \cdot \\
\hline
\cdot & \cdot & \cdot & \cdot \\
\hline
\cdot & \cdot & \cdot & \cdot \\
\hline
\end{array}\right) = \{2\};$$

$$J\left(\begin{array}{c|c|c|c|c}
\hline
\cdot & \cdot & \cdot & \cdot & \cdot \\
\hline
\cdot & \cdot & \cdot & \cdot & \cdot \\
\hline
\end{array}\right) = \emptyset.$$

It is easy to see that the set $J(P)$ is a subset of $\{1, 2, \ldots, n - 2\}$ containing no two consecutive integers. Moreover, this set $J(P)$ uniquely determines $P$, and for every subset $I$ of $\{1, 2, \ldots, n - 2\}$ containing no two consecutive integers, there exists some way $P$ to subdivide the table into dominos such that $J(P) = I$.

Hence, the number of all ways to subdivide the table into dominos equals the number of all subsets $I$ of $\{1, 2, \ldots, n - 2\}$ containing no two consecutive integers. Exercise 6 says that this latter number is $f_{n-1}$; therefore, so is the former number.
(I have made this remark because I found it instructive. If you merely want a proof that the number of all ways to subdivide the table into dominoes equals \( f_n - 1 \), then I guess it is easier to just prove it by induction without taking the detour through Exercise 6. This proof is sketched in [GrKnPa §7.1], followed by an informal yet insightful discussion of “infinite sums of dominoes” and various related ideas.)

Either Exercise 6 or Remark 4.4 can be used to prove properties of Fibonacci numbers in a combinatorial way; see [BenQui04] for some examples of such proofs.

Here is another formula for certain recursive sequences, coming out of a recent paper on cluster algebras:

**Exercise 7.** Let \( r \in \mathbb{Z} \). Define a sequence \((c_0, c_1, c_2, \ldots)\) of integers recursively by \( c_0 = 0, c_1 = 1 \) and \( c_n = rc_{n-1} - c_{n-2} \) for all \( n \geq 2 \). Show that

\[
    c_n = \sum_{i=0}^{n-1} (-1)^i \binom{n-1-i}{i} r^{n-1-2i}
\]

for every \( n \in \mathbb{N} \). Here, we use the following convention: Any expression of the form \( a \cdot b \), where \( a \) is 0, has to be interpreted as 0, even if \( b \) is undefined.

### 4.4. Additional exercises

This section contains some further exercises. As the earlier “additional exercises”, these will not be relied on in the rest of this text, and solutions will not be provided.

**Additional exercise 8.** Let \( q \) and \( r \) be two complex numbers. Prove that the sequence \((q^0 - r^0, q^1 - r^1, q^2 - r^2, \ldots)\) is \((a, b)\)-recurrent for two appropriately chosen \( a \) and \( b \). Find these \( a \) and \( b \).

**Additional exercise 9.** Let \( \varphi \) be the golden ratio (i.e., the real number \( \frac{1 + \sqrt{5}}{2} \)). Let \((f_0, f_1, f_2, \ldots)\) be the Fibonacci sequence.

(a) Show that \( f_{n+1} - \varphi f_n = \frac{1}{\sqrt{5}} \varphi^n \) for every \( n \in \mathbb{N} \), where \( \varphi = \frac{1 - \sqrt{5}}{2} \).

(Notice that \( \varphi = \frac{1 - \sqrt{5}}{2} \approx -0.618 \) lies between \(-1\) and 0, and thus the powers

---

\[ ^{68} \text{Specifically, Exercise 7 is part of [LeeSchl] Definition 1], but I have reindexed the sequence and fixed the missing upper bound in the sum.} \]

\[ ^{69} \text{The purpose of this convention is to make sure that the right hand side of (89) is well-defined, even though the expression } r^{n-1-2i} \text{ that appears in it might be undefined (it will be undefined when } r = 0 \text{ and } n - 1 - 2i < 0).} \]

Of course, the downside of this convention is that we might not have \( a \cdot b = b \cdot a \) (because \( a \cdot b \) might be well-defined while \( b \cdot a \) is not, or vice versa).
ψ^n converge to 0 as n → ∞. So \( \frac{f_{n+1} - \phi f_n}{f_n} \to \phi \) as well.

(b) Show that

\[
\mathcal{f}_n = \text{round}\left( \frac{1}{\sqrt{5}} \phi^n \right) \quad \text{for every } n \in \mathbb{N}.
\]

Here, if x is a real number, then round x denotes the integer closest to x (where, in case of a tie, we take the higher of the two candidates).70

**Additional exercise 10.** Let \((f_0, f_1, f_2, \ldots)\) be the Fibonacci sequence. A set \(I\) of integers is said to be *lacunar* if no two elements of \(I\) are consecutive (i.e., there exists no \(i \in I\) such that \(i + 1 \in I\)). Show that, for every \(n \in \mathbb{N}\), there exists a unique lacunar subset \(S\) of \(\{2, 3, 4, \ldots\}\) such that \(n = \sum_{s \in S} f_s\).

(For example, if \(n = 17\), then \(S = \{2, 4, 7\}\), because \(17 = 1 + 3 + 13 = f_2 + f_4 + f_7\).)

**Remark 4.5.** The representation of \(n\) in the form \(n = \sum_{s \in S} f_s\) in Exercise 10 is known as the **Zeckendorf representation** of \(n\). It has a number of interesting properties and trivia related to it; for example, there is a rule of thumb for converting miles into kilometers that uses it. It can also be used to define a curious "Fibonacci multiplication" operation on nonnegative integers [Knuth88].

**Additional exercise 11.** Let \((f_0, f_1, f_2, \ldots)\) be the Fibonacci sequence.

(a) Prove the identities

\[
\begin{align*}
1f_n &= f_n \quad \text{for all } n \geq 0; \\
2f_n &= f_{n-2} + f_{n+1} \quad \text{for all } n \geq 2; \\
3f_n &= f_{n-2} + f_{n+2} \quad \text{for all } n \geq 2; \\
4f_n &= f_{n-2} + f_n + f_{n+2} \quad \text{for all } n \geq 2.
\end{align*}
\]

(b) Notice that the right hand sides of these identities have a specific form: they are sums of \(f_{n+t}\) for \(t\) ranging over a lacunar subset of \(\mathbb{Z}\). (See Additional exercise 10 for the definition of "lacunar"). Try to find similar identities for \(5f_n\) and \(6f_n\).

(c) Prove that such identities exist in general. More precisely, prove the following: Let \(T\) be a finite set, and \(a_t\) be an integer for every \(t \in T\). Then, there exists

70This does not really matter in our situation, because \(\frac{1}{\sqrt{5}} \phi^n\) will never be a half-integer.
a unique lacunar subset $S$ of $\mathbb{Z}$ such that
\[
\sum_{t \in T} f_{n+a_t} = \sum_{s \in S} f_{n+s} \quad \text{for every } n \in \mathbb{Z} \text{ which satisfies } n \geq \max \left( \{-a_t \mid t \in T\} \cup \{-s \mid s \in S\} \right).
\]
(The condition $n \geq \max \left( \{-a_t \mid t \in T\} \cup \{-s \mid s \in S\} \right)$ merely ensures that all the $f_{n+a_t}$ and $f_{n+s}$ are well-defined.)

Remark 4.6. Additional exercise \[\text{(c)}\] is \[\text{[Gri11, Theorem 1]}\]. I’d be delighted to see other proofs!

Similarly I am highly interested in analogues of Additional exercises \[\text{[10] and 11} \] for other $(a,b)$-recurrent sequences (e.g., Lucas numbers).

Additional exercise 12. (a) Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. Prove that $f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$ for any positive integer $m$ and any $n \in \mathbb{N}$.

(b) Generalize to $(a, b)$-recurrent sequences with arbitrary $a$ and $b$.

(c) Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. Prove that $f_m \mid f_{mk}$ for any $m \in \mathbb{N}$ and $k \in \mathbb{N}$.

Additional exercise 13. (a) Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. For every $n \in \mathbb{N}$ and $k \in \mathbb{N}$ satisfying $0 \leq k \leq n$, define a rational number \( \left( \begin{array}{c} n \\ k \end{array} \right)_F \) by
\[
\left( \begin{array}{c} n \\ k \end{array} \right)_F = \frac{f_n f_{n-1} \cdots f_{n-k+1}}{f_k f_{k-1} \cdots f_1}.
\]
This is called the $(n,k)$-th Fibonomial coefficient (in analogy to the binomial coefficient \( \left( \begin{array}{c} n \\ k \end{array} \right) = \frac{n (n-1) \cdots (n-k+1)}{k (k-1) \cdots 1} \)).

Show that \( \left( \begin{array}{c} n \\ k \end{array} \right)_F \) is an integer.

(b) Try to extend as many identities for binomial coefficients as you can to Fibonomial coefficients.

(c) Generalize to $(a,b)$-recurrent sequences with arbitrary $a$ and $b$.

5. Permutations

This chapter is devoted to permutations. We first recall how they are defined.

5.1. Permutations and the symmetric group
Definition 5.1. First, let us stipulate, once and for all, how we define the composition of two maps: If \( X, Y \) and \( Z \) are three sets, and if \( \alpha : X \to Y \) and \( \beta : Y \to Z \) are two maps, then \( \beta \circ \alpha \) denotes the map from \( X \) to \( Z \) which sends every \( x \in X \) to \( \beta(\alpha(x)) \). This map \( \beta \circ \alpha \) is called the composition of \( \beta \) and \( \alpha \) (and is sometimes abbreviated as \( \beta \alpha \)). This is the classical notation for composition of maps, and the reason why I am so explicitly reminding you of it is that some people (e.g., Herstein in [Herstein]) use a different convention that conflicts with it: They write maps “on the right” (i.e., they denote the image of an element \( x \in X \) under the map \( \alpha : X \to Y \) by \( x^\alpha \) or \( x \alpha \) instead of \( \alpha(x) \)), and they define composition “the other way round” (i.e., they write \( \alpha \circ \beta \) for what we call \( \beta \circ \alpha \)). They have reasons for what they are doing, but I shall use the classical notation because most of the literature agrees with it.

Definition 5.2. Let us also recall what it means for two maps to be inverse.

Let \( X \) and \( Y \) be two sets. Two maps \( f : X \to Y \) and \( g : Y \to X \) are said to be mutually inverse if they satisfy \( g \circ f = \text{id}_X \) and \( f \circ g = \text{id}_Y \). (In other words, two maps \( f : X \to Y \) and \( g : Y \to X \) are mutually inverse if and only if every \( x \in X \) satisfies \( g(f(x)) = x \) and every \( y \in Y \) satisfies \( f(g(y)) = y \).)

Let \( f : X \to Y \) is a map. If there exists a map \( g : Y \to X \) such that \( f \) and \( g \) are mutually inverse, then this map \( g \) is unique (this is easy to check) and is called the inverse of \( f \) and denoted by \( f^{-1} \). In this case, the map \( f \) is said to be invertible. It is easy to see that if \( g \) is the inverse of \( f \), then \( f \) is the inverse of \( g \).

It is well-known that a map \( f : X \to Y \) is invertible if and only if \( f \) is bijective (i.e., both injective and surjective). The words “invertible” and “bijective” are thus synonyms (at least when used for a map between two sets – in other situations, they can be rather different). Nevertheless, both of them are commonly used, often by the same authors (since they convey slightly different mental images).

A bijective map is also called a bijection or a 1-to-1 correspondence (or a one-to-one correspondence). When there is a bijection from \( X \) to \( Y \), one says that the elements of \( X \) are in bijection with (or in one-to-one correspondence with) the elements of \( Y \). It is well-known that two sets \( X \) and \( Y \) have the same cardinality if and only if there exists a bijection from \( X \) to \( Y \).

Definition 5.3. A permutation of a set \( X \) means a bijection from \( X \) to \( X \). The permutations of a given set \( X \) can be composed (i.e., if \( \alpha \) and \( \beta \) are two permutations of \( X \), then so is \( \alpha \circ \beta \)) and have inverses (which, again, are permutations of \( X \)). More precisely:

- If \( \alpha \) and \( \beta \) are two permutations of a given set \( X \), then the composition \( \alpha \circ \beta \) is again a permutation of \( X \).
- Any three permutations \( \alpha, \beta \) and \( \gamma \) of \( X \) satisfy \( (\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma) \).

(This holds, more generally, for arbitrary maps which can be composed.)
• The identity map \(id : X \to X\) (this is the map which sends every element \(x \in X\) to itself) is a permutation of \(X\); it is also called the identity permutation. Every permutation \(\alpha\) of \(X\) satisfies \(id \circ \alpha = \alpha\) and \(\alpha \circ id = \alpha\). (Again, this can be generalized to arbitrary maps.)

• For every permutation \(\alpha\) of \(X\), the inverse map \(\alpha^{-1}\) is well-defined and is again a permutation of \(X\). We have \(\alpha \circ \alpha^{-1} = id\) and \(\alpha^{-1} \circ \alpha = id\).

In the lingo of algebraists, these four properties show that the set of all permutations of \(X\) is a [group](https://en.wikipedia.org/wiki/Group_(mathematics)) whose binary operation is composition, and whose neutral element is the identity permutation \(id : X \to X\). This group is known as the symmetric group of the set \(X\). (We will define the notion of a group later, in Definition 6.97; thus you might not understand the preceding two sentences at this point. If you do not care about groups, you should just remember that the symmetric group of \(X\) is the set of all permutations of \(X\).)

**Remark 5.4.** Some authors define a permutation of a finite set \(X\) to mean a list of all elements of \(X\), each occurring exactly once. This is not the meaning that the word “permutation” has in these notes! It is a different notion which, for historical reasons, has been called “permutation” as well. On the Wikipedia page for “permutation”, the two notions are called “active” and “passive”, respectively: An “active” permutation of \(X\) means a bijection from \(X\) to \(X\) (that is, a permutation of \(X\) in our meaning of this word), whereas a “passive” permutation of \(X\) means a list of all elements of \(X\), each occurring exactly once. For example, if \(X = \{\text{“cat”}, \text{“dog”}, \text{“archaeopteryx”}\}\), then the map

\[
\begin{align*}
\text{“cat”} \mapsto \text{“archaeopteryx”}, \\
\text{“archaeopteryx”} \mapsto \text{“dog”}, \\
\text{“dog”} \mapsto \text{“cat”}
\end{align*}
\]

is an “active” permutation of \(X\), whereas the list (\(\text{“dog”, “cat”, “archaeopteryx”}\)) is a “passive” permutation of \(X\).

When \(X\) is the set \(\{1, 2, \ldots, n\}\) for some \(n \in \mathbb{N}\), then it is possible to equate each “active” permutation of \(X\) with a “passive” permutation of \(X\) (namely, its one-line notation, defined below). More generally, this can be done when \(X\) comes with a fixed total order. In general, if \(X\) is a finite set, then the number of “active” permutations of \(X\) equals the number of “passive” permutations of \(X\) (and both numbers equal \(|X|!\)), but until you fix some ordering of the elements of \(X\), there is no “natural” way to match the “passive” permutations with the “active” ones. (And when \(X\) is infinite, the notion of a “passive” permutation is not even well-defined.)

To reiterate: For us, the word “permutation” shall always mean an “active” permutation!

Recall that \(\mathbb{N} = \{0, 1, 2, \ldots\}\). Fix \(n \in \mathbb{N}\).
Let $S_n$ be the symmetric group of the set $\{1,2,\ldots,n\}$. This is the set of all permutations of the set $\{1,2,\ldots,n\}$. It contains the identity permutation $\text{id} \in S_n$ which sends every $i \in \{1,2,\ldots,n\}$ to $i$. A well-known fact states that the size of this group is $|S_n| = n!$ (that is, there are exactly $n!$ permutations of $\{1,2,\ldots,n\}$).

We will often write a permutation $\sigma \in S_n$ as the list $(\sigma(1),\sigma(2),\ldots,\sigma(n))$ of its values. This is known as the one-line notation for permutations (because it is a single-rowed list, as opposed to e.g. the two-line notation which is a two-rowed table). For instance, the permutation in $S_3$ which sends 1 to 2, 2 to 1 and 3 to 3 is written (2,1,3) in one-line notation.

The exact relation between lists and permutations is given by the following simple fact:

**Proposition 5.5.** Let $n \in \mathbb{N}$. Let $[n] = \{1,2,\ldots,n\}$.

(a) If $\sigma \in S_n$, then each element of $[n]$ appears exactly once in the list $(\sigma(1),\sigma(2),\ldots,\sigma(n))$.

(b) If $(p_1,p_2,\ldots,p_n)$ is a list of elements of $[n]$ such that each element of $[n]$ appears exactly once in this list $(p_1,p_2,\ldots,p_n)$, then there exists a unique permutation $\sigma \in S_n$ such that $(p_1,p_2,\ldots,p_n) = (\sigma(1),\sigma(2),\ldots,\sigma(n))$.

(c) Let $k \in \{0,1,\ldots,n\}$. If $(p_1,p_2,\ldots,p_k)$ is a list of some elements of $[n]$ such that $p_1,p_2,\ldots,p_k$ are distinct, then there exists a permutation $\sigma \in S_n$ such that $(p_1,p_2,\ldots,p_k) = (\sigma(1),\sigma(2),\ldots,\sigma(k))$.

At this point, let us clarify what we mean by “distinct”: Several objects $u_1,u_2,\ldots,u_k$ are said to be distinct if every $i \in \{1,2,\ldots,k\}$ and $j \in \{1,2,\ldots,k\}$ satisfying $i \neq j$ satisfy $u_i \neq u_j$. (Some people call this “pairwise distinct”.) So, for example, the numbers 2,1,6 are distinct, but the numbers 6,1,6 are not (although 6 and 1 are distinct). Instead of saying that some objects $u_1,u_2,\ldots,u_k$ are distinct, we can also say that “the list $(u_1,u_2,\ldots,u_k)$ has no repetitions.”

**Remark 5.6.** The $\sigma$ in Proposition 5.5 (b) is uniquely determined, but the $\sigma$ in Proposition 5.5 (c) is not (in general). More precisely, in Proposition 5.5 (c), there are $(n-k)!$ possible choices of $\sigma$ that work. (This is easy to check.)

**Proof of Proposition 5.5** Proposition 5.5 is a really basic fact and its proof is simple. I am going to present the proof at high detail in order to make sure you correctly understand every notion involved in it; if you find it obvious, you are (probably) getting it right and you don’t need to read my boring proof.

Recall that $S_n$ is the set of all permutations of the set $\{1,2,\ldots,n\}$. In other words, $S_n$ is the set of all permutations of the set $[n]$ (since $\{1,2,\ldots,n\} = [n]$).

---

71 Combinatorialists often omit the parentheses and the commas (i.e., they just write $\sigma(1) \sigma(2) \cdots \sigma(n)$, hoping that no one will mistake this for a product), since there is unfortunately another notation for permutations (the cycle notation) which also writes them as lists (actually, lists of lists) but where the lists have a different meaning.

72 A repetition just means an element which occurs more than once in the list. It does not matter whether the occurrences are at consecutive positions or not.
(a) Let $\sigma \in S_n$. Let $i \in [n]$. We have $\sigma \in S_n$. In other words, $\sigma$ is a permutation of $[n]$ (since $S_n$ is the set of all permutations of the set $[n]$). In other words, $\sigma$ is a bijective map $[n] \to [n]$. Hence, $\sigma$ is both surjective and injective.

Now, we make the following two observations:

- The number $i$ appears in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.
- The number $i$ appears at most once in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.

Combining these two observations, we conclude that the number $i$ appears exactly once in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.

Let us now forget that we fixed $i$. We thus have shown that if $i \in [n]$, then $i$ appears exactly once in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. In other words, each element of $[n]$ appears exactly once in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. This proves Proposition 5.5 (a).

(b) Let $(p_1, p_2, \ldots, p_n)$ be a list of elements of $[n]$ such that each element of $[n]$ appears exactly once in this list $(p_1, p_2, \ldots, p_n)$.

We have $p_i \in [n]$ for every $i \in [n]$ (since $(p_1, p_2, \ldots, p_n)$ is a list of elements of $[n]$).

We define a map $\tau : [n] \to [n]$ by setting

$$(\tau(i) = p_i \text{ for every } i \in [n]).$$

(90)

(This is well-defined, because we have $p_i \in [n]$ for every $i \in [n]$.) The map $\tau$ is injective and surjective. Hence, the map $\tau$ is bijective. In other words, $\tau$ is a

---

73Proof. The map $\sigma$ is surjective. Hence, there exists some $j \in [n]$ such that $i = \sigma(j)$. In other words, the number $i$ appears in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Qed.

74Proof. Let us assume the contrary (for the sake of contradiction). Thus, $i$ appears more than once in the list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. In other words, $i$ appears at least twice in this list. In other words, there exist two distinct elements $p$ and $q$ of $[n]$ such that $\sigma(p) = i$ and $\sigma(q) = i$. Consider these $p$ and $q$.

We have $p \neq q$ (since $p$ and $q$ are distinct), so that $\sigma(p) \neq \sigma(q)$ (since $\sigma$ is injective). This contradicts $\sigma(p) = i = \sigma(q)$. This contradiction proves that our assumption was wrong, qed.

75Proof. Let $u$ and $v$ be two elements of $[n]$ such that $\tau(u) = \tau(v)$. We shall show that $u = v$.

Indeed, we assume the contrary (for the sake of contradiction). Thus, $u \neq v$.

The definition of $\tau(u)$ shows that $\tau(u) = p_u$. But we also have $\tau(u) = \tau(v) = p_v$ (by the definition of $\tau(v)$). Now, the element $\tau(u)$ of $[n]$ appears (at least) twice in the list $(p_1, p_2, \ldots, p_n)$: once at the $u$-th position (since $\tau(u) = p_u$), and again at the $v$-th position (since $\tau(u) = p_v$). (And these are two distinct positions, because $u \neq v$.)

But let us recall that each element of $[n]$ appears exactly once in this list $(p_1, p_2, \ldots, p_n)$. Hence, no element of $[n]$ appears more than once in the list $(p_1, p_2, \ldots, p_n)$. In particular, $\tau(u)$ cannot appear more than once in this list $(p_1, p_2, \ldots, p_n)$. This contradicts the fact that $\tau(u)$ appears twice in the list $(p_1, p_2, \ldots, p_n)$.

This contradiction shows that our assumption was wrong. Hence, $u = v$ is proven.

Now, let us forget that we fixed $u$ and $v$. We thus have proven that if $u$ and $v$ are two elements of $[n]$ such that $\tau(u) = \tau(v)$, then $u = v$. In other words, the map $\tau$ is injective. Qed.

76Proof. Let $u \in [n]$. Each element of $[n]$ appears exactly once in the list $(p_1, p_2, \ldots, p_n)$. Applying
permutation of \([n]\) (since \(\tau\) is a map \([n] \rightarrow [n]\)). In other words, \(\tau \in S_n\) (since \(S_n\) is the set of all permutations of the set \([n]\)). Clearly, \((\tau(1), \tau(2), \ldots, \tau(n)) = (p_1, p_2, \ldots, p_n)\) (because of \((90)\)), so that \((p_1, p_2, \ldots, p_n) = (\tau(1), \tau(2), \ldots, \tau(n))\).

Hence, there exists a permutation \(\sigma \in S_n\) such that

\[
(p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n))
\]

(namely, \(\sigma = \tau\)). Moreover, there exists at most one such permutation\(^{77}\). Combining the claims of the previous two sentences, we conclude that there exists a unique permutation \(\sigma \in S_n\) such that

\[
(p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n))
\]

This proves Proposition 5.5 (b).

(c) Let \((p_1, p_2, \ldots, p_k)\) be a list of some elements of \([n]\) such that \(p_1, p_2, \ldots, p_k\) are distinct. Thus, the list \((p_1, p_2, \ldots, p_k)\) contains \(k\) of the \(n\) elements of \([n]\) (because \(p_1, p_2, \ldots, p_k\) are distinct). Let \(q_1, q_2, \ldots, q_{n-k}\) be the remaining \(n-k\) elements of \([n]\) (listed in any arbitrary order, with no repetition). Then, \((p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k})\) is a list of all \(n\) elements of \([n]\), with no repetitions\(^{78}\). In other words, each element of \([n]\) appears exactly once in this list \((p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k})\) (and each entry in this list is an element of \([n]\)). Hence, we can apply Proposition 5.5 (b) to \((p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k})\) instead of \((p_1, p_2, \ldots, p_n)\). As a consequence, we conclude that there exists a unique permutation \(\sigma \in S_n\) such that

\[
(p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k}) = (\sigma(1), \sigma(2), \ldots, \sigma(n))
\]

Let \(\tau\) be this \(\sigma\).

Thus, \(\tau \in S_n\) is a permutation such that

\[
(p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k}) = (\tau(1), \tau(2), \ldots, \tau(n)).
\]

\(^{77}\text{Proof.}\) Let \(\sigma_1\) and \(\sigma_2\) be two permutations \(\sigma \in S_n\) such that \((p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n))\). Thus, \(\sigma_1\) is a permutation in \(S_n\) such that \((p_1, p_2, \ldots, p_n) = (\sigma_1(1), \sigma_1(2), \ldots, \sigma_1(n))\), and \(\sigma_2\) is a permutation in \(S_n\) such that \((p_1, p_2, \ldots, p_n) = (\sigma_2(1), \sigma_2(2), \ldots, \sigma_2(n))\).

We have \((\sigma_1(1), \sigma_1(2), \ldots, \sigma_1(n)) = (p_1, p_2, \ldots, p_n) = (\sigma_2(1), \sigma_2(2), \ldots, \sigma_2(n))\). In other words, every \(i \in [n]\) satisfies \(\sigma_1(i) = \sigma_2(i)\). In other words, \(\sigma_1 = \sigma_2\).

Let us now forget that we fixed \(\sigma_1\) and \(\sigma_2\). We thus have shown that if \(\sigma_1\) and \(\sigma_2\) are two permutations \(\sigma \in S_n\) such that \((p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n))\), then \(\sigma_1 = \sigma_2\). In other words, any two permutations \(\sigma \in S_n\) such that \((p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n))\) must be equal to each other. In other words, there exists at most one permutation \(\sigma \in S_n\) such that

\[
(p_1, p_2, \ldots, p_n) = (\sigma(1), \sigma(2), \ldots, \sigma(n)).
\]

\(^{78}\text{It has no repetitions because:}\)

- there are no repetitions among \(p_1, p_2, \ldots, p_k\);
- there are no repetitions among \(q_1, q_2, \ldots, q_{n-k}\);
- the two lists \((p_1, p_2, \ldots, p_k)\) and \((q_1, q_2, \ldots, q_{n-k})\) have no elements in common (because we defined \(q_1, q_2, \ldots, q_{n-k}\) to be the “remaining” \(n-k\) elements of \([n]\), where “remaining” means “not contained in the list \((p_1, p_2, \ldots, p_k)\)”.)
Now,
\[
(p_1, p_2, \ldots, p_k)
\]
\[
= \left( \begin{array}{c}
\text{the list of the first } k \text{ entries of the list } (p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_{n-k}) \\
= (\tau(1), \tau(2), \ldots, \tau(n)) \end{array} \right)
\]
\[
= (\tau(1), \tau(2), \ldots, \tau(k)).
\]

Hence, there exists a permutation \( \sigma \in S_n \) such that
\[
(p_1, p_2, \ldots, p_k) = (\sigma(1), \sigma(2), \ldots, \sigma(k)) \] (namely, \( \sigma = \tau \)). This proves Proposition 5.5 (c).

5.2. Inversions, lengths and the permutations \( s_i \in S_n \)

For each \( i \in \{1, 2, \ldots, n-1\} \), let \( s_i \) be the permutation in \( S_n \) that switches \( i \) with \( i+1 \) but leaves all other numbers unchanged. Formally speaking, \( s_i \) is the permutation in \( S_n \) given by
\[
\left( s_i(k) = \begin{cases}
  i+1, & \text{if } k = i; \\
  i, & \text{if } k = i+1; \\
  k, & \text{if } k \notin \{i, i+1\}
\end{cases} \right. 
\]

Thus, in one-line notation
\[
s_i = (1, 2, \ldots, i-1, i+1, i, i+2, \ldots, n). 
\]

Notice that \( s_i^2 = \text{id} \) for every \( i \in \{1, 2, \ldots, n-1\} \). (Here, we are using the notation \( a^2 \) for \( a \circ a \), where \( a \) is a permutation in \( S_n \).)

**Exercise 8.** (a) Show that \( s_i \circ s_{i+1} \circ s_i = s_{i+1} \circ s_i \circ s_{i+1} \) for all \( i \in \{1, 2, \ldots, n-2\} \).

(b) Show that every permutation \( \sigma \in S_n \) can be written as a composition of several permutations of the form \( s_k \) (with \( k \in \{1, 2, \ldots, n-1\} \)). For example, if \( n = 3 \), then the permutation \( (3,1,2) \) in \( S_3 \) can be written as the composition \( s_2 \circ s_1 \), while the permutation \( (3,2,1) \) in \( S_3 \) can be written as the composition \( s_1 \circ s_2 \circ s_1 \) or also as the composition \( s_2 \circ s_1 \circ s_2 \).

[Hint: If you do not immediately see why this works, consider reading further.]

(c) Let \( w_0 \) denote the permutation in \( S_n \) which sends each \( k \in \{1, 2, \ldots, n\} \) to \( n+1-k \). (In one-line notation, this \( w_0 \) is written as \( (n, n-1, \ldots, 1) \).) Find an explicit way to write \( w_0 \) as a composition of several permutations of the form \( s_i \) (with \( i \in \{1, 2, \ldots, n-1\} \)).
Remark 5.7. Symmetric groups appear in almost all parts of mathematics; unsurprisingly, there is no universally accepted notation for them. We are using the notation $S_n$ for the $n$-th symmetric group; other common notations for it are $S_n$, $\Sigma_n$ and $\text{Sym}(n)$. The permutations that we call $s_1, s_2, \ldots, s_{n-1}$ are often called $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$. As already mentioned in Definition 5.1, some people write the composition of maps “backwards”, which causes their $\sigma \circ \tau$ to be our $\tau \circ \sigma$, etc. (Sadly, most authors are so sure that their notation is standard that they never bother to define it.)

In the language of group theory, the statement of Exercise 8 (b) says (or, more precisely, yields) that the permutations $s_1, s_2, \ldots, s_{n-1}$ generate the group $S_n$.

Definition 5.8. If $\sigma \in S_n$ is a permutation, then an inversion of $\sigma$ means a pair $(i, j)$ of integers satisfying $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. For instance, the inversions of the permutation $(3,1,2)$ in $S_3$ are $(1,2)$ and $(1,3)$ (because $3 > 1$ and $3 > 2$), while the only inversion of the permutation $(1,3,2)$ in $S_3$ is $(2,3)$ (since $3 > 2$).

If $\sigma \in S_n$ is a permutation, then the length of $\sigma$ means the number of inversions of $\sigma$. This length is denoted by $\ell(\sigma)$; it is a nonnegative integer.

Any $\sigma \in S_n$ satisfies $0 \leq \ell(\sigma) \leq \binom{n}{2}$ (since the number of inversions of $\sigma$ is clearly no larger than the total number of pairs $(i, j)$ of integers satisfying $1 \leq i < j \leq n$; but the latter number is $\binom{n}{2}$). The only permutation in $S_n$ having length 0 is the identity permutation $\text{id} = (1,2,\ldots,n) \in S_n$.

Exercise 9. (a) Show that every permutation $\sigma \in S_n$ and every $k \in \{1,2,\ldots,n-1\}$ satisfy

$$\ell(\sigma \circ s_k) = \begin{cases} \ell(\sigma) + 1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma) - 1, & \text{if } \sigma(k) > \sigma(k+1) \end{cases} \quad (91)$$

and

$$\ell(s_k \circ \sigma) = \begin{cases} \ell(\sigma) + 1, & \text{if } \sigma^{-1}(k) < \sigma^{-1}(k+1); \\ \ell(\sigma) - 1, & \text{if } \sigma^{-1}(k) > \sigma^{-1}(k+1) \end{cases}. \quad (92)$$

(b) Show that any two permutations $\sigma$ and $\tau$ in $S_n$ satisfy $\ell(\sigma \circ \tau) \equiv \ell(\sigma) + \ell(\tau) \mod 2$.

(c) Show that any two permutations $\sigma$ and $\tau$ in $S_n$ satisfy $\ell(\sigma \circ \tau) \leq \ell(\sigma) + \ell(\tau)$.

(d) If $\sigma \in S_n$ is a permutation satisfying $\sigma(1) \leq \sigma(2) \leq \cdots \leq \sigma(n)$, then show that $\sigma = \text{id}$.

*The fact that the identity permutation $\text{id} \in S_n$ has length $\ell(\text{id}) = 0$ is trivial. The fact that it is the only one such permutation is easy (it essentially follows from Exercise 9 (d)).*
(e) Let \( \sigma \in S_n \). Show that \( \sigma \) can be written as a composition of \( \ell (\sigma) \) permutations of the form \( s_k \) (with \( k \in \{1, 2, \ldots, n-1\} \)).

(f) Let \( \sigma \in S_n \). Then, show that \( \ell (\sigma) = \ell (\sigma^{-1}) \).

(g) Let \( \sigma \in S_n \). Show that \( \ell (\sigma) \) is the smallest \( N \in \mathbb{N} \) such that \( \sigma \) can be written as a composition of \( N \) permutations of the form \( s_k \) (with \( k \in \{1, 2, \ldots, n-1\} \)).

**Example 5.9.** Let us justify Exercise 5(a) on an example. The solution to Exercise 5(a) given below is essentially a (tedious) formalization of the ideas seen in this example.

Let \( n = 5, k = 3 \) and \( \sigma = (4, 2, 1, 5, 3) \) (written in one-line notation). Then, \( \sigma \circ s_k = (4, 2, 5, 1, 3) \); this is the permutation obtained by switching the \( k \)-th and the \( (k+1) \)-th entry of \( \sigma \) (where the word “entry” refers to the one-line notation).

On the other hand, \( s_k \circ \sigma = (3, 2, 1, 5, 4) \); this is the permutation obtained by switching the entry \( k \) with the entry \( k+1 \) of \( \sigma \). Mind the difference between these two operations.

The inversions of \( \sigma = (4, 2, 1, 5, 3) \) are \( (1, 2), (1, 3), (1, 5), (2, 3) \) and \( (4, 5) \). These are the pairs \( (i, j) \) of positions such that \( i \) is before \( j \) (that is, \( i < j \)) but the \( i \)-th entry of \( \sigma \) is larger than the \( j \)-th entry of \( \sigma \) (that is, \( \sigma (i) > \sigma (j) \)). In other words, these are the pairs of positions at which the entries of \( \sigma \) are out of order. On the other hand, the inversions of \( s_k \circ \sigma = (3, 2, 1, 5, 4) \) are \( (1, 2), (1, 3), (2, 3) \) and \( (4, 5) \). These are precisely the inversions of \( \sigma \) except for \( (1, 5) \). This is no surprise: In fact, \( s_k \circ \sigma \) is obtained from \( \sigma \) by switching the entry \( k \) with the entry \( k+1 \) of \( \sigma \), and this operation clearly preserves all inversions other than the one that is directly being turned around (i.e., the inversion \( (i, j) \) where \( \{\sigma (i), \sigma (j)\} = \{k, k+1\} \); in our case, this is the inversion \( (1, 5) \)). In general, when \( \sigma^{-1} (k) > \sigma^{-1} (k+1) \) (that is, when \( k \) appears further left than \( k+1 \) in the one-line notation of \( \sigma \)), the inversions of \( s_k \circ \sigma \) are the inversions of \( \sigma \) except for \( (\sigma^{-1} (k+1), \sigma^{-1} (k)) \). Therefore, in this case, the number of inversions of \( s_k \circ \sigma \) equals the number of inversions of \( \sigma \) plus \( 1 \). That is, in this case, \( \ell (s_k \circ \sigma) = \ell (\sigma) + 1 \). When \( \sigma^{-1} (k) < \sigma^{-1} (k+1) \), a similar argument shows \( \ell (s_k \circ \sigma) = \ell (\sigma) - 1 \). This explains why 92 holds (although formalizing this argument will be tedious).

The inversions of \( \sigma \circ s_k = (4, 2, 5, 1, 3) \) are \( (1, 2), (1, 4), (1, 5), (2, 4), (3, 4) \) and \( (3, 5) \). Unlike the inversions of \( s_k \circ \sigma \), these are not directly related to the inversions of \( \sigma \), so the argument in the previous paragraph does not prove 91. However, instead of considering inversions of \( \sigma \), one can consider inversions of \( \sigma^{-1} \). These are even more intuitive: They are the pairs of integers \( (i, j) \) with \( 1 \leq i < j \leq n \) such that \( i \) appears further right than \( j \) in the one-line notation of \( \sigma \). For instance, the inversions of \( \sigma^{-1} \) are \( (1, 2), (1, 4), (2, 4), (3, 4) \) and \( (3, 5) \), whereas the inversions of \( (\sigma \circ s_k)^{-1} \) are all of these and also \( (1, 5) \). But there is no need to repeat our proof of 92; it is easier to deduce 91 from 92 by applying 92 to \( \sigma^{-1} \) instead of \( \sigma \) and appealing to Exercise 5(f). (Again, see the solution below for the details.)
Notice that Exercise 9(e) immediately yields Exercise 8(b).

**Remark 5.10.** When \( n = 0 \) or \( n = 1 \), we have \( \{1,2,\ldots,n-1\} = \emptyset \). Hence, Exercise 8(e) looks strange in the case when \( n = 0 \) or \( n = 1 \), because in this case, there are no permutations of the form \( s_k \) to begin with. Nevertheless, it is correct. Indeed, when \( n = 0 \) or \( n = 1 \), there is only one permutation \( \sigma \in S_n \), namely the identity permutation \( \text{id} \), and it has length \( \ell(\sigma) = \ell(\text{id}) = 0 \). Thus, in this case, Exercise 8(e) claims that \( \text{id} \) can be written as a composition of 0 permutations of the form \( s_k \) (with \( k \in \{1,2,\ldots,n-1\} \)). This is true: Even from an empty set we can always pick 0 elements; and the composition of 0 permutations will be \( \text{id} \).

**Remark 5.11.** The term “length” for \( \ell(\sigma) \) can be confusing: It does not refer to the length of the \( n \)-tuple \( (\sigma(1),\sigma(2),\ldots,\sigma(n)) \) (which is \( n \)). The reason why it is called “length” is Exercise 9(g): it says that \( \ell(\sigma) \) is the smallest number of permutations of the form \( s_k \) which can be multiplied to give \( \sigma \); thus, it is the smallest possible length of an expression of \( \sigma \) as a product of \( s_k \).s. The use of the word “length”, unfortunately, is not standard across literature. Some authors call “Coxeter length” what we call “length”, and use the word “length” itself for a different notion.

**Exercise 10.** Let \( \sigma \in S_n \). In Exercise 8(b), we have seen that \( \sigma \) can be written as a composition of several permutations of the form \( s_k \) (with \( k \in \{1,2,\ldots,n-1\} \)). Usually there will be several ways to do so (for instance, \( \text{id} = s_1 \circ s_1 = s_2 \circ s_2 = \cdots = s_{n-1} \circ s_{n-1} \)). Show that, whichever of these ways we take, the number of permutations composed will be congruent to \( \ell(\sigma) \) modulo 2.

### 5.3. The sign of a permutation

**Definition 5.12.** We define the sign of a permutation \( \sigma \in S_n \) as the integer \((-1)^{\ell(\sigma)}\). We denote this sign by \((-1)^\sigma\) or \(\text{sign} \sigma\) or \(\text{sgn} \sigma\). We say that a permutation \( \sigma \) is even if its sign is 1 (that is, if \( \ell(\sigma) \) is even), and odd if its sign is \(-1\) (that is, if \( \ell(\sigma) \) is odd).

Signs of permutations have the following properties:

- The sign of the identity permutation \( \text{id} \in S_n \) is \((-1)^{\text{id}} = 1\) (because the definition of \((-1)^{\text{id}}\) yields \((-1)^{\text{id}} = (-1)^{\ell(\text{id})} = 1\) (since \( \ell(\text{id}) = 0\)). In other words, \( \text{id} \in S_n \) is even.
- For every \( k \in \{1,2,\ldots,n-1\} \), the sign of the permutation \( s_k \in S_n \) is \((-1)^{s_k} =\)
• If $\sigma$ and $\tau$ are two permutations in $S_n$, then $(-1)^{\sigma \circ \tau} = (-1)^\sigma \cdot (-1)^\tau$.

• If $\sigma \in S_n$, then $(-1)^{\sigma^{-1}} = (-1)^\sigma$.

The first and the third of these properties are often summarized as the statement that “sign is a group homomorphism from the group $S_n$ to the multiplicative group $\{1, -1\}$.” In this statement, “sign” means the map from $S_n$ to $\{1, -1\}$ which sends every permutation $\sigma$ to its sign $(-1)^{\ell(\sigma)}$, and the “multiplicative group $\{1, -1\}$” means the group $\{1, -1\}$ whose binary operation is multiplication.

We have defined the sign of a permutation $\sigma \in S_n$. More generally, it is possible to define the sign of a permutation of an arbitrary finite set $X$, even though the length of such a permutation is not defined.

**Exercise 11.** Let $n \geq 2$. Show that the number of even permutations in $S_n$ is $n!/2$, and the number of odd permutations in $S_n$ is also $n!/2$.

---

$^\text{80}$Proof. Let $k \in \{1, 2, \ldots, n-1\}$. Applying $^\text{91}$ to $\sigma = \text{id}$, we obtain

\[ \ell(\text{id} \circ s_k) = \begin{cases} \ell(\text{id}) + 1, & \text{if } \text{id}(k) < \text{id}(k+1); \\ \ell(\text{id}) - 1, & \text{if } \text{id}(k) > \text{id}(k+1) \end{cases} \]

\[ = \begin{cases} \ell(\text{id}) + 1, & \text{if } \text{id}(k) = k - (k+1) = \text{id}(k+1) \\ \ell(\text{id}) - 1, & \text{if } \text{id}(k) = k + (k+1) = \text{id}(k+1) \end{cases} \]

\[ = 0. \]

This rewrites as $\ell(s_k) = 1$ (since $\text{id} \circ s_k = s_k$). Now, the definition of $(-1)^{s_k}$ yields $(-1)^{s_k} = (-1)^{\ell(s_k)} = -1$ (since $\ell(s_k) = 1$), qed.

$^\text{81}$Proof. Let $\sigma \in S_n$ and $\tau \in S_n$. Exercise $^\text{92}$ (b) yields $\ell(\sigma \circ \tau) \equiv \ell(\sigma) + \ell(\tau) \pmod{2}$, so that $(-1)^{\ell(\sigma \circ \tau)} = (-1)^{\ell(\sigma) + \ell(\tau)} = (-1)^{\ell(\sigma)} \cdot (-1)^{\ell(\tau)}$. But the definition of the sign of a permutation yields $(-1)^{\sigma \circ \tau} = (-1)^{\ell(\sigma \circ \tau)} = (-1)^{\ell(\sigma)} \cdot (-1)^{\ell(\tau)}$. Hence, $(-1)^{\sigma \circ \tau} = (-1)^{\ell(\sigma)} \cdot (-1)^{\ell(\tau)} = (-1)^{\sigma} \cdot (-1)^{\tau}$, qed.

$^\text{82}$Proof. Let $\sigma \in S_n$. The definition of $(-1)^{\sigma^{-1}}$ yields $(-1)^{\sigma^{-1}} = (-1)^{\ell(\sigma^{-1})}$. But recall that $\ell(\sigma) = \ell(\sigma^{-1})$. The definition of $(-1)^{\sigma^{-1}}$ yields $(-1)^{\sigma^{-1}} = (-1)^{\ell(\sigma^{-1})}$ (since $\ell(\sigma) = \ell(\sigma^{-1})$).

Compared with $(-1)^{\sigma^{-1}} = (-1)^{\ell(\sigma^{-1})}$, this yields $(-1)^{\sigma^{-1}} = (-1)^{\tau}$, qed.

$^\text{83}$How does it work? If $X$ is a finite set, then we can always find a bijection $\phi : X \to \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. (Constructing such a bijection is tantamount to writing down a list of all elements of $X$, with no duplicates.) Given such a bijection $\phi$, we can define the sign of any permutation $\sigma$ of $X$ as follows:

\[ (-1)^{\sigma} = (-1)^{\phi \circ \sigma \circ \phi^{-1}}. \]  

Here, the right hand side is well-defined because $\phi \circ \sigma \circ \phi^{-1}$ is a permutation of $\{1, 2, \ldots, n\}$. What is not immediately obvious is that this sign is independent on the choice of $\phi$, and that it is a group homomorphism to $\{1, -1\}$ (that is, we have $(-1)^{\text{id}} = 1$ and $(-1)^{\sigma \circ \tau} = (-1)^{\sigma} \cdot (-1)^{\tau}$). We will prove these facts further below (in Exercise $^\text{93}$).
The sign of a permutation is used in the combinatorial definition of the determinant. Let us briefly show this definition now; we shall return to it later (in Chapter 6) to study it in much more detail.

**Definition 5.13.** Let \( n \in \mathbb{N} \). Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix (say, with complex entries, although this does not matter much – it suffices that the entries can be added and multiplied and the axioms of associativity, distributivity, commutativity, unity etc. hold). The determinant \( \det A \) of \( A \) is defined as

\[
\sum_{\sigma \in S_n} (-1)^\sigma a_{1,\sigma(1)}a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.
\]

Let me try to describe the sum (94) in slightly more visual terms: The sum (94) has \( n! \) addends, each of which has the form \( "(-1)^\sigma \) times a product". The product has \( n \) factors, which are entries of \( A \), and are chosen in such a way that there is exactly one entry taken from each row and exactly one from each column. Which precise entries are taken depends on \( \sigma \): namely, for each \( i \), we take the \( \sigma(i) \)-th entry from the \( i \)-th row.

Convince yourself that the classical formulas

\[
\begin{align*}
\det \begin{pmatrix} a \end{pmatrix} &= a; \\
\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= ad - bc; \\
\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} &= aei + bfg + cdh - ahf - bdi - ceg
\end{align*}
\]

are particular cases of (94). Whenever \( n \geq 2 \), the sum in (94) contains precisely \( n!/2 \) plus signs and \( n!/2 \) minus signs (because of Exercise 11).

Definition 5.13 is merely one of several equivalent definitions of the determinant. You will probably see two of them in an average linear algebra class. Each of them has its own advantages and drawbacks. Definition 5.13 is the most direct, assuming that one knows about the sign of a permutation.

### 5.4. Infinite permutations

(This section is optional; it explores some technical material which is useful in combinatorics, but is not necessary for what follows. I advise the reader to skip it at the first read.)

We have introduced the notion of a permutation of an arbitrary set; but so far, we have only studied permutations of finite sets. In this section (which is tangential to our project; probably nothing from this section will be used ever after), let me discuss permutations of the infinite set \( \{1, 2, 3, \ldots\} \). (A lot of what I say below can be easily adapted to the sets \( \mathbb{N} \) and \( \mathbb{Z} \) as well.)
We recall that a permutation of a set \( X \) means a bijection from \( X \) to \( X \).

Let \( S_\infty \) be the symmetric group of the set \( \{1,2,3,\ldots\} \). This is the set of all permutations of \( \{1,2,3,\ldots\} \). It contains the identity permutation \( \text{id} \in S_\infty \) which sends every \( i \in \{1,2,3,\ldots\} \) to \( i \). The set \( S_\infty \) is uncountable.\(^{84}\)

We shall try to study \( S_\infty \) similarly to how we studied \( S_n \) for \( n \in \mathbb{N} \). However, we soon will notice that the analogy between \( S_\infty \) and \( S_n \) will break down.\(^{85}\) To amend this, we shall define a subset \( S_{(\infty)} \) of \( S_\infty \) (mind the parentheses around the “\( \infty \)” which is smaller and more wieldy, and indeed shares many of the properties of the finite symmetric group \( S_n \).

We define \( S_{(\infty)} \) as follows:

\[
S_{(\infty)} = \{ \sigma \in S_\infty \mid \sigma(i) = i \text{ for all but finitely many } i \in \{1,2,3,\ldots\} \}.
\]  

(95)

Let us first explain what “all but finitely many \( i \in \{1,2,3,\ldots\} \)” means:

**Definition 5.14.** Let \( I \) be a set. Let \( A(i) \) be a statement for every \( i \in I \). Then, we say that “\( A(i) \) for all but finitely many \( i \in I \)” if and only if there exists some finite subset \( J \) of \( I \) such that every \( i \in I \setminus J \) satisfies \( A(i) \).\(^{86}\)

Thus, for a permutation \( \sigma \in S_\infty \), we have the following equivalence of statements:

\[
(\sigma(i) = i \text{ for all but finitely many } i \in \{1,2,3,\ldots\})
\]

\[
\iff (\text{there exists some finite subset } J \text{ of } \{1,2,3,\ldots\} \text{ such that}
\]

\[
every i \in \{1,2,3,\ldots\} \setminus J \text{ satisfies } \sigma(i) = i
\]

\[
\iff (\text{there exists some finite subset } J \text{ of } \{1,2,3,\ldots\} \text{ such that}
\]

\[
\text{the only } i \in \{1,2,3,\ldots\} \text{ that satisfy } \sigma(i) \neq i \text{ are elements of } J
\]

\[
\iff (\text{the set of all } i \in \{1,2,3,\ldots\} \text{ that satisfy } \sigma(i) \neq i \text{ is}
\]

\[
\text{contained in some finite subset } J \text{ of } \{1,2,3,\ldots\}
\]

\[
\iff (\text{there are only finitely many } i \in \{1,2,3,\ldots\} \text{ that satisfy } \sigma(i) \neq i).
\]

Hence, (95) rewrites as follows:

\[
S_{(\infty)} = \{ \sigma \in S_\infty \mid \text{there are only finitely many } i \in \{1,2,3,\ldots\} \text{ that satisfy } \sigma(i) \neq i \}.
\]

\(^{84}\)More generally, while a finite set of size \( n \) has \( n! \) permutations, an infinite set \( S \) has uncountably many permutations (even if \( S \) is countable).

\(^{85}\)The uncountability of \( S_\infty \) is the first hint that \( S_\infty \) is “too large” a set to be a good analogue of the finite set \( S_n \).

\(^{86}\)Thus, the statement “\( A(i) \) for all but finitely many \( i \in I \)” can be restated as “\( A(i) \) holds for all \( i \in I \), except for finitely many exceptions” or as “there are only finitely many \( i \in I \) which do not satisfy \( A(i) \)”.

I prefer the first wording, because it makes the most sense in constructive logic.

**Caution:** Do not confuse the words “all but finitely many \( i \in I \)” in this definition with the words “infinitely many \( i \in I \)”.

For instance, it is true that \( n \) is even for infinitely many \( n \in \mathbb{Z} \), but it is not true that \( n \) is even for all but finitely many \( n \in \mathbb{Z} \). Conversely, it is true that \( n > 1 \) for all but finitely many \( n \in \{1,2,\ldots\} \) (because the only \( n \in \{1,2,\ldots\} \) which does not satisfy \( n > 1 \) is 1), but it is not true that \( n > 1 \) for infinitely many \( n \in \{1,2,\ldots\} \) (because there are no infinitely many \( n \in \{1,2,\ldots\} \) to begin with).

You will encounter the “all but finitely many” formulation often in abstract algebra. (Some people abbreviate it as “almost all”, but this abbreviation means other things as well.)
Example 5.15. Here is an example of a permutation which is in \( S_\infty \) but not in \( S_{(\infty)} \): Let \( \tau \) be the permutation of \( \{1, 2, 3, \ldots\} \) given by

\[
(\tau(1), \tau(2), \tau(3), \tau(4), \tau(5), \tau(6), \ldots) = (2, 1, 4, 3, 6, 5, \ldots).
\]

(It adds 1 to every odd positive integer, and subtracts 1 from every even positive integer.) Then, \( \tau \in S_\infty \) but \( \tau \notin S_{(\infty)} \).

On the other hand, let us show some examples of permutations in \( S_{(\infty)} \). For each \( i \in \{1, 2, 3, \ldots\} \), let \( s_i \) be the permutation in \( S_\infty \) that switches \( i \) with \( i + 1 \) but leaves all other numbers unchanged. (This is similar to the permutation \( s_i \) in \( S_n \) that was defined earlier. We have taken the liberty to re-use the name \( s_i \), hoping that no confusion will arise.)

Again, we have \( s_i^2 = \text{id} \) for every \( i \in \{1, 2, 3, \ldots\} \) (where \( a^2 \) means \( a \circ a \) for any \( a \in S_\infty \)).

Proposition 5.16. We have \( s_k \in S_{(\infty)} \) for every \( k \in \{1, 2, 3, \ldots\} \).

Proof of Proposition 5.16. Let \( k \in \{1, 2, 3, \ldots\} \). The permutation \( s_k \) has been defined as the permutation in \( S_\infty \) that switches \( k \) with \( k + 1 \) but leaves all other numbers unchanged. In other words, it satisfies \( s_k(k) = k + 1, s_k(k+1) = k \) and

\[
s_k(i) = i \quad \text{for every } i \in \{1, 2, 3, \ldots\} \text{ such that } i \notin \{k, k+1\}.
\]

(96)

Now, every \( i \in \{1, 2, 3, \ldots\} \setminus \{k, k+1\} \) satisfies \( s_k(i) = i \).\footnote{\( s_k(i) = i \) \text{ for every } \( i \in \{1, 2, 3, \ldots\} \setminus \{k, k+1\} \). This proves Proposition 5.16.} Hence, there exists some finite subset \( J \) of \( \{1, 2, 3, \ldots\} \) such that every \( i \in \{1, 2, 3, \ldots\} \setminus J \) satisfies \( s_k(i) = i \) (namely, \( J = \{k, k+1\} \)). In other words, \( s_k(i) = i \) for all but finitely many \( i \in \{1, 2, 3, \ldots\} \).

Thus, \( s_k \) is an element of \( S_\infty \) satisfying \( s_k(i) = i \) for all but finitely many \( i \in \{1, 2, 3, \ldots\} \). Hence,

\[
s_k \in \{\sigma \in S_\infty \mid \sigma(i) = i \text{ for all but finitely many } i \in \{1, 2, 3, \ldots\}\} = S_{(\infty)}.
\]

This proves Proposition 5.16.

Permutations can be composed and inverted, leading to new permutations. Let us first see that the same is true for elements of \( S_{(\infty)} \):

Proposition 5.17. (a) The identity permutation \( \text{id} \in S_\infty \) of \( \{1, 2, 3, \ldots\} \) satisfies \( \text{id} \in S_{(\infty)} \).

(b) For every \( \sigma \in S_{(\infty)} \) and \( \tau \in S_{(\infty)} \), we have \( \sigma \circ \tau \in S_{(\infty)} \).

(c) For every \( \sigma \in S_{(\infty)} \), we have \( \sigma^{-1} \in S_{(\infty)} \).

Proof. Let \( i \in \{1, 2, 3, \ldots\} \setminus \{k, k+1\} \). Thus, \( i \in \{1, 2, 3, \ldots\} \) and \( i \notin \{k, k+1\} \). Hence, (96) shows that \( s_k(i) = i \), qed.
Proof of Proposition 5.17. We have defined $S_{(\infty)}$ as the set of all $\sigma \in S_\infty$ such that $\sigma(i) = i$ for all but finitely many $i \in \{1, 2, 3, \ldots\}$. In other words, $S_{(\infty)}$ is the set of all $\sigma \in S_\infty$ such that there exists a finite subset $K$ of $\{1, 2, 3, \ldots\}$ such that (every $i \in \{1, 2, 3, \ldots\} \setminus K$ satisfies $\sigma(i) = i$). As a consequence, we have the following two facts:

1. If $K$ is a finite subset of $\{1, 2, 3, \ldots\}$, and if $\gamma \in S_\infty$ is a permutation such that
   \[(\text{every } i \in \{1, 2, 3, \ldots\} \setminus K \text{ satisfies } \gamma(i) = i), \tag{97}\]
   then
   \[\gamma \in S_{(\infty)}. \tag{98}\]

2. If $\gamma \in S_{(\infty)}$, then
   \[
   \left( \text{there exists some finite subset } K \text{ of } \{1, 2, 3, \ldots\} \text{ such that every } i \in \{1, 2, 3, \ldots\} \setminus K \text{ satisfies } \gamma(i) = i \right). \tag{99}\]

We can now step to the actual proof of Proposition 5.17.

(a) Every $i \in \{1, 2, 3, \ldots\} \setminus \emptyset$ satisfies $\text{id}(i) = i$. Thus, (98) (applied to $K = \emptyset$ and $\gamma = \text{id}$) yields $\text{id} \in S_{(\infty)}$. This proves Proposition 5.17 (a).

(b) Let $\sigma \in S_{(\infty)}$ and $\tau \in S_{(\infty)}$.

From (99) (applied to $\gamma = \sigma$), we conclude that there exists some finite subset $K$ of $\{1, 2, 3, \ldots\}$ such that every $i \in \{1, 2, 3, \ldots\} \setminus K$ satisfies $\sigma(i) = i$. Let us denote this $K$ by $J_1$. Thus, $J_1$ is a finite subset of $\{1, 2, 3, \ldots\}$, and

\[\text{every } i \in \{1, 2, 3, \ldots\} \setminus J_1 \text{ satisfies } \sigma(i) = i. \tag{100}\]

From (99) (applied to $\gamma = \tau$), we conclude that there exists some finite subset $K$ of $\{1, 2, 3, \ldots\}$ such that every $i \in \{1, 2, 3, \ldots\} \setminus K$ satisfies $\tau(i) = i$. Let us denote this $K$ by $J_2$. Thus, $J_2$ is a finite subset of $\{1, 2, 3, \ldots\}$, and

\[\text{every } i \in \{1, 2, 3, \ldots\} \setminus J_2 \text{ satisfies } \tau(i) = i. \tag{101}\]

The sets $J_1$ and $J_2$ are finite. Hence, their union $J_1 \cup J_2$ is finite. Moreover,

\[\text{every } i \in \{1, 2, 3, \ldots\} \setminus (J_1 \cup J_2) \text{ satisfies } (\sigma \circ \tau)(i) = i\]

Therefore, (98) (applied to $K = J_1 \cup J_2$ and $\gamma = \sigma \circ \tau$) yields $\sigma \circ \tau \in S_{(\infty)}$. This proves Proposition 5.17 (b).

Proof. Let $i \in \{1, 2, 3, \ldots\} \setminus (J_1 \cup J_2)$. Thus, $i \in \{1, 2, 3, \ldots\}$ and $i \notin J_1 \cup J_2$.

We have $i \notin J_1 \cup J_2$ and thus $i \notin J_1$ (since $J_1 \subseteq J_1 \cup J_2$). Hence, $i \in \{1, 2, 3, \ldots\} \setminus J_1$. Similarly, $i \in \{1, 2, 3, \ldots\} \setminus J_2$. Thus, (101) yields $\tau(i) = i$. Hence, $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$ (by (100)), qed.
(c) Let $\sigma \in S_\infty$.

From (99) (applied to $\gamma = \sigma$), we conclude that there exists some finite subset $K$ of $\{1, 2, 3, \ldots\}$ such that every $i \in \{1, 2, 3, \ldots\} \setminus K$ satisfies $\sigma(i) = i$. Consider this $K$. Thus, $K$ is a finite subset of $\{1, 2, 3, \ldots\}$, and every $i \in \{1, 2, 3, \ldots\} \setminus K$ satisfies $\sigma(i) = i$. (102)

Now,

\[ \text{every } i \in \{1, 2, 3, \ldots\} \setminus K \text{ satisfies } \sigma^{-1}(i) = i \]

Therefore, (98) (applied to $\gamma = \sigma^{-1}$) yields $\sigma^{-1} \in S_\infty$. This proves Proposition 5.17 (c). \[ \square \]

In the language of group theorists, Proposition 5.17 shows that $S_\infty$ is a subgroup of the group $S_\infty$. The elements of $S_\infty$ are called the finitary permutations of $\{1, 2, 3, \ldots\}$, and $S_\infty$ is called the finitary symmetric group of $\{1, 2, 3, \ldots\}$.

We now have the following analogue of Exercise 8 (without its part (c)):

Exercise 12. (a) Show that

\[ s_i \circ s_{i+1} \circ s_i = s_{i+1} \circ s_i \circ s_{i+1} \]

for all $i \in \{1, 2, 3, \ldots\}$.

(b) Show that every permutation $\sigma \in S_\infty$ can be written as a composition of several permutations of the form $s_k$ (with $k \in \{1, 2, 3, \ldots\}$).

Remark 5.18. In the language of group theory, the statement of Exercise 12 (b) says (or, more precisely, yields) that the permutations $s_1, s_2, s_3, \ldots$ generate the group $S_\infty$.

If $\sigma \in S_\infty$ is a permutation, then an inversion of $\sigma$ means a pair $(i, j)$ of integers satisfying $1 \leq i < j$ and $\sigma(i) > \sigma(j)$. This definition of an inversion is, of course, analogous to the definition of an inversion of a $\sigma \in S_n$; thus we could try to define the length of a $\sigma \in S_\infty$. However, here we run into troubles: A permutation $\sigma \in S_\infty$ might have infinitely many inversions!

It is here that we really need to restrict ourselves to $S_\infty$. This indeed helps:

Proposition 5.19. Let $\sigma \in S_\infty$. Then:

(a) There exists some $N \in \{1, 2, 3, \ldots\}$ such that every integer $i > N$ satisfies $\sigma(i) = i$.

(b) There are only finitely many inversions of $\sigma$.

Proof of Proposition 5.19 (a) We can apply (99) to $\gamma = \sigma$. As a consequence, we obtain that there exists some finite subset $K$ of $\{1, 2, 3, \ldots\}$ such that

\[ \text{every } i \in \{1, 2, 3, \ldots\} \setminus K \text{ satisfies } \sigma(i) = i. \]

(103)

Consider this $K$.

\[ \text{Proof. Let } i \in \{1, 2, 3, \ldots\} \setminus K. \text{ Thus, } \sigma(i) = i \text{ (according to (102)), so that } \sigma^{-1}(i) = i, \text{ qed.} \]
The set $K$ is finite. Hence, the set $K \cup \{1\}$ is finite; this set is also nonempty (since it contains 1) and a subset of $\{1,2,3,\ldots\}$. Therefore, this set $K \cup \{1\}$ has a greatest element (since every finite nonempty subset of $\{1,2,3,\ldots\}$ has a greatest element). Let $n$ be this greatest element. Clearly, $n \in K \cup \{1\} \subseteq \{1,2,3,\ldots\}$, so that $n > 0$.

Every $j \in K \cup \{1\}$ satisfies
\[ j \leq n \tag{104} \]
(since $n$ is the greatest element of $K \cup \{1\}$). Now, let $i$ be an integer such that $i > n$. Then, $i > n > 0$, so that $i$ is a positive integer. If we had $i \in K$, then we would have $i \in K \subseteq K \cup \{1\}$ and thus $i \leq n$ (by (104), applied to $j = i$), which would contradict $i > n$. Hence, we cannot have $i \in K$. We thus have $i \notin K$. Since $i \in \{1,2,3,\ldots\}$, this shows that $i \in \{1,2,3,\ldots\} \setminus K$. Thus, $\sigma(i) = i$ (by (103)).

Let us now forget that we fixed $i$. We thus have shown that every integer $i > n$ satisfies $\sigma(i) = i$. Hence, Proposition 5.19 (a) holds (we can take $N = n$).

(b) Proposition 5.19 (a) shows that there exists some $N \in \{1,2,3,\ldots\}$ such that every integer $i > N$ satisfies $\sigma(i) = i$. \hfill (105)

Consider such an $N$. We shall now show that

every inversion of $\sigma$ is an element of $\{1,2,\ldots,N\}^2$.

In fact, let $c$ be an inversion of $\sigma$. We will show that $c$ is an element of $\{1,2,\ldots,N\}^2$.

We know that $c$ is an inversion of $\sigma$. In other words, $c$ is a pair $(i,j)$ of integers satisfying $1 \leq i < j$ and $\sigma(i) > \sigma(j)$ (by the definition of an “inversion of $\sigma$”). Consider this $(i,j)$. We then have $i \leq N$ \hfill (106) and $j \leq N$ \hfill (107). Consequently, $(i,j) \in \{1,2,\ldots,N\}^2$. Hence, $c = (i,j) \in \{1,2,\ldots,N\}^2$.

Now, let us forget that we fixed $c$. We thus have shown that if $c$ is an inversion of $\sigma$, then $c$ is an element of $\{1,2,\ldots,N\}^2$. In other words, every inversion of $\sigma$ is an element of $\{1,2,\ldots,N\}^2$. Thus, there are only finitely many inversions of $\sigma$ (since there are only finitely many elements of $\{1,2,\ldots,N\}^2$). Proposition 5.19 (b) is thus proven. \hfill \Box

Actually, Proposition 5.19 (b) has a converse: If a permutation $\sigma \in S_\infty$ has only finitely many inversions, then $\sigma$ belongs to $S_{(\infty)}$. This is easy to prove; but we won’t use this.

If $\sigma \in S_{(\infty)}$ is a permutation, then the length of $\sigma$ means the number of inversions of $\sigma$. This is well-defined, because there are only finitely many inversions of $\sigma$ (by

\begin{align*}
90 & \text{Proof. Assume the contrary. Thus, } i > N. \text{ Hence, } (105) \text{ shows that } \sigma(i) = i. \text{ Also, } i < j, \text{ so that } j > i > N. \text{ Hence, } (105) \text{ (applied to } j \text{ instead of } i) \text{ shows that } \sigma(j) = j. \text{ Thus, } \sigma(i) = i < j = \sigma(j). \text{ This contradiction shows that our assumption was wrong. qed.} \\
91 & \text{Proof. Assume the contrary. Thus, } j > N. \text{ Hence, } (105) \text{ (applied to } j \text{ instead of } i) \text{ shows that } \sigma(j) = j. \text{ Now, } \sigma(i) > \sigma(j) > N. \text{ Therefore, } (105) \text{ (applied to } \sigma(i) \text{ instead of } i) \text{ yields } \sigma(\sigma(i)) = \sigma(i). \text{ But } \sigma \text{ is a permutation, and thus an injective map. Hence, from } \sigma(\sigma(i)) = \sigma(i), \text{ we obtain } \sigma(i) = i. \text{ Thus, } \sigma(i) = i < j = \sigma(j). \text{ This contradiction shows that our assumption was wrong. qed.}
\end{align*}
Proposition 5.19 (b). The length of \( \sigma \) is denoted by \( \ell (\sigma) \); it is a nonnegative integer. The only permutation having length 0 is the identity permutation \( \text{id} \in S_\infty \).

We have the following analogue of Exercise 9:

**Exercise 13.** (a) Show that every permutation \( \sigma \in S_\infty \) and every \( k \in \{1, 2, 3, \ldots\} \) satisfy

\[
\ell (\sigma \circ s_k) = \begin{cases} 
\ell (\sigma) + 1, & \text{if } \sigma (k) < \sigma (k + 1); \\
\ell (\sigma) - 1, & \text{if } \sigma (k) > \sigma (k + 1) 
\end{cases}
\]

and

\[
\ell (s_k \circ \sigma) = \begin{cases} 
\ell (\sigma) + 1, & \text{if } \sigma^{-1} (k) < \sigma^{-1} (k + 1); \\
\ell (\sigma) - 1, & \text{if } \sigma^{-1} (k) > \sigma^{-1} (k + 1) 
\end{cases}
\]

(b) Show that any two permutations \( \sigma \) and \( \tau \) in \( S_\infty \) satisfy \( \ell (\sigma \circ \tau) \equiv \ell (\sigma) + \ell (\tau) \mod 2 \).

(c) Show that any two permutations \( \sigma \) and \( \tau \) in \( S_\infty \) satisfy \( \ell (\sigma \circ \tau) \leq \ell (\sigma) + \ell (\tau) \).

(d) If \( \sigma \in S_\infty \) is a permutation satisfying \( \sigma (1) \leq \sigma (2) \leq \sigma (3) \leq \cdots \), then show that \( \sigma = \text{id} \).

(e) Let \( \sigma \in S_\infty \). Show that \( \sigma \) can be written as a composition of \( \ell (\sigma) \) permutations of the form \( s_k \) (with \( k \in \{1, 2, 3, \ldots\} \)).

(f) Let \( \sigma \in S_\infty \). Then, show that \( \ell (\sigma) = \ell (\sigma^{-1}) \).

(g) Let \( \sigma \in S_\infty \). Show that \( \ell (\sigma) \) is the smallest \( N \in \mathbb{N} \) such that \( \sigma \) can be written as a composition of \( N \) permutations of the form \( s_k \) (with \( k \in \{1, 2, 3, \ldots\} \)).

We also have an analogue of Exercise 10:

**Exercise 14.** Let \( \sigma \in S_\infty \). In Exercise 12 (b), we have seen that \( \sigma \) can be written as a composition of several permutations of the form \( s_k \) (with \( k \in \{1, 2, 3, \ldots\} \)). Usually there will be several ways to do so (for instance, \( \text{id} = s_1 \circ s_1 = s_2 \circ s_2 = s_3 \circ s_3 = \cdots \)). Show that, whichever of these ways we take, the number of permutations composed will be congruent to \( \ell (\sigma) \mod 2 \).

Having defined the length of a permutation \( \sigma \in S_\infty \), we can now define the sign of such a permutation. Again, we mimic the definition of the sign of a \( \sigma \in S_n \):

**Definition 5.20.** We define the *sign* of a permutation \( \sigma \in S_\infty \) as the integer \((-1)^{\ell (\sigma)}\). We denote this sign by \((-1)^{\sigma}\) or \(\text{sgn } \sigma\). We say that a permutation \( \sigma \) is *even* if its sign is 1 (that is, if \( \ell (\sigma) \) is even), and *odd* if its sign is \(-1\) (that is, if \( \ell (\sigma) \) is odd).

Signs of permutations have the following properties:

- The sign of the identity permutation \( \text{id} \in S_\infty \) is \((-1)^{\text{id}} = 1\). In other words, \( \text{id} \in S_\infty \) is even.
• For every \( k \in \{1, 2, 3, \ldots\} \), the sign of the permutation \( s_k \in S_\infty \) is \((-1)^k = -1\).

• If \( \sigma \) and \( \tau \) are two permutations in \( S_\infty \), then \((-1)^{\sigma \circ \tau} = (-1)^\sigma \cdot (-1)^\tau\).

• If \( \sigma \in S_\infty \), then \((-1)^{\sigma^{-1}} = (-1)^\sigma\).

The proofs of all these properties are analogous to the proofs of the analogous properties for permutations in \( S_n \).

**Remark 5.21.** We have defined the sign of a permutation \( \sigma \in S_\infty \). No such notion exists for permutations \( \sigma \in S_\infty \). In fact, one can show that if an element \( \lambda_\sigma \) of \( \{1, -1\} \) is chosen for each \( \sigma \in S_\infty \) in such a way that every two permutations \( \sigma, \tau \in S_\infty \) satisfy \((-1)^{\sigma \circ \tau} = (-1)^\sigma \cdot (-1)^\tau\), then all of the \( \lambda_\sigma \) are 1. (Indeed, this follows from a result of Oystein Ore; see [http://mathoverflow.net/questions/54371](http://mathoverflow.net/questions/54371).)

**Remark 5.22.** For every \( n \in \mathbb{N} \) and every \( \sigma \in S_n \), we can define a permutation \( \sigma_\infty \in S_\infty \) by setting

\[
\sigma_\infty (i) = \begin{cases} 
\sigma(i), & \text{if } i \leq n; \\
i, & \text{if } i > n
\end{cases}
\text{ for all } i \in \{1, 2, 3, \ldots\}.
\]

Essentially, \( \sigma_\infty \) is the permutation \( \sigma \) extended to the set of all positive integers in the laziest possible way: It just sends each \( i > n \) to itself.

For every \( n \in \mathbb{N} \), there is an injective map \( i_n : S_n \to S_\infty \) defined as follows:

\[
i_n (\sigma) = \sigma_\infty \quad \text{for every } \sigma \in S_n.
\]

This map \( i_n \) is an example of what algebraists call a group homomorphism: It satisfies

\[
i_n (\text{id}) = \text{id};
\]

\[
i_n (\sigma \circ \tau) = i_n (\sigma) \circ i_n (\tau) \quad \text{for all } \sigma, \tau \in S_n;
\]

\[
i_n (\sigma^{-1}) = (i_n (\sigma))^{-1} \quad \text{for all } \sigma \in S_n.
\]

(This is all easy to check.) Thus, we can consider the image \( i_n (S_n) \) of \( S_n \) under this map as a “copy” of \( S_n \) which is “just as good as the original” (i.e., composition in this copy behaves in the same way as composition in the original). It is easy to characterize this copy inside \( S_\infty \): Namely,

\[
i_n (S_n) = \left\{ \sigma \in S_\infty \mid \sigma(i) = i \text{ for all } i > n \right\}.
\]

Using Proposition 5.19 (a), it is easy to check that \( S_\infty = \bigcup_{n \in \mathbb{N}} i_n (S_n) = i_0 (S_0) \cup i_1 (S_1) \cup i_2 (S_2) \cup \cdots \). Therefore, many properties of \( S_\infty \) can be derived from analogous properties of \( S_n \) for finite \( n \). For example, using this tactic,
we could easily derive Exercise 13 from Exercise 9 and derive Exercise 14 from Exercise 10. (However, we can just as well solve Exercises 13 and 14 by copying the solutions of Exercises 9 and 10 and making the necessary changes; this is how I solve these exercises further below.)

5.5. More on lengths of permutations

Let us summarize some of what we have learnt about permutations. We have defined the length $\ell(\sigma)$ and the inversions of a permutation $\sigma \in S_n$, where $n$ is a nonnegative integer. We recall the basic properties of these objects:

- For each $k \in \{1, 2, \ldots, n - 1\}$, we defined $s_k$ to be the permutation in $S_n$ that switches $k$ with $k + 1$ but leaves all other numbers unchanged. These permutations satisfy $s_k^2 = \text{id}$ for every $i \in \{1, 2, \ldots, n - 1\}$ and
  \[ s_i \circ s_{i+1} \circ s_i = s_{i+1} \circ s_i \circ s_{i+1} \quad \text{for all } i \in \{1, 2, \ldots, n - 2\} \]  
  (according to Exercise 8(a)). Also, it is easy to check that
  \[ s_i \circ s_j = s_j \circ s_i \quad \text{for all } i, j \in \{1, 2, \ldots, n - 1\} \text{ with } |i - j| > 1. \]  

- An inversion of a permutation $\sigma \in S_n$ means a pair $(i, j)$ of integers satisfying $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. The length $\ell(\sigma)$ of a permutation $\sigma \in S_n$ is the number of inversions of $\sigma$.

- Any two permutations $\sigma \in S_n$ and $\tau \in S_n$ satisfy
  \[ \ell(\sigma \circ \tau) \equiv \ell(\sigma) + \ell(\tau) \mod 2 \]  
  (by Exercise 9(b)) and
  \[ \ell(\sigma \circ \tau) \leq \ell(\sigma) + \ell(\tau) \]  
  (by Exercise 9(c)).

- If $\sigma \in S_n$, then $\ell(\sigma) = \ell(\sigma^{-1})$ (according to Exercise 9(f)).

- If $\sigma \in S_n$, then $\ell(\sigma)$ is the smallest $N \in \mathbb{N}$ such that $\sigma$ can be written as a composition of $N$ permutations of the form $s_k$ (with $k \in \{1, 2, \ldots, n - 1\}$). (This follows from Exercise 9(g).)

By now, we know almost all about the $s_k$’s and about the lengths of permutations that is necessary for studying determinants. (“Almost” because Exercise 16 below will also be useful.) I shall now sketch some more advanced properties of these things, partly as a curiosity, partly to further your intuition; none of these properties shall be used further below.
First, here is a way to visualize lengths of permutations using graph theory:

Fix $n \in \mathbb{N}$. We define the $n$-th right Bruhat graph to be the (undirected) graph whose vertices are the permutations $\sigma \in S_n$, and whose edges are defined as follows: Two vertices $\sigma \in S_n$ and $\tau \in S_n$ are adjacent if and only if there exists a $k \in \{1, 2, \ldots, n-1\}$ such that $\sigma = \tau \circ s_k$. (This condition is clearly symmetric in $\sigma$ and $\tau$: If $\sigma = \tau \circ s_k$, then $\tau = \sigma \circ s_k$.) For instance, the 3-rd right Bruhat graph looks as follows:

![Diagram of the 3rd right Bruhat graph]

where we are writing permutations in one-line notation (and omitting parentheses and commas). The 4-th right Bruhat graph can be seen [on Wikipedia].

These graphs have lots of properties. There is a canonical way to direct their edges: The edge between $\sigma$ and $\tau$ is directed towards the vertex with the larger length. (The lengths of $\sigma$ and $\tau$ always differ by 1 if there is an edge between $\sigma$ and $\tau$.) This way, the $n$-th right Bruhat graph is an acyclic directed graph. It therefore defines a partially ordered set, called the right permutohedron order on $S_n$, whose elements are the permutations $\sigma \in S_n$ and whose order relation is defined as follows: We have $\sigma \leq \tau$ if and only if there is a directed path from $\sigma$ to $\tau$ in the directed $n$-th right Bruhat graph. If you know the (combinatorial) notion of a lattice, you might notice that this right permutohedron order is a lattice.

The word “permutohedron” in “permutohedron order” hints at what might be its least expected property: The $n$-th Bruhat graph can be viewed as the graph formed by the vertices and the edges of a certain polytope in $n$-dimensional space $\mathbb{R}^n$. This polytope – called the $n$-th permutohedron – is the convex hull of the points $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ for $\sigma \in S_n$. These points are its vertices; however, its vertex $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ corresponds to the vertex $\sigma^{-1}$ (not $\sigma$) of the $n$-th Bruhat graph. Feel free to roam its Wikipedia page for other (combinatorial and geometric) curiosities.

The notion of a length fits perfectly into this whole picture. For instance, the length $\ell(\sigma)$ of a permutation $\sigma$ is the smallest length of a path from id $\in S_n$ to $\sigma$ on the $n$-th right Bruhat graph (and this holds no matter whether the graph

---

92Don’t omit the word “right” in “right Bruhat graph”; else it means a different graph with more edges.

93also known as the right weak order or right weak Bruhat order (but, again, do not omit the words “right” and “weak”)

94Some spell it “permutahedron” instead. The word is of relatively recent origin (1969).
is considered to be directed or not). For the undirected Bruhat graphs, we have something more general:

**Exercise 15.** Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ and $\tau \in S_n$. Show that $\ell (\sigma^{-1} \circ \tau)$ is the smallest length of a path between $\sigma$ and $\tau$ on the (undirected) $n$-th right Bruhat graph.

(Recall that the length of a path in a graph is defined as the number of edges along this path.)

How many permutations in $S_n$ have a given length? The number is not easy to compute directly; however, its generating function is nice. Namely,

$$
\sum_{w \in S_n} q^{\ell(w)} = (1 + q) (1 + q + q^2) \cdots (1 + q + q^2 + \cdots + q^{n-1})
$$

(where $q$ is an indeterminate). See [Stan11, Corollary 1.3.13] for a proof (but notice that Stanley denotes $S_n$ by $\mathcal{S}_n$, and $\ell (w)$ by $\text{inv} (w)$).

**Remark 5.23.** Much more can be said. Let me briefly mention (without proof) two other related results.

We can ask ourselves in what different ways a permutation can be written as a composition of $N$ permutations of the form $s_k$. For instance, the permutation $w_0 \in S_3$ which sends 1, 2 and 3 to 3, 2 and 1, respectively (that is, $w_0 = (3, 2, 1)$ in one-line notation) can be written as a product of three $s_k$'s in the two forms

$$
w_0 = s_1 \circ s_2 \circ s_1, \quad w_0 = s_2 \circ s_1 \circ s_2,
$$

but can also be written as a product of five $s_k$'s (e.g., as $w_0 = s_1 \circ s_2 \circ s_1 \circ s_2 \circ s_2$) or seven $s_k$'s or nine $s_k$'s, etc. Are the different representations of $w_0$ related?

Clearly, the two representations in (112) are connected to each other by the equality $s_1 \circ s_2 \circ s_1 = s_2 \circ s_1 \circ s_2$, which is a particular case of (108). Also, the representation $w_0 = s_1 \circ s_2 \circ s_1 \circ s_2 \circ s_2$ reduces to $w_0 = s_1 \circ s_2 \circ s_1$ by “cancelling” the two adjacent $s_2$’s at the end (recall that $s_i \circ s_i = s_i^2 = \text{id}$ for every $i$).

Interestingly, this generalizes. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. A reduced expression for $\sigma$ will mean a representation of $\sigma$ as a composition of $\ell (\sigma)$ permutations of the form $s_k$. (As we know, less than $\ell (\sigma)$ such permutations do not suffice; thus the name “reduced”.) Then, (one of the many versions of) Matsumoto’s theorem states that any two reduced expressions of $\sigma$ can be obtained from one another by a rewriting process, each step of which is either an application of (108) (i.e., you pick an “$s_i \circ s_i+1 \circ s_i$” in the expression and replace it by “$s_i+1 \circ s_i \circ s_{i+1}$”, or vice versa) or an application of (109) (i.e., you pick an “$s_i \circ s_j$” with $|i - j| > 1$ and replace it by “$s_j \circ s_i$”, or vice versa). For instance, for $n = 4$ and $\sigma = (4, 3, 1, 2, 5)$ (in one-line notation), the two reduced expressions $\sigma = s_1 \circ s_2 \circ s_3 \circ s_1 \circ s_2$ and $\sigma = s_2 \circ s_3 \circ s_1 \circ s_2 \circ s_3$ can be obtained from one another.
by the following rewriting process:

\[
S_1 \circ S_2 \circ S_3 \circ S_1 = S_1 \circ S_2 \circ S_3 \circ S_2 = S_2 \circ S_3 \circ S_2 \circ S_3 \circ S_1 \circ S_2 \circ S_3 \circ S_2
\]

(by (109))

See, e.g., Williamson’s thesis [William03, Corollary 1.2.3] or Knutson’s notes [Knutson, §2.3] for a proof of this fact. (Knutson, instead of saying that “\(\sigma = s_{k_1} \circ s_{k_2} \circ \cdots \circ s_{k_p}\) is a reduced expression for \(\sigma\)”, says that “\(k_1k_2 \cdots k_p\) is a reduced word for \(\sigma\).”)

Something subtler holds for “non-reduced” expressions. Namely, if we have a representation of \(\sigma\) as a composition of some number of permutations of the form \(s_k\) (not necessarily \(\ell(\sigma)\) of them), then we can transform it into a reduced expression by a rewriting process which consists of applications of (108) and (109) as before and also of cancellation steps (i.e., picking an “\(s_i \circ s_i\)” in the expression and removing it). This follows from [LLPT95, Proposition (2.6)] and can also easily be derived from [William03, Corollary 1.2.3 and Corollary 1.1.6].

This all is stated and proven in greater generality in good books on Coxeter groups, such as [BjoBre05]. We won’t need these results in the following, but they are an example of what one can see if one looks at permutations closely.

### 5.6. More on signs of permutations

In Section 5.3, we have defined the sign \((-1)^{\sigma} = \text{sign } \sigma = \text{sgn } \sigma\) of a permutation \(\sigma\). We recall the most important facts about it:

- We have \((-1)^{\sigma} = (-1)^{\ell(\sigma)}\) for every \(\sigma \in S_n\). (This is the definition of \((-1)^{\sigma}\).)
  Thus, for every \(\sigma \in S_n\), we have \((-1)^{\sigma} = (-1)^{\ell(\sigma)} \in \{1, -1\}\).
- The permutation \(\sigma \in S_n\) is said to be even if \((-1)^{\sigma} = 1\), and is said to be odd if \((-1)^{\sigma} = -1\).
- The sign of the identity permutation \(\text{id} \in S_n\) is \((-1)^{\text{id}} = 1\).
- For every \(k \in \{1, 2, \ldots, n - 1\}\), the sign of the permutation \(s_k \in S_n\) is \((-1)^{s_k} = -1\).

\(^{95}\)What the authors of [LLPT95] call a “presentation” of a permutation \(\sigma \in S_n\) is a finite list \(\{s_{k_1}, s_{k_2}, \ldots, s_{k_p}\}\) of elements of \(\{s_1, s_2, \ldots, s_{n-1}\}\) satisfying \(\sigma = s_{k_1} \circ s_{k_2} \circ \cdots \circ s_{k_p}\). What the authors of [LLPT95] call a “minimal presentation” of \(\sigma\) is what we call a reduced expression of \(\sigma\).
• If $\sigma$ and $\tau$ are two permutations in $S_n$, then
\[
(-1)^{\sigma \tau} = (-1)^\sigma \cdot (-1)^\tau.
\] (113)

• If $\sigma \in S_n$, then
\[
(-1)^{\sigma^{-1}} = (-1)^\sigma.
\] (114)

A simple consequence of the above facts is the following proposition:

**Proposition 5.24.** Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_k$ be $k$ permutations in $S_n$. Then,
\[
(-1)^{\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k} = (-1)^{\sigma_1} \cdot (-1)^{\sigma_2} \cdots (-1)^{\sigma_k}.
\] (115)

**Proof of Proposition 5.24.** Straightforward induction over $k$. The induction base (i.e., the case when $k = 0$) follows from the fact that $(-1)^{\text{id}} = 1$ (since the composition of 0 permutations is id). The induction step is easily done using (113). \qed

We state a few more properties, which should not be difficult by now:

**Definition 5.25.** Let $n \in \mathbb{N}$. Let $i$ and $j$ be two distinct elements of $\{1, 2, \ldots, n\}$. We let $t_{ij}$ be the permutation in $S_n$ which switches $i$ with $j$ while leaving all other elements of $\{1, 2, \ldots, n\}$ unchanged. Such a permutation is called a *transposition* (and is often denoted by $(i, j)$ in literature; but we prefer not to do so, since it is too similar to one-line notation).

Notice that the permutations $s_1, s_2, \ldots, s_{n-1}$ are transpositions (namely, $s_i = t_{i,i+1}$ for every $i \in \{1, 2, \ldots, n-1\}$), but they are not the only transpositions (when $n \geq 3$).

**Exercise 16.** Let $n \in \mathbb{N}$. Let $i$ and $j$ be two distinct elements of $\{1, 2, \ldots, n\}$.

(a) Find $\ell(t_{ij})$.

(b) Show that $(-1)^{t_{ij}} = -1$.

**Exercise 17.** Let $n \in \mathbb{N}$. Let $w_0$ denote the permutation in $S_n$ which sends each $k \in \{1, 2, \ldots, n\}$ to $n+1-k$. Compute $\ell(w_0)$ and $(-1)^{w_0}$.

**Exercise 18.** Let $X$ be a finite set. We want to define the sign of any permutation of $X$. (We have sketched this definition before (see (93)), but now we shall do it in detail.)

Fix a bijection $\phi : X \to \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. (Such a bijection always exists. Indeed, constructing such a bijection is tantamount to writing down a list of all elements of $X$, with no duplicates.) For every permutation $\sigma$ of $X$, set
\[
(-1)^\sigma = (-1)^{\phi \circ \sigma \circ \phi^{-1}}.
\]
Here, the right hand side is well-defined because $\phi \circ \sigma \circ \phi^{-1}$ is a permutation of \{1, 2, \ldots, n\}.

(a) Prove that $(-1)_\phi^\sigma$ depends only on the permutation $\sigma$ of $X$, but not on the bijection $\phi$. (In other words, for a given $\sigma$, any two different choices of $\phi$ will lead to the same $(-1)_\phi^\sigma$.) This allows us to define the sign of the permutation $\sigma$ to be $(-1)_\phi^\sigma$ for any choice of bijection $\phi: X \to \{1, 2, \ldots, n\}$. We denote this sign simply by $(-1)_\phi^\sigma$.

(b) Show that the permutation $\text{id}: X \to X$ satisfies $(-1)_\phi^{\text{id}} = 1$.

(c) Show that $(-1)_\phi^{\sigma \circ \tau} = (-1)_\phi^{\sigma} \cdot (-1)_\phi^\tau$ for any two permutations $\sigma$ and $\tau$ of $X$.

Remark 5.26. Let $n \in \mathbb{N}$. Recall that a transposition in $S_n$ means a permutation of the form $t_{i,j}$, where $i$ and $j$ are two distinct elements of \{1, 2, \ldots, n\}. Therefore, if $\tau$ is a transposition in $S_n$, then

$$\langle -1 \rangle^\tau = -1.$$  \hspace{1cm} (116)

(In fact, if $\tau$ is a transposition in $S_n$, then $\tau$ can be written in the form $\tau = t_{i,j}$ for two distinct elements $i$ and $j$ of \{1, 2, \ldots, n\}; and therefore, for these two elements $i$ and $j$, we have $\langle -1 \rangle^\tau = (-1)^{i,j} = -1$ (according to Exercise 16 (b)). This proves (116).)

Now, let $\sigma \in S_n$ be any permutation. Assume that $\sigma$ is written in the form $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ for some transpositions $\tau_1, \tau_2, \ldots, \tau_k$ in $S_n$. Then,

$$(-1)^\sigma = (-1)^{\tau_1 \circ \tau_2 \circ \cdots \circ \tau_k} = (-1)^{\tau_1} \cdot (-1)^{\tau_2} \cdot \cdots \cdot (-1)^{\tau_k}$$

(by (116), applied to $\sigma_i = \tau_i$)

$$= (-1) \cdot (-1) \cdot \cdots \cdot (-1) = (-1)^k.$$ \hspace{1cm} (117)

Since many permutations can be written as products of transpositions in a simple way, this formula gives a useful method for computing signs.

Remark 5.27. Let $n \in \mathbb{N}$. It is not hard to prove that

$$(-1)^\sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \quad \text{for every } \sigma \in S_n.$$ \hspace{1cm} (118)

(Of course, it is no easier to compute $(-1)^\sigma$ using this seemingly explicit formula than by counting inversions.) We shall prove (118) in Exercise 19 (c).
Remark 5.28. The sign of a permutation is also called its *signum* or its *signature*. Different authors define the sign of a permutation $\sigma$ in different ways. Some (e.g., Hefferon in [Hefferon, Definition 4.7]) define it as we do; others (e.g., Conrad in [Conrad] or Hoffman and Kunze in [HoffKun, p. 152]) define it using (117); yet others define it using something called the *cycle decomposition* of a permutation; some even define it using (118), or using a similar ratio of two polynomials. However, it is not hard to check that all of these definitions are equivalent. (We already know that the first two of them are equivalent.)

Exercise 19. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$.

(a) If $x_1, x_2, \ldots, x_n$ are $n$ elements of $C$, then prove that

$$\prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = (-1)^{\sigma} \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

(b) More generally: For every $(i, j) \in \{1, 2, \ldots, n\}^2$, let $a_{(i,j)}$ be an element of $C$. Assume that

$$a_{(j,i)} = -a_{(i,j)} \quad \text{for every } (i, j) \in \{1, 2, \ldots, n\}^2. \quad (119)$$

Prove that

$$\prod_{1 \leq i < j \leq n} a_{(\sigma(i), \sigma(j))} = (-1)^{\sigma} \cdot \prod_{1 \leq i < j \leq n} a_{(i,j)}.$$

(c) Prove (118).

(d) Use Exercise 19 (a) to give a new solution to Exercise 9 (b).

5.7. Cycles

Next, we shall discuss another specific class of permutations: the *cycles*.

Definition 5.29. Let $n \in \mathbb{N}$. Let $[n] = \{1, 2, \ldots, n\}$.

Let $k \in \{1, 2, \ldots, n\}$. Let $i_1, i_2, \ldots, i_k$ be $k$ distinct elements of $[n]$. We define $\text{cyc}_{i_1, i_2, \ldots, i_k}$ to be the permutation in $S_n$ which sends $i_1, i_2, \ldots, i_k$ to $i_2, i_3, \ldots, i_k, i_1$, respectively, while leaving all other elements of $[n]$ fixed. In other words, we define $\text{cyc}_{i_1, i_2, \ldots, i_k}$ to be the permutation in $S_n$ given by

$$\left(\text{cyc}_{i_1, i_2, \ldots, i_k}(p) = \begin{cases} i_{j+1}, & \text{if } p = i_j \text{ for some } j \in \{1, 2, \ldots, k\}; \\ p, & \text{otherwise} \end{cases} \right),$$

for every $p \in [n]$,

where $i_{k+1}$ means $i_1$.

(Again, the notation $\text{cyc}_{i_1, i_2, \ldots, i_k}$ conceals the parameter $n$, which will hopefully not cause any confusion.)
A permutation of the form $\text{cyc}_{i_1, i_2, \ldots, i_k}$ is said to be a $k$-cycle (or sometimes just a cycle, or a cyclic permutation). Of course, the name stems from the fact that it “cycles” through the elements $i_1, i_2, \ldots, i_k$ (by sending each of them to the next one and the last one back to the first) and leaves all other elements unchanged.

**Example 5.30.** Let $n \in \mathbb{N}$. The following facts follow easily from Definition 5.29:

(a) For every $i \in \{1, 2, \ldots, n\}$, we have $\text{cyc}_i = \text{id}$. In other words, any 1-cycle is the identity permutation id.

(b) If $i$ and $j$ are two distinct elements of $\{1, 2, \ldots, n\}$, then $\text{cyc}_{i,j} = t_{i,j}$. (See Definition 5.25 for the definition of $t_{i,j}$.)

(c) If $k \in \{1, 2, \ldots, n-1\}$, then $\text{cyc}_{k,k+1} = s_k$.

(d) If $n = 5$, then $\text{cyc}_{2,5,3}$ is the permutation which sends 1 to 1, 2 to 5, 3 to 2, 4 to 4, and 5 to 3. (In other words, it is the permutation which is $(1, 5, 2, 4, 3)$ in one-line notation.)

(e) If $k \in \{1, 2, \ldots, n\}$, and if $i_1, i_2, \ldots, i_k$ are $k$ pairwise distinct elements of $[n]$, then

$$\text{cyc}_{i_1, i_2, \ldots, i_k} = \text{cyc}_{i_2, i_3, \ldots, i_k, i_1} = \text{cyc}_{i_3, i_4, \ldots, i_k, i_1, i_2} = \cdots = \text{cyc}_{i_k, i_1, i_2, \ldots, i_{k-1}}.$$ 

(In less formal words: The $k$-cycle $\text{cyc}_{i_1, i_2, \ldots, i_k}$ does not change when we cyclically rotate the list $(i_1, i_2, \ldots, i_k)$.)

**Remark 5.31.** What we called $\text{cyc}_{i_1, i_2, \ldots, i_k}$ in Definition 5.29 is commonly denoted by $(i_1, i_2, \ldots, i_k)$ in the literature. But this latter notation $(i_1, i_2, \ldots, i_k)$ would clash with one-line notation for permutations (the cycle $\text{cyc}_{1,2,3} \in S_3$ is not the same as the permutation which is $(1, 2, 3)$ in one-line notation) and also with the standard notation for $k$-tuples. This is why we prefer to use the notation $\text{cyc}_{i_1, i_2, \ldots, i_k}$. (That said, we are not going to use $k$-cycles very often.)

The following exercise gathers some properties of cycles. Parts (a) and (d) and, to a lesser extent, (b) are fairly important and you should make sure you know how to solve them. The significantly more difficult part (c) is more of a curiosity with an interesting proof (I have not found an application of it so far; skip it if you do not want to spend time on what is essentially a contest problem).

**Exercise 20.** Let $n \in \mathbb{N}$. Let $[n] = \{1, 2, \ldots, n\}$. Let $k \in \{1, 2, \ldots, n\}$.

(a) For every $\sigma \in S_n$ and every $k$ distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, prove that

$$\sigma \circ \text{cyc}_{i_1, i_2, \ldots, i_k} \circ \sigma^{-1} = \text{cyc}_{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)}.$$

(b) For every $p \in \{0, 1, \ldots, n-k\}$, prove that

$$\ell \left( \text{cyc}_{p+1, p+2, \ldots, p+k} \right) = k - 1.$$
(c) For every $k$ distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, prove that
\[
\ell \left( \text{cyc}_{i_1, i_2, \ldots, i_k} \right) \geq k - 1.
\]

(d) For every $k$ distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, prove that
\[
(-1)^{\text{cyc}_{i_1, i_2, \ldots, i_k}} = (-1)^{k-1}.
\]

Remark 5.32. Exercise 20 (d) shows that every $k$-cycle in $S_n$ has sign $(-1)^{k-1}$. However, the length of a $k$-cycle need not be $k - 1$. Exercise 20 (c) shows that this length is always $\geq k - 1$, but it can take other values as well. For instance, in $S_4$, the length of the 3-cycle $\text{cyc}_{1,4,3}$ is 4. (Another example are the transpositions $t_{i,j}$ from Definition 5.25; these are 2-cycles but can have length > 1.)

I don’t know a simple way to describe when equality holds in Exercise 20 (c). It holds whenever $i_1, i_2, \ldots, i_k$ are consecutive integers (due to Exercise 20 (b)), but also in some other cases; for example, the 4-cycle $\text{cyc}_{1,3,4,2}$ in $S_4$ has length 3.

Remark 5.33. The main reason why cycles are useful is that, essentially, every permutation can be “decomposed” into cycles. We shall not use this fact, but since it is generally important, let us briefly explain what it means. (You will probably learn more about it in any standard course on abstract algebra.)

Fix $n \in \mathbb{N}$. Let $[n] = \{1, 2, \ldots, n\}$. Two cycles $\alpha$ and $\beta$ in $S_n$ are said to be disjoint if they can be written as $\alpha = \text{cyc}_{i_1, i_2, \ldots, i_k}$ and $\beta = \text{cyc}_{j_1, j_2, \ldots, j_\ell}$ for $k + \ell$ distinct elements $i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_\ell$ of $[n]$. For example, the two cycles $\text{cyc}_{1,3}$ and $\text{cyc}_{2,6,7}$ in $S_8$ are disjoint, but the two cycles $\text{cyc}_{1,4}$ and $\text{cyc}_{2,4}$ are not. It is easy to see that any two disjoint cycles $\alpha$ and $\beta$ commute (i.e., satisfy $\alpha \circ \beta = \beta \circ \alpha$). Therefore, when you see a composition $\alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_p$ of several pairwise disjoint cycles, you can reorder its factors arbitrarily without changing the result (for example, $\alpha_3 \circ \alpha_1 \circ \alpha_4 \circ \alpha_2 = \alpha_1 \circ \alpha_2 \circ \alpha_3 \circ \alpha_4$ if $p = 4$).

Now, the fact I am talking about says the following: Every permutation in $S_n$ can be written as a composition of several pairwise disjoint cycles. For example, let $n = 9$, and let $\sigma \in S_9$ be the permutation which is written $(4, 6, 1, 3, 5, 2, 9, 8, 7)$ in one-line notation (i.e., we have $\sigma(1) = 4, \sigma(2) = 6$, etc.). Then, $\sigma$ can be written as a composition of several pairwise disjoint cycles as follows:
\[
\sigma = \text{cyc}_{1,4,3} \circ \text{cyc}_{7,9} \circ \text{cyc}_{2,6}.
\]

Indeed, here is how such a decomposition can be found: Let us draw a directed graph whose vertices are 1, 2, $\ldots$, $n$, and which has an arc $i \to \sigma(i)$ for every $i \in [n]$. (Thus, it has $n$ arcs altogether; some of them can be loops.) For our
permutation $\sigma \in S_9$, this graph looks as follows:

![Graph](image)

Obviously, at each vertex $i$ of this graph, exactly one arc begins (namely, the arc $i \to \sigma(i)$). Moreover, since $\sigma$ is invertible, it is also clear that at each vertex $i$ of this graph, exactly one arc ends (namely, the arc $\sigma^{-1}(i) \to i$). Due to the way we constructed this graph, it is clear that it completely describes our permutation $\sigma$: Namely, if we want to find $\sigma(i)$ for a given $i \in [n]$, we should just locate the vertex $i$ on the graph, and follow the arc that begins at this vertex; the endpoint of this arc will be $\sigma(i)$.

Now, a look at this graph reveals five directed cycles (in the sense of “paths which end at the same vertex at which they begin”, not yet in the sense of “cyclic permutations”). The first one passes through the vertices 2 and 6; the second passes through the vertices 3, 1 and 4; the third, through the vertex 5 (it is what is called a “trivial cycle”), and so on. To each of these cycles we can assign a cyclic permutation in $S_n$: namely, if the cycle passes through the vertices $i_1, i_2, \ldots, i_k$ (in this order, and with no repetitions), then we assign to it the cyclic permutation $\text{cyc}_{i_1, i_2, \ldots, i_k} \in S_n$. The cyclic permutations assigned to all five directed cycles are pairwise disjoint, and their composition is

$$\text{cyc}_{2,6} \circ \text{cyc}_{3,1,4} \circ \text{cyc}_{5} \circ \text{cyc}_{7,9} \circ \text{cyc}_{8}.$$  

But this composition must be $\sigma$ (because if we apply this composition to an element $i \in [n]$, then we obtain the “next vertex after $i$” on the directed cycle which passes through $i$; but due to how we constructed our graph, this “next vertex” will be precisely $\sigma(i)$). Hence, we have

$$\sigma = \text{cyc}_{2,6} \circ \text{cyc}_{3,1,4} \circ \text{cyc}_{5} \circ \text{cyc}_{7,9} \circ \text{cyc}_{8}. \quad (122)$$

Thus, we have found a way to write $\sigma$ as a composition of several pairwise disjoint cycles. We can rewrite (and even simplify) this representation a bit: Namely, we can simplify (122) by removing the factors $\text{cyc}_{5}$ and $\text{cyc}_{8}$ (because both of these factors equal id); thus we obtain $\sigma = \text{cyc}_{2,6} \circ \text{cyc}_{3,1,4} \circ \text{cyc}_{7,9}$. We can furthermore switch $\text{cyc}_{2,6}$ with $\text{cyc}_{3,1,4}$ (since disjoint cycles commute), therefore obtaining $\sigma = \text{cyc}_{3,1,4} \circ \text{cyc}_{2,6} \circ \text{cyc}_{7,9}$. Next, we can switch $\text{cyc}_{2,6}$ with $\text{cyc}_{7,9}$,
obtaining $\sigma = \text{cyc}_{3,1,4} \circ \text{cyc}_{7,9} \circ \text{cyc}_{2,6}$. Finally, we can rewrite $\text{cyc}_{3,1,4}$ as $\text{cyc}_{1,4,3}$, and we obtain (120).

In general, for every $n \in \mathbb{N}$, every permutation $\sigma \in S_n$ can be represented as a composition of several pairwise disjoint cycles (which can be found by drawing a directed graph as in our example above). This representation is not literally unique, because we can modify it by:

- adding or removing trivial factors (i.e., factors of the form $\text{cyc}_i = \text{id}$);
- switching different cycles;
- rewriting $\text{cyc}_{i_1,i_2,\ldots,i_k}$ as $\text{cyc}_{i_2,i_3,\ldots,i_k,i_1}$.

However, it is unique up to these modifications; in other words, any two representations of $\sigma$ as a composition of several pairwise disjoint cycles can be transformed into one another by such modifications.

The proofs of all these statements are fairly easy. (One does have to check certain things, e.g., that the directed graph really consists of disjoint directed cycles.)

Representing a permutation $\sigma \in S_n$ as a composition of several pairwise disjoint cycles can be done very quickly, and thus gives a quick way to find $(-1)^\sigma$ (because Exercise 20(d) tells us how to find the sign of a $k$-cycle). This is significantly faster than counting inversions of $\sigma$.

### 5.8. Additional exercises

Permutations and symmetric groups are a staple of combinatorics; there are countless results involving them. For an example, Bóna’s book [Bona12], as well as significant parts of Stanley’s [Stan11] and [Stan01] are devoted to them. In this section, I shall only give a haphazard selection of exercises, which are not relevant to the rest of these notes (thus can be skipped at will). I am not planning to provide solutions for all of them.

**Additional exercise 14.** Let $n \in \mathbb{N}$. Let $d = \text{lcm}(1,2,\ldots,n)$.

(a) Show that $\pi^d = \text{id}$ for every $\pi \in S_n$.

(b) Let $k$ be an integer such that every $\pi \in S_n$ satisfies $\pi^k = \text{id}$. Show that $d \mid k$.

**Additional exercise 15.** Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\sigma \in S_n$ and $\tau \in S_m$. We define a permutation $\sigma \times \tau$ of the set $\{1,2,\ldots,n\} \times \{1,2,\ldots,m\}$ by setting

$$
(\sigma \times \tau)(a,b) = (\sigma(a),\tau(b)) \quad \text{for every } (a,b) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}.
$$

(a) Prove that $\sigma \times \tau$ is a well-defined permutation.

(b) Prove that $\sigma \times \tau = (\sigma \times \text{id}) \circ (\text{id} \times \tau)$. 
(c) According to Exercise 18 (applied to $X = \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$), the permutation $\sigma \times \tau$ has a well-defined sign $(-1)^{\sigma \times \tau}$. Prove that $(-1)^{\sigma \times \tau} = ((-1)^m)^{\sigma}((-1)^n)^{\tau}$.

The next two additional exercises concern the inversions of a permutation. They use the following definition:

**Definition 5.34.** Let $n \in \mathbb{N}$. For every $\sigma \in S_n$, we let $\text{Inv } \sigma$ denote the set of all inversions of $\sigma$.

Exercise 9 (c) shows that any $n \in \mathbb{N}$ and any two permutations $\sigma$ and $\tau$ in $S_n$ satisfy the inequality $\ell(\sigma \circ \tau) \leq \ell(\sigma) + \ell(\tau)$. In the following exercise, we will see when this inequality becomes an equality:

**Additional exercise 16.** Let $n \in \mathbb{N}$. Let $\sigma, \tau \in S_n$.

(a) Prove that $\ell(\sigma \circ \tau) = \ell(\sigma) + \ell(\tau)$ holds if and only if $\text{Inv } \tau \subseteq \text{Inv } (\sigma \circ \tau)$.

(b) Prove that $\ell(\sigma \circ \tau) = \ell(\sigma) + \ell(\tau)$ holds if and only if $\text{Inv } (\sigma^{-1}) \subseteq \text{Inv } (\tau^{-1} \circ \sigma^{-1})$.

(c) Prove that $\text{Inv } \sigma \subseteq \text{Inv } \tau$ holds if and only if $\ell(\tau) = \ell(\tau \circ \sigma^{-1}) + \ell(\sigma)$.

(d) Assume that $\text{Inv } \sigma = \text{Inv } \tau$. Prove that $\sigma = \tau$.

Additional exercise 16 (d) shows that if two permutations in $S_n$ have the same set of inversions, then they are equal. In other words, a permutation in $S_n$ is uniquely determined by its set of inversions. The next additional exercise shows what set of inversions a permutation can have:

**Additional exercise 17.** Let $n \in \mathbb{N}$. Let $G = \{(i, j) \in \mathbb{Z}^2 \mid 1 \leq i < j \leq n\}$.

A subset $U$ of $G$ is said to be transitive if every $a, b, c \in \{1, 2, \ldots, n\}$ satisfying $(a, b) \in U$ and $(b, c) \in U$ also satisfy $(a, c) \in U$.

A subset $U$ of $G$ is said to be inversive if there exists a $\sigma \in S_n$ such that $U = \text{Inv } \sigma$.

Let $U$ be a subset of $G$. Prove that $U$ is inversive if and only if both $U$ and $G \setminus U$ are transitive.

6. An introduction to determinants

In this chapter, we will define and study determinants in a combinatorial way (in the spirit of Hefferon’s book [Hefferon], Gill Williamson’s notes [Gill12 Chapter 3], Laue’s notes [Laue] and Zeilberger’s paper [Zeilbe]). Nowadays, students usually learn about determinants in the context of linear algebra, after having made

---

96My notes differ from these sources in the following:

- Hefferon’s book [Hefferon] is an introductory textbook for a first course in Linear Algebra, and so treats rather little of the theory of determinants (noticeably less than what we do). It is, however, a good introduction into the “other part” of linear algebra (i.e., the theory of
the acquaintance of vector spaces, matrices, linear transformations, Gaussian elimination etc.; this approach to determinants (which I like to call the “linear-algebraic approach”) has certain advantages and certain disadvantages to our combinatorial approach.97

We shall study determinants of matrices over commutative rings98. First, let us define what these words (“commutative ring”, “matrix” and “determinant”) mean.

### 6.1. Commutative rings

**Definition 6.1.** If $\mathbb{K}$ is a set, then a binary operation on $\mathbb{K}$ means a map from $\mathbb{K} \times \mathbb{K}$ to $\mathbb{K}$. (In other words, it means a function which takes two elements of $\mathbb{K}$ as input, and returns an element of $\mathbb{K}$ as output.) For instance, the map from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ which sends every pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ to $3a - b$ is a binary operation on $\mathbb{Z}$.

Sometimes, a binary operation $f$ on a set $\mathbb{K}$ will be written infix. This means that the image of $(a, b) \in \mathbb{K} \times \mathbb{K}$ under $f$ will be denoted by $af b$ instead of $f(a, b)$. For instance, the binary operation $+$ on the set $\mathbb{Z}$ (which sends a pair $(a, b)$ of integers to their sum $a + b$) is commonly written infix, because one writes $a + b$ and not $+(a, b)$ for the sum of $a$ and $b$.

**Definition 6.2.** A commutative ring means a set $\mathbb{K}$ endowed with

- two binary operations called “addition” and “multiplication”, and denoted by $+$ and $\cdot$, respectively, and both written infix99 and

...vector spaces and linear maps), and puts determinants into the context of that other part, which makes some of their properties appear less mysterious. (Like many introductory textbooks, it only discusses matrices over fields, not over commutative rings; it also uses more handwaving in the proofs.)

- Zeilberger’s paper [Zeilbe] mostly proves advanced results (apart from its Section 5, which proves our Theorem 6.22). I would recommend reading it after reading this chapter.

- Laue’s notes [Laue] are a brief introduction to determinants that prove the main results in just 14 pages (although at the cost of terser writing and stronger assumptions on the reader’s preknowledge). If you read these notes, make sure to pay attention to the “Prerequisites and some Terminology” section, as it explains the (unusual) notations used in these notes.

- Gill Williamson’s [Gill12, Chapter 3] probably comes the closest to what I am doing below (and is highly recommended, not least because it goes much further into various interesting directions!). My notes are more elementary and more detailed in what they do.

97Its main advantage is that it gives more motivation and context. However, the other (combinatorial) approach requires less preknowledge and involves less technical subtleties (for example, it defines the determinant directly by an explicit formula, while the linear-algebraic approach defines it implicitly by a list of conditions which happen to determine it uniquely), which is why I have chosen it. (Of course, it helped that the combinatorial approach is, well, combinatorial.)

98This is a rather general setup, which includes determinants of matrices with real entries, of matrices with complex entries, of matrices with polynomial entries, and many other situations. One benefit of working combinatorially is that studying determinants in this general setup is no more difficult than studying them in more restricted settings.
• two elements called $0_K$ and $1_K$

such that the following axioms are satisfied:

• **Commutativity of addition**: We have $a + b = b + a$ for all $a \in K$ and $b \in K$.

• **Commutativity of multiplication**: We have $ab = ba$ for all $a \in K$ and $b \in K$. Here and in the following, $ab$ is shorthand for $a \cdot b$ (as is usual for products of numbers).

• **Associativity of addition**: We have $a + (b + c) = (a + b) + c$ for all $a \in K$, $b \in K$ and $c \in K$.

• **Associativity of multiplication**: We have $a(bc) = (ab)c$ for all $a \in K$, $b \in K$ and $c \in K$.

• **Neutrality of 0**: We have $a + 0_K = 0_K + a = a$ for all $a \in K$.

• **Existence of additive inverses**: For every $a \in K$, there exists an element $a' \in K$ such that $a + a' = a' + a = 0_K$. This $a'$ is commonly denoted by $-a$ and called the additive inverse of $a$. (It is easy to check that it is unique.)

• **Unitality (a.k.a. neutrality of 1)**: We have $1_Ka = a1_K = a$ for all $a \in K$.

• **Annihilation**: We have $0_Ka = a0_K = 0_K$ for all $a \in K$.

• **Distributivity**: We have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a \in K$, $b \in K$ and $c \in K$.

(Some of these axioms are redundant, in the sense that they can be derived from others. For instance, the equality $(a + b)c = ac + bc$ can be derived from the axiom $a(b + c) = ab + ac$ using commutativity of multiplication. Also, annihilation follows from the other axioms\(^\text{100}\). The reasons why we have chosen these axioms and not fewer (or more, or others) are somewhat a matter of taste. For example,

\(^99\)i.e., we write $a + b$ for the image of $(a, b) \in K \times K$ under the binary operation called “addition”, and we write $a \cdot b$ for the image of $(a, b) \in K \times K$ under the binary operation called “multiplication”\(^1\)

\(^{100}\)In fact, let $a \in K$. Distributivity yields $(0_K + 0_K)a = 0_Ka + 0_Ka$, so that $0_Ka + 0_Ka = (0_K + 0_K)a = 0_Ka$. Adding $- (0_Ka)$ on the left, we obtain $- (0_Ka) + (0_Ka + 0_Ka) = 0_Ka = 0_Ka$ (by neutrality of $0_K$).

$- (0_Ka) = - (0_Ka) + 0_Ka = 0_K$ (by the definition of $- (0_Ka)$), and associativity of addition shows that $- (0_Ka) + (0_Ka + 0_Ka) = (0_Ka + 0_Ka) + 0_Ka = 0_K + 0_Ka = 0_Ka$ (by neutrality of $0_K$), so that $0_Ka = - (0_Ka) + (0_Ka + 0_Ka) = - (0_Ka) + 0_Ka = 0_K$. Thus, $0_Ka = 0_K$ is proven. Similarly one can show $a0_K = 0_K$. Therefore, annihilation follows from the other axioms.)
I like to explicitly require annihilation, because it is an important axiom in the definition of a semiring, where it no longer follows from the others.)

**Definition 6.3.** As we have seen in Definition 6.2, a commutative ring consists of a set \( K \), two binary operations on this set named \(+\) and \( \cdot \), and two elements of this set named \( 0 \) and \( 1 \). Thus, formally speaking, we should encode a commutative ring as the 5-tuple \( (K, +, \cdot, 0, 1) \). Sometimes we will actually do so; but most of the time, we will refer to the commutative ring just as the “commutative ring \( K \)”, hoping that the other four entries of the 5-tuple (namely, \(+\), \( \cdot \), \( 0 \) and \( 1 \)) are clear from the context. This kind of abbreviation is commonplace in mathematics; it is called “pars pro toto” (because we are referring to a large structure by the same symbol as for a small part of it, and hoping that the rest can be inferred from the context). It is an example of what is called “abuse of notation”.

The elements \( 0 \) and \( 1 \) of a commutative ring \( K \) are called the zero and the unity of \( K \). They are usually denoted by \( 0 \) and \( 1 \) (without the subscript \( K \) when this can cause no confusion (and, unfortunately, often also when it can). They are not always identical with the actual integers 0 and 1.

The binary operations \(+\) and \( \cdot \) in Definition 6.2 are also usually not identical with the binary operations \(+\) and \( \cdot \) on the set of integers, and are denoted by \(+_K\) and \( \cdot_K\) when confusion can arise.

The set \( K \) is called the underlying set of the commutative ring \( K \). Let us again remind ourselves that the underlying set of a commutative ring \( K \) is just a part of the data of \( K \).

Here are some examples and non-examples of rings:

- The sets \( \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \) (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) are commutative rings. (Notice that existence of multiplicative inverses is not required!)

- The set \( \mathbb{N} \) of nonnegative integers (again endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) is not a commutative ring. It fails the existence of additive inverses. (Of course, negative numbers exist, but this does not count because they don’t lie in \( \mathbb{N} \).

- We can define a commutative ring \( \mathbb{Z}' \) as follows: We define a binary operation \( \tilde{\times} \) on \( \mathbb{Z} \) (written infix) by
  \[
  (a \tilde{\times} b = -ab \quad \text{for all } (a, b) \in \mathbb{Z} \times \mathbb{Z} .
  \]

\( ^{101}\) Some people say “unit” instead of “unity”, but other people use the word “unit” for something different, which makes every use of this word a potential pitfall.

\( ^{102}\) The following list of examples is long, and some of these examples rely on knowledge that you might not have yet. As usual with examples, you need not understand them all. When I say that Laurent polynomial rings are examples of commutative rings, I do not assume that you know what Laurent polynomials are; I merely want to ensure that, if you have already encountered Laurent polynomials, then you get to know that they form a commutative ring.

---

101 Some people say “unit” instead of “unity”, but other people use the word “unit” for something different, which makes every use of this word a potential pitfall.

102 The following list of examples is long, and some of these examples rely on knowledge that you might not have yet. As usual with examples, you need not understand them all. When I say that Laurent polynomial rings are examples of commutative rings, I do not assume that you know what Laurent polynomials are; I merely want to ensure that, if you have already encountered Laurent polynomials, then you get to know that they form a commutative ring.
Now, let \( \mathbb{Z}' \) be the set \( \mathbb{Z} \), endowed with the usual addition \( + \) and the (unusual) multiplication \( \tilde{\times} \), with the zero \( 0_{\mathbb{Z}'} = 0 \) and with the unity \( 1_{\mathbb{Z}'} = -1 \). It is easy to check that \( \mathbb{Z}' \) is a commutative ring\(^{103}\); it is an example of a commutative ring whose unity is clearly not equal to the integer 1 (which is why it is important to never omit the subscript \( \mathbb{Z}' \) in \( 1_{\mathbb{Z}'} \) here).

That said, \( \mathbb{Z}' \) is not a very interesting ring: It is essentially “a copy of \( \mathbb{Z} \), except that every integer \( n \) has been renamed as \( -n \)”. To formalize this intuition, we would need to introduce the notion of a ring isomorphism, which we don’t want to do right here; but the idea is that the bijection \( \varphi : \mathbb{Z} \to \mathbb{Z}' \), \( n \mapsto -n \) satisfies

\[
\varphi (a + b) = \varphi (a) + \varphi (b) \quad \text{for all } (a, b) \in \mathbb{Z} \times \mathbb{Z};
\]
\[
\varphi (a \cdot b) = \varphi (a) \tilde{\times} \varphi (b) \quad \text{for all } (a, b) \in \mathbb{Z} \times \mathbb{Z};
\]
\[
\varphi (0) = 0_{\mathbb{Z}'};
\]
\[
\varphi (1) = 1_{\mathbb{Z}'};
\]

and thus the ring \( \mathbb{Z}' \) can be viewed as the ring \( \mathbb{Z} \) with its elements “relabeled” using this bijection.

- The polynomial rings \( \mathbb{Z}[x] \), \( \mathbb{Q}[a, b] \), \( \mathbb{C}[z_1, z_2, \ldots, z_n] \) are commutative rings. Laurent polynomial rings are also commutative rings. (Do not worry if you have not seen these rings yet.)

- The set of all functions \( \mathbb{Q} \to \mathbb{Q} \) is a commutative ring, where addition and multiplication are defined pointwise (i.e., addition is defined by \( (f + g) (x) = f(x) + g(x) \) for all \( x \in \mathbb{Q} \), and multiplication is defined by \( (fg) (x) = f(x) \cdot g(x) \) for all \( x \in \mathbb{Q} \)), where the zero is the “constant-0” function (sending every \( x \in \mathbb{Q} \) to 0), and where the unity is the “constant-1” function (sending every \( x \in \mathbb{Q} \) to 1). Of course, the same construction works if we consider functions \( \mathbb{R} \to \mathbb{C} \), or functions \( \mathbb{C} \to \mathbb{Q} \), or functions \( \mathbb{N} \to \mathbb{Q} \), instead of functions \( \mathbb{Q} \to \mathbb{Q} \). \(^{104}\)

- The set \( S \) of all real numbers of the form \( a + b \sqrt{5} \) with \( a, b \in \mathbb{Q} \) (endowed with the usual notions of “addition” and “multiplication” defined on \( \mathbb{R} \)) is a commutative ring\(^{105}\).

\(^{103}\) Notice that we have named this new commutative ring \( \mathbb{Z}' \), not \( \mathbb{Z} \) (despite having \( \mathbb{Z}' = \mathbb{Z} \) as sets). The reason is that if we had named it \( \mathbb{Z} \), then we could no longer speak of “the commutative ring \( \mathbb{Z} \)” without being ambiguous (we would have to specify every time whether we mean the usual multiplication or the unusual one).

\(^{104}\) But not if we consider functions \( \mathbb{Q} \to \mathbb{N} \); such functions might fail the existence of additive inverses.

Generally, if \( X \) is any set and \( K \) is any commutative ring, then the set of all functions \( X \to K \) is a commutative ring, where addition and multiplication are defined pointwise, where the zero is the “constant-0\(_K\)” function, and where the unity is the “constant-1\(_K\)” function.

\(^{105}\) To prove this, we argue as follows:
• We could define a different ring structure on the set \( S \) (that is, a commutative ring which, as a set, is identical with \( S \), but has a different choice of operations) as follows: We define a binary operation \( * \) on \( S \) by setting

\[
(a + b\sqrt{5}) \ast (c + d\sqrt{5}) = ac + bd\sqrt{5} \quad \text{for all } (a, b) \in \mathbb{Q} \times \mathbb{Q}.
\]

Now, let \( S' \) be the set \( S \), endowed with the usual addition + and the (unusual) multiplication \( \ast \), with the zero \( 0_{S'} = 0 \) and with the unity \( 1_{S'} = 1 + \sqrt{5} \) (not the integer 1). It is easy to check that \( S' \) is a commutative ring. The sets \( S \) and \( S' \) are identical, but the commutative rings \( S \) and \( S' \) are not. For example, the ring \( S' \) has two nonzero elements whose product is 0 (namely, \( 1 \ast \sqrt{5} = 0 \)), whereas the ring \( S \) has no such things. This shows that not only do we have \( S' \neq S \) as commutative rings, but there is also no way to regard \( S' \) as “a copy of \( S \) with its elements renamed” (in the same way as we have regarded \( \mathbb{Z}' \) as “a copy of \( \mathbb{Z} \) with its elements renamed”). This example should stress the point that a commutative ring \( K \) is not just a set; it is a set endowed with two operations (+ and \( \cdot \)) and two elements (0\(_{K}\) and 1\(_{K}\)), and these operations and elements are no less important than the set.

• The set \( S_3 \) of all real numbers of the form \( a + b\sqrt{5} \) with \( a, b \in \mathbb{Q} \) (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) is not a commutative ring. Indeed, multiplication is not a binary operation on this set \( S_3 \): It does not always send two elements of \( S_3 \) to an element of \( S_3 \).

For instance, \( (1 + 1\sqrt{5}) (1 + 1\sqrt{5}) = 1 + 2\sqrt{5} + \left(\sqrt{5}\right)^2 \) is not in \( S_3 \).

• The set of all \( 2 \times 2 \)-matrices over \( \mathbb{Q} \) is not a commutative ring, because commutativity of multiplication does not hold for this set. (In general, \( AB \neq BA \) for matrices.)

• If you like the empty set, you will enjoy the zero ring. This is the commutative ring which is defined as the one-element set \{0\}, with zero and unity both

---

106 This is well-defined, because every element of \( S \) can be written in the form \( a + b\sqrt{5} \) for a unique pair \((a, b) \in \mathbb{Q} \times \mathbb{Q} \). This is a consequence of the irrationality of \( \sqrt{5} \).

107 Again, we do not call it \( S \), in order to be able to distinguish between different ring structures.

108 Keep in mind that, due to our “pars pro toto” notation, “commutative ring \( S \)” means more than “set \( S \)”.

---
being 0 (nobody said that they have to be distinct!), with addition given by \( 0 + 0 = 0 \) and with multiplication given by \( 0 \cdot 0 = 0 \). Of course, it is not an empty set \(^{109}\) but it plays a similar role in the world of commutative rings as the empty set does in the world of sets: It carries no information itself, but things would break if it were to be excluded \(^{110}\).

Notice that the zero and the unity of the zero ring are identical, i.e., we have \( 0_K = 1_K \). This shows why it is dangerous to omit the subscripts and just denote the zero and the unity by 0 and 1; in fact, you don’t want to rewrite the equality \( 0_K = 1_K \) as “0 = 1”! (Most algebraists make a compromise between wanting to omit the subscripts and having to clarify what 0 and 1 mean: They say that “0 = 1 in \( K \)” to mean “0\_K = 1\_K”.)

Generally, a trivial ring is defined to be a commutative ring containing only one element (which then necessarily is both the zero and the unity of this ring). The addition and the multiplication of a trivial ring are uniquely determined (since there is only one possible value that a sum or a product could take). Every trivial ring can be viewed as the zero ring with its element 0 relabelled \(^{111}\).

- In set theory, the symmetric difference of two sets \( A \) and \( B \) is defined to be the set \( (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) \). This symmetric difference is denoted by \( A \triangle B \). Now, let \( S \) be any set. Let \( 2^S \) denote the powerset of \( S \) (that is, the set of all subsets of \( S \)). It is easy to check that the following ten properties hold:

\[
\begin{align*}
A \triangle B &= B \triangle A & \text{for any sets } A \text{ and } B; \\
A \cap B &= B \cap A & \text{for any sets } A \text{ and } B; \\
(A \triangle B) \triangle C &= A \triangle (B \triangle C) & \text{for any sets } A, B \text{ and } C; \\
(A \cap B) \cap C &= A \cap (B \cap C) & \text{for any sets } A, B \text{ and } C; \\
A \triangle \emptyset &= \emptyset \triangle A = A & \text{for any set } A; \\
A \cap S &= S \cap A = A & \text{for any subset } A \text{ of } S; \\
\emptyset \cap A &= A \cap \emptyset = \emptyset & \text{for any set } A; \\
A \cap (B \triangle C) &= (A \cap B) \triangle (A \cap C) & \text{for any sets } A, B \text{ and } C; \\
(A \triangle B) \cap C &= (A \cap C) \triangle (B \cap C) & \text{for any sets } A, B \text{ and } C.
\end{align*}
\]

Therefore, \( 2^S \) becomes a commutative ring, where the addition is defined to be the operation \( \triangle \), the multiplication is defined to be the operation \( \cap \), the

\(^{109}\) A commutative ring cannot be empty, as it contains at least one element (namely, 0).

\(^{110}\) Some authors do prohibit the zero ring from being a commutative ring (by requiring every commutative ring to satisfy \( 0 \neq 1 \)). I think most of them run into difficulties from this decision sooner or later.

\(^{111}\) In more formal terms, the preceding statement would say that “every trivial ring is isomorphic to the zero ring”.

---
zero is defined to be the set $\varnothing$, and the unity is defined to be the set $S$.  

The commutative ring $2^S$ has the property that $a^2 = a$ for every $a \in 2^S$. (This simply means that $A \cap A = A$ for every $A \subseteq S$.) Commutative rings that have this property are called \textit{Boolean rings}. (Of course, $2^S$ is the eponymic example for a Boolean ring; but there are also others.)

- For every positive integer $n$, the residue classes of integers modulo $n$ form a commutative ring, which is called $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ (depending on the author). This ring has $n$ elements (often called “integers modulo $n$”). When $n$ is a composite number (e.g., $n = 6$), this ring has the property that products of nonzero \textit{elements} can be zero (e.g., we have $2 \cdot 3 \equiv 0 \mod 6$); this means that there is no way to define division by all nonzero elements in this ring (even if we are allowed to create fractions). Notice that $\mathbb{Z}/1\mathbb{Z}$ is a trivial ring.

We notice that if $n$ is a positive integer, and if $K$ is the commutative ring $\mathbb{Z}/n\mathbb{Z}$, then $1_K + 1_K + \ldots + 1_K = 0_K$ (because the left hand side of this equality is the residue class of $n$ modulo $n$, while the right hand side is the residue class of 0 modulo $n$, and these two residue classes are clearly equal).

- Let us try to define “division by zero”. So, we introduce a new symbol $\infty$, and we try to extend the addition on $\mathbb{Q}$ to the set $\mathbb{Q} \cup \{\infty\}$ by setting $a + \infty = \infty$ for all $a \in \mathbb{Q} \cup \{\infty\}$. We might also try to extend the multiplication in some way, and perhaps to add some more elements (such as another symbol $-\infty$ to serve as the product $(-1)\infty$). I claim that (whatever we do with the multiplication, and whatever new elements we add) we do not get a commutative ring. Indeed, assume the contrary. Thus, there exists a commutative ring $W$ which contains $\mathbb{Q} \cup \{\infty\}$ as a subset, and which has $a + \infty = \infty$ for all $a \in \mathbb{Q}$. Thus, in $W$, we have $1 + \infty = \infty = 0 + \infty$. Adding $(-1)\infty$ to both sides of this equality, we obtain $1 + \infty + (-1)\infty = 0 + \infty + (-1)\infty$, so that $1 = 0$, but this is absurd. Hence, we have found a contradiction. This is why “division by zero is impossible”: One can define objects that behave like “infinity” (and they are useful), but they break various standard rules such as the axioms of a commutative ring. In contrast to this, adding a “number” $i$ satisfying $i^2 = -1$ to the real numbers is harmless: The complex numbers $\mathbb{C}$ are still a commutative ring.

\begin{itemize}
    \item The ten properties listed above show that the axioms of a commutative ring are satisfied for $(2^S, \triangle, \cap, \varnothing, S)$. In particular, the sixth property shows that every subset $A$ of $S$ has an additive inverse – namely, itself. Of course, it is unusual for an element of a commutative ring to be its own additive inverse, but in this example it happens all the time!
    \item An element $a$ of a commutative ring $K$ is said to be \textit{nonzero} if $a \neq 0_K$. (This is not the same as saying that $a$ is not the integer 0, because the integer 0 might not be $0_K$.)
    \item because $\infty + (-1)\infty = 1\infty + (-1)\infty = (1 + (-1))\infty = 0\infty = 0$
\end{itemize}
Here is an “almost-ring” beloved to many combinatorialists: The max-plus semiring $\mathbb{T}$ (also called the tropical semiring\footnote{Caution: Both of these names mean many other things as well.}). We create a new symbol $-\infty$, and we set $\mathbb{T} = \mathbb{Z} \cup \{-\infty\}$ as sets, but we do not “inherit” the addition and the multiplication from $\mathbb{Z}$. Instead, we denote the “addition” and “multiplication” operations on $\mathbb{Z}$ by $+_\mathbb{Z}$ and $\cdot_{\mathbb{Z}}$, and we define two new “addition” and “multiplication” operations $+_\mathbb{T}$ and $\cdot_{\mathbb{T}}$ on $\mathbb{T}$ as follows:

$$a +_\mathbb{T} b = \max\{a, b\};$$
$$a \cdot_{\mathbb{T}} b = a +_\mathbb{Z} b.$$

(Here, we set $\max\{-\infty, n\} = \max\{n, -\infty\} = n$ and $(-\infty) +_\mathbb{Z} n = n +_\mathbb{Z} (-\infty) = -\infty$ for every $n \in \mathbb{T}$.)

It turns out that the set $\mathbb{T}$ endowed with the two operations $+_\mathbb{Z}$ and $\cdot_{\mathbb{Z}}$, the zero $0_\mathbb{T} = -\infty$ and the unity $1_\mathbb{T} = 0$ comes rather close to being a commutative ring. It satisfies all axioms of a commutative ring except for the existence of additive inverses. Such a structure is called a \textit{semiring}. Other examples of semirings are $\mathbb{N}$ and a reasonably defined $\mathbb{N} \cup \{\infty\}$ (with $0\infty = 0$ and $a\infty = \infty$ for all $a > 0$).

If $\mathbb{K}$ is a commutative ring, then we can define a subtraction in $\mathbb{K}$, even though we have not required a subtraction operation as part of the definition of a commutative ring $\mathbb{K}$. Namely, the subtraction of a commutative ring $\mathbb{K}$ is the binary operation $-\in\mathbb{K}$ (again written infix) defined as follows: For every $a \in \mathbb{K}$ and $b \in \mathbb{K}$, set $a - b = a + b'$, where $b'$ is the additive inverse of $b$. It is not hard to check that $a - b$ is the unique element $c$ of $\mathbb{K}$ satisfying $a = b + c$; thus, subtraction is “the undoing of addition” just as in the classical situation of integers. Again, the notation $-$ for the subtraction of $\mathbb{K}$ is denoted by $-\mathbb{K}$ whenever a confusion with the subtraction of integers could arise.

Whenever $a$ is an element of a commutative ring $\mathbb{K}$, we write $-a$ for the additive inverse of $a$. This is the same as $0_\mathbb{K} - a$.

The intuition for commutative rings is essentially that all computations that can be made with the operations $+$, $-$ and $\cdot$ on integers can be similarly made in a commutative ring. For instance, if $a_1, a_2, \ldots, a_n$ are $n$ elements of a commutative ring, then the sum $a_1 + a_2 + \cdots + a_n$ is well-defined, and can be computed by adding the elements $a_1, a_2, \ldots, a_n$ to each other in any order\footnote{For instance, we can compute the sum $a + b + c + d$ of four elements $a, b, c, d$ in many ways: For example, we can first add $a$ and $b$, then add $c$ and $d$, and finally add the two results; alternatively, we can first add $a$ and $b$, then add $c$ to the result, then finally add $d$ to the result. In a commutative ring, all such ways lead to the same result. To prove this is a slightly tedious induction argument that uses commutativity and associativity.}. The same holds for products. If $n$ is an integer and $a$ is an element of a commutative ring $\mathbb{K}$, then we
define an element $na$ of $\mathbb{K}$ by

$$na = \begin{cases} a + a + \cdots + a, & \text{if } n \geq 0; \\ -a + a + \cdots + a, & \text{if } n < 0. \end{cases}$$

If $n$ is a nonnegative integer and $a$ is an element of a commutative ring $\mathbb{K}$, then $a^n$ is a well-defined element of $\mathbb{K}$ (namely, $a^n = a \cdot a \cdot \cdots \cdot a$). The following identities hold:

1. $- (a + b) = (-a) + (-b)$ for $a, b \in \mathbb{K}$; (123)
2. $- (-a) = a$ for $a \in \mathbb{K}$; (124)
3. $- (ab) = (-a) b = a (-b)$ for $a, b \in \mathbb{K}$; (125)
4. $- (na) = (-n) a = n (-a)$ for $a \in \mathbb{K}$ and $n \in \mathbb{Z}$; (126)
5. $n (ab) = (na) b = a (nb)$ for $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$; (127)
6. $(nm) a = n (ma)$ for $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$; (128)
7. $0^n = \begin{cases} 0, & \text{if } n > 0; \\ 1, & \text{if } n = 0 \end{cases}$ for $n \in \mathbb{N}$; (129)
8. $a^{n+m} = a^n a^m$ for $a \in \mathbb{K}$ and $n, m \in \mathbb{N}$; (130)
9. $(ab)^n = a^n b^n$ for $a, b \in \mathbb{K}$ and $n \in \mathbb{N}$; (131)
10. $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ for $a, b \in \mathbb{K}$ and $n \in \mathbb{N}$. (132)

Here, we are using the standard notations $+$, $\cdot$, $0$ and $1$ for the addition, the multiplication, the zero and the unity of $\mathbb{K}$, because confusion (e.g., confusion of the 0 with the integer 0) is rather unlikely. We shall keep doing so in the following, apart from situations where confusion can realistically occur.

\[\text{[117]}\]

Notice that this definition of $na$ is not a particular case of the product of two elements of $\mathbb{K}$, because $n$ is not an element of $\mathbb{K}$.

\[\text{[118]}\]

For instance, in the statement “$- (a + b) = (-a) + (-b)$ for $a, b \in \mathbb{K}$”, it is clear that the $+$ can only stand for the addition of $\mathbb{K}$ and not (say) for the addition of integers (since $a, b, -a$ and $-b$ are elements of $\mathbb{K}$, not (generally) integers). The only statement whose meaning is ambiguous is “$0^n$ for $n \in \mathbb{N}$”. In this statement, the “0” in “$n > 0$” and the “0” in “$n = 0$” clearly mean the integer 0 (since they are being compared with the integer $n$), but the other two appearances of “0” and the “1” are ambiguous. I hope that the context makes it clear enough that they mean the zero and the unity of $\mathbb{K}$ (and not the integers 0 and 1).

\[\text{[119]}\]

Notice that the equalities (127) and (128) are not particular cases of the associativity of multiplication which we required to hold for $\mathbb{K}$. Indeed, the latter associativity says that $a (bc) = (ab) c$ for all $a \in \mathbb{K}$, $b \in \mathbb{K}$ and $c \in \mathbb{K}$. But in (127) and (128), the $n$ is an integer, not an element of $\mathbb{K}$.
Furthermore, finite sums such as \( \sum_{s \in S} a_s \) (where \( S \) is a finite set, and \( a_s \in K \) for every \( s \in S \)), and finite products such as \( \prod_{s \in S} a_s \) (where \( S \) is a finite set, and \( a_s \in K \) for every \( s \in S \)) are defined whenever \( K \) is a commutative ring. Again, the definition is the same as for numbers, and these sums and products behave as they do for numbers. For example, Exercise [19] still holds if we replace “\( C \)” by “\( K \)” in it (and the same solution proves it) whenever \( K \) is a commutative ring.

**Remark 6.4.** The notion of a “commutative ring” is not fully standardized; there exist several competing definitions:

For some people, a “commutative ring” is *not* endowed with an element 1 (although it *can* have such an element), and, consequently, does not have to satisfy the unitality axiom. According to their definition, for example, the set \( \{0, 2, 4, 6, \ldots\} = \{2n \mid n \in \mathbb{N}\} \) is a commutative ring (with the usual addition and multiplication). (In contrast, our definition of a “commutative ring” does not accept \( \{0, 2, 4, 6, \ldots\} \) as a commutative ring, because it does not contain any element which would fill the role of 1.) These people tend to use the notation “commutative ring with unity” (or “commutative ring with 1”) to mean a commutative ring which is endowed with a 1 and satisfies the unitality axiom (i.e., what we call a “commutative ring”).

On the other hand, there are authors who use the word “ring” for what we call “commutative ring”. These are mostly the authors who work with commutative rings all the time and find the name “commutative ring” too long.

When you are reading about rings, it is important to know which meaning of “ring” the author is subscribing to. (Often this can be inferred from the examples given.)

### 6.2. Matrices

We have briefly defined determinants in Definition 5.13, but we haven’t done much with them. This will be amended now. But let us first recall the definitions of basic notions in matrix algebra.

In the following, we fix a commutative ring \( K \). The elements of \( K \) will be called *scalars* (to distinguish them from *vectors* and *matrices*, which we will soon discuss, and which are structures containing several elements of \( K \)).

If you feel uncomfortable with commutative rings, you are free to think that \( K = \mathbb{Q} \) or \( K = \mathbb{C} \) in the following; but everything I am doing works for any commutative ring unless stated otherwise.

Given two nonnegative integers \( n \) and \( m \), an \( n \times m \)-matrix (or, more precisely, \( n \times m \)-matrix over \( K \)) means a rectangular table with \( n \) rows and \( m \) columns whose entries are elements of \( K \).  

Formally speaking, this means that an \( n \times m \)-matrix is a map from \( \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\} \) to
is a $2 \times 3$-matrix. A matrix simply means an $n \times m$-matrix for some $n \in \mathbb{N}$ and $m \in \mathbb{N}$. These $n$ and $m$ are said to be the dimensions of the matrix.

If $A$ is an $n \times m$-matrix, and if $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$, then the $(i, j)$-th entry of $A$ means the entry of $A$ in row $i$ and column $j$. For instance, the $(1, 2)$-th entry of the matrix $egin{pmatrix} 1 & -2/5 & 4 \\ 1/3 & -1/2 & 0 \end{pmatrix}$ is $-2/5$.

If $n \in \mathbb{N}$ and $m \in \mathbb{N}$, and if we are given an element $a_{ij} \in \mathbb{K}$ for every $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$, then we use the notation $(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ for the $n \times m$-matrix whose $(i, j)$-th entry is $a_{ij}$ for all $(i, j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$. Thus,

$$(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}.$$  

The letters $i$ and $j$ are not set in stone; they are bound variables like the $k$ in “$\sum_{k=1}^{n} k$”. Thus, you are free to write $(a_{x,y})_{1 \leq x \leq n, 1 \leq y \leq m}$ or $(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ instead of $(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ (and we will use this freedom eventually).  

Matrices can be added if they share the same dimensions: If $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ and $B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ are two $n \times m$-matrices, then $A + B$ means the $n \times m$-matrix $(a_{ij} + b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$. Thus, matrices are added “entry by entry”; for example,  

$$(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} + \begin{pmatrix} a' & b' & c' \\ d' & e' & f' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' & c + c' \\ d + d' & e + e' & f + f' \end{pmatrix}. $$

Similarly, subtraction is defined: If $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ and $B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$, then $A - B = (a_{ij} - b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$.

Similarly, one can define the product of a scalar $\lambda \in \mathbb{K}$ with a matrix $A$: If $\lambda \in \mathbb{K}$ is a scalar, and if $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ is an $n \times m$-matrix, then $\lambda A$ means the $n \times m$-matrix $(\lambda a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$.

Defining the product of two matrices is trickier. Matrices are not multiplied “entry by entry”; this would not be a very interesting definition. Instead, their product is defined as follows: If $n$, $m$ and $\ell$ are three nonnegative integers, then the product $AB$ of an $n \times m$-matrix $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ with an $m \times \ell$-matrix

---

121 Many authors love to abbreviate “$a_{i,j}$” by “$a_{ij}$” (hoping that the reader will not mistake the subscript “$ij$” for a product or (in the case where $i$ and $j$ are single-digit numbers) for a two-digit number). The only advantage of this abbreviation that I am aware of is that it saves you a comma; I do not understand why it is so popular. But you should be aware of it in case you are reading other texts.
B = (b_{ij})_{1 \leq i \leq m, 1 \leq j \leq \ell} means the n × \ell-matrix

\[
\left( \sum_{k=1}^{m} a_{i,k} b_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq \ell}.
\]

This definition looks somewhat counterintuitive, so let me comment on it. First of all, for AB to be defined, A and B are not required to have the same dimensions; instead, A must have as many columns as B has rows. The resulting matrix AB then has as many rows as A and as many columns as B. Every entry of AB is a sum of products of an entry of A with an entry of B (not a single such product).

More precisely, the (i,j)-th entry of AB is a sum of products of an entry in the i-th row of A with the respective entry in the j-th column of B. For example,

\[
\begin{pmatrix}
  a & b & c \\
  d & e & f \\
\end{pmatrix}
\begin{pmatrix}
  a' & d' & g' \\
  b' & e' & h' \\
  c' & f' & i' \\
\end{pmatrix}
= 
\begin{pmatrix}
  aa' + bb' + cc' & ad' + be' + cf' & ag' + bh' + ci' \\
  da' + eb' + fc' & dd' + ee' + ff' & dg' + eh' + fi' \\
\end{pmatrix}.
\]

The multiplication of matrices is not commutative! It is easy to find examples of two matrices A and B for which the products AB and BA are distinct, or one of them is well-defined but the other is not.

For every \( n \in \mathbb{N} \), we let \( I_n \) denote the \( n \times n \)-matrix \((\delta_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}\), where \( \delta_{ij} \) is defined to be

\[
\begin{cases}
  1, & \text{if } i = j; \\
  0, & \text{if } i \neq j.
\end{cases}
\]

This matrix \( I_n \) looks as follows:

\[
I_n = \begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1
\end{pmatrix}.
\]

It has the property that \( I_n B = B \) for every \( m \in \mathbb{N} \) and every \( n \times m \)-matrix B; also, \( A I_n = A \) for every \( k \in \mathbb{N} \) and every \( k \times n \)-matrix A. (Proving this is a good way to check that you understand how matrices are multiplied.) The matrix \( I_n \) is called the \( n \times n \) identity matrix. (Some call it \( E_n \) or just I, when the value of \( n \) is clear from the context.)

Matrix multiplication is associative: If \( n, m, k, \ell \in \mathbb{N} \), and if A is an \( n \times m \)-matrix, B is an \( m \times k \)-matrix, and C is a \( k \times \ell \)-matrix, then \( A (BC) = (AB) C \). The proof of this is straightforward using our definition of products of matrices.

122This happens if A has as many columns as B has rows, but B does not have as many columns as A has rows.

123Here, 0 and 1 mean the zero and the unity of \( K \) (which may and may not be the integers 0 and 1).

124Check that \( A (BC) \) and \( (AB) C \) both are equal to the matrix \( \left( \sum_{u=1}^{m} \sum_{v=1}^{k} a_{i,u} b_{u,v} c_{v,j} \right)_{1 \leq i \leq n, 1 \leq j \leq \ell} \).
associativity allows us to write products like $ABC$ without parentheses. By induction, we can see that longer products such as $A_1A_2\cdots A_k$ for arbitrary $k \in \mathbb{N}$ can also be bracketed at will, because all bracketings lead to the same result (e.g., for four matrices $A$, $B$, $C$ and $D$, we have $A(B(CD)) = A((BC)D) = (AB)(CD) = (A(BC))D = ((AB)C)D$, provided that the dimensions of the matrices are appropriate to make sense of the products). We define an empty product of $n \times n$-matrices to be the $n \times n$ identity matrix $I_n$.

For every $n \times n$-matrix $A$ and every $k \in \mathbb{N}$, we can thus define an $n \times n$-matrix $A^k$ by $A^k = A\underbrace{A\cdots A}_k$. In particular, $A^0 = I_n$ (since we defined an empty product of $k$ factors of $n \times n$-matrices to be $I_n$).

Further properties of matrix multiplication are easy to state and to prove:

- For every $n \in \mathbb{N}$, $m \in \mathbb{N}$, $k \in \mathbb{N}$ and $\lambda \in \mathbb{K}$, every $n \times m$-matrix $A$ and every $m \times k$-matrix $B$, we have $\lambda (AB) = (\lambda A)B = A(\lambda B)$. (This allows us to write $\lambda AB$ for each of the matrices $\lambda (AB)$, $(\lambda A)B$ and $A(\lambda B)$.)
- For every $n \in \mathbb{N}$, $m \in \mathbb{N}$ and $k \in \mathbb{N}$, every two $n \times m$-matrices $A$ and $B$, and every $m \times k$-matrix $C$, we have $(A + B)C = AC + BC$.
- For every $n \in \mathbb{N}$, $m \in \mathbb{N}$ and $k \in \mathbb{N}$, every $n \times m$-matrix $A$, and every two $m \times k$-matrices $B$ and $C$, we have $A(B + C) = AB + AC$.
- For every $n \in \mathbb{N}$, $m \in \mathbb{N}$, $\lambda \in \mathbb{K}$ and $\mu \in \mathbb{K}$, and every $n \times m$-matrix $A$, we have $\lambda (\mu A) = (\lambda \mu)A$. (This allows us to write $\lambda \mu A$ for both $\lambda (\mu A)$ and $(\lambda \mu)A$.)

For given $n \in \mathbb{N}$ and $m \in \mathbb{N}$, we let $\mathbb{K}^{n \times m}$ denote the set of all $n \times m$-matrices. (This is one of the two standard notations for this set; the other is $M_{n,m}(\mathbb{K})$.

For given $n \in \mathbb{N}$ and $m \in \mathbb{N}$, we define the $n \times m$ zero matrix to be the $n \times m$-matrix whose all entries are $0$ (that is, the $n \times m$-matrix $(0)_{1 \leq i \leq n, 1 \leq j \leq m}$). We denote this matrix by $0_{n \times m}$. If $A$ is any $n \times m$-matrix, then the $n \times m$-matrix $-A$ is defined to be $0_{n \times m} - A$.

A square matrix is a matrix which has as many rows as it has columns; in other words, a square matrix is an $n \times n$-matrix for some $n \in \mathbb{N}$. If $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ is a square matrix, then the $n$-tuple $(a_{1,1}, a_{2,2}, \ldots, a_{n,n})$ is called the diagonal of $A$. (Some authors abbreviate $(a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ by $(a_{i,j})_{1 \leq i,j \leq n'}$; this notation has some mild potential for confusion, though.) The entries of the diagonal of $A$ are called the diagonal entries of $A$.

For a given $n \in \mathbb{N}$, the product of two $n \times n$-matrices is always well-defined, and is an $n \times n$-matrix again. The set $\mathbb{K}^{n \times n}$ satisfies all the axioms of a commutative ring except for commutativity of multiplication. This makes it into what is commonly

---

125The comma between “$i$” and “$j$” in “$1 \leq i, j \leq n$” can be understood either to separate $i$ from $j$, or to separate the inequality $1 \leq i$ from the inequality $j \leq n$. I remember seeing this ambiguity causing a real misunderstanding.
called a noncommutative ring. We shall study noncommutative rings later (in Section 6.15).

### 6.3. Determinants

Square matrices have determinants. Let us recall how determinants are defined:

**Definition 6.5.** Let $n \in \mathbb{N}$. Let $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ be an $n \times n$-matrix. The determinant $\det A$ of $A$ is defined as

$$
\sum_{\sigma \in S_n} (-1)^\sigma a_{1,\sigma(1)}a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.
$$

(133)

In other words,

$$
\det A = \sum_{\sigma \in S_n} (-1)^\sigma a_{1,\sigma(1)}a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}
$$

(134)

$$
= \prod_{i=1}^{n} a_{i,\sigma(i)}
$$

(135)

For example, the determinant of a $1 \times 1$ matrix $(a_{1,1})$ is

$$
\det (a_{1,1}) = \sum_{\sigma \in S_1} (-1)^\sigma a_{1,\sigma(1)} = (-1)^{\text{id}} a_{1,1}
$$

since the only permutation $\sigma \in S_1$ is $\text{id}$

$$
= a_{1,1}.
$$

(136)

---

126 A noncommutative ring is defined in the same way as we defined a commutative ring, except for the fact that commutativity of multiplication is removed from the list of axioms. (The words “noncommutative ring” do not imply that commutativity of multiplication must be false for this ring; they merely say that commutativity of multiplication is not required to hold for it. For example, the noncommutative ring $\mathbb{K}^{n \times n}$ is actually commutative when $n \leq 1$ or when $\mathbb{K}$ is a trivial ring.)

Instead of saying “noncommutative ring”, many algebraists just say “ring”. We shall, however, keep the word “noncommutative” in order to avoid confusion.
The determinant of a $2 \times 2$ matrix \[
\begin{pmatrix}
a_{1,1} & a_{1,2} \\
a_{2,1} & a_{2,2}
\end{pmatrix}
\] is
\[
\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = \sum_{\sigma \in S_2} (-1)^\sigma a_{1,\sigma(1)} a_{2,\sigma(2)}
\]
\[
= (-1)^{id} a_{1,id(1)} a_{2,id(2)} + (-1)^{s_1} a_{1,s_1(1)} a_{2,s_1(2)}
\]
\[
= a_{1,1} a_{2,2} - a_{1,2} a_{2,1}.
\]

Similarly, for a $3 \times 3$-matrix, the formula is
\[
\det \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} = a_{1,1} a_{2,2} a_{3,3} + a_{1,2} a_{2,3} a_{3,1} + a_{1,3} a_{2,1} a_{3,2} - a_{1,1} a_{2,3} a_{3,2} - a_{1,2} a_{2,1} a_{3,3} - a_{1,3} a_{2,2} a_{3,1}.
\]

Also, the determinant of the $0 \times 0$-matrix is $1$ \[^{127}\] (This might sound like hair-splitting, but being able to work with $0 \times 0$-matrices simplifies some proofs by induction, because it allows one to take $n = 0$ as an induction base.)

The equality (135) (or, equivalently, (134)) is known as the Leibniz formula. Out of several known ways to define the determinant, it is probably the most direct. In practice, however, computing a determinant using (135) quickly becomes impractical when $n$ is high (since the sum has $n!$ terms). In most situations that occur both in mathematics and in applications, determinants can be computed in various simpler ways.

Some authors write $|A|$ instead of $\det A$ for the determinant of a square matrix $A$. I do not like this notation, as it clashes (in the case of $1 \times 1$-matrices) with the notation $|a|$ for the absolute value of a real number $a$.

Here is a first example of a determinant which ends up very simple:

\[^{127}\]In more details:

There is only one $0 \times 0$-matrix; it has no rows and no columns and no entries. According to (135), its determinant is
\[
\sum_{\sigma \in S_0} (-1)^{\sigma} \prod_{i=1}^{0} a_{i,\sigma(i)} = \sum_{\sigma \in S_0} (-1)^{\sigma} = (-1)^{id} = 1
\]
(since the only $\sigma \in S_0$ is id)
Example 6.6. Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( K \), and let \( y_1, y_2, \ldots, y_n \) be \( n \) further elements of \( K \). Let \( A \) be the \( n \times n \)-matrix \( (x_i y_j)_{1 \leq i, j \leq n} \). What is \( \det A \)?

For \( n = 0 \), we have \( \det A = 1 \) (since the \( 0 \times 0 \)-matrix has determinant 1).

For \( n = 1 \), we have \( A = \begin{pmatrix} x_1 y_1 \end{pmatrix} \) and thus \( \det A = x_1 y_1 \).

For \( n = 2 \), we have \( A = \begin{pmatrix} x_1 y_1 & x_1 y_2 \\ x_2 y_1 & x_2 y_2 \end{pmatrix} \) and thus \( \det A = (x_1 y_1)(x_2 y_2) - (x_1 y_2)(x_2 y_1) = 0 \).

What do you expect for greater values of \( n \)? The pattern might not be clear at this point yet, but if you compute further examples, you will realize that \( \det A = 0 \) also holds for \( n = 3 \), for \( n = 4 \), for \( n = 5 \ldots \) This suggests that \( \det A = 0 \) for every \( n \geq 2 \). How to prove this?

Let \( n \geq 2 \). Then, \( (134) \) (applied to \( a_{ij} = x_i y_j \)) yields

\[
\det A = \sum_{\sigma \in S_n} (-1)^\sigma \left( x_1 y_{\sigma(1)} \right) \left( x_2 y_{\sigma(2)} \right) \cdots \left( x_n y_{\sigma(n)} \right)
\]

\[
= \sum_{\sigma \in S_n} (-1)^\sigma \left( x_1 x_2 \cdots x_n \right) \left( y_{\sigma(1)} y_{\sigma(2)} \cdots y_{\sigma(n)} \right)
\]

\[
(\text{since} \ \sigma \text{ is a permutation})
\]

\[
= \sum_{\sigma \in S_n} (-1)^\sigma \left( x_1 x_2 \cdots x_n \right) (y_1 y_2 \cdots y_n)
\]

\[
= \left( \sum_{\sigma \in S_n} (-1)^\sigma \right) \left( x_1 x_2 \cdots x_n \right) (y_1 y_2 \cdots y_n).
\]

(138)

Now, every \( \sigma \in S_n \) is either even or odd (but not both), and thus we have

\[
\sum_{\sigma \in S_n} (-1)^\sigma
\]

\[
= \sum_{\sigma \in S_n; \sigma \text{ is even}} (-1)^\sigma + \sum_{\sigma \in S_n; \sigma \text{ is odd}} (-1)^\sigma
\]

\[
= \sum_{\sigma \in S_n; \sigma \text{ is even}} 1 + \sum_{\sigma \in S_n; \sigma \text{ is odd}} (-1)
\]

\[
= \left( \text{the number of even permutations} \ \sigma \in S_n \right) \cdot 1 + \left( \text{the number of odd permutations} \ \sigma \in S_n \right) \cdot (-1)
\]

\[
= \left( \text{the number of even permutations} \ \sigma \in S_n \right) \cdot 1 + \left( \text{the number of odd permutations} \ \sigma \in S_n \right) \cdot (-1)
\]

\[
= \left( \frac{n!}{2} \right) \cdot 1 + \left( \frac{n!}{2} \right) \cdot (-1)
\]

\[
= \frac{n!}{2} \cdot 1 + \frac{n!}{2} \cdot (-1) = 0.
\]
Hence, (138) becomes \[
\det A = \left( \sum_{\sigma \in S_n} (-1)^{\sigma} (x_1x_2 \cdots x_n)(y_1y_2 \cdots y_n) \right) = 0,
\]
we wanted to prove.

We will eventually learn a simpler way to prove this.

**Example 6.7.** Here is an example similar to Example 6.6, but subtler.

Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( K \), and let \( y_1, y_2, \ldots, y_n \) be \( n \) further elements of \( K \). Let \( A \) be the \( n \times n \)-matrix \( (x_i + y_j)_{1 \leq i \leq n, 1 \leq j \leq n} \). What is \( \det A \)?

For \( n = 0 \), we have \( \det A = 1 \) again.

For \( n = 1 \), we have \( A = \begin{pmatrix} x_1 + y_1 \end{pmatrix} \) and thus \( \det A = x_1 + y_1 \).

For \( n = 2 \), we have \( A = \begin{pmatrix} x_1 + y_1 & x_1 + y_2 \\ x_2 + y_1 & x_2 + y_2 \end{pmatrix} \) and thus \( \det A = (x_1 + y_1)(x_2 + y_2) - (x_1 + y_2)(x_2 + y_1) = -(y_1 - y_2)(x_1 - x_2) \).

However, it turns out that for every \( n \geq 3 \), we again have \( \det A = 0 \). This is harder to prove than the similar claim in Example 6.6. We will eventually see how to do it easily, but as for now let me outline a direct proof. (I am being rather telegraphic here; do not worry if you do not understand the following argument, as there will be easier and more detailed proofs below.)

From (134), we obtain
\[
\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} (x_1 + y_{\sigma(1)}) (x_2 + y_{\sigma(2)}) \cdots (x_n + y_{\sigma(n)}) \tag{139}.
\]

If we expand the product \( (x_1 + y_{\sigma(1)}) (x_2 + y_{\sigma(2)}) \cdots (x_n + y_{\sigma(n)}) \), we obtain a sum of \( 2^n \) terms:
\[
(x_1 + y_{\sigma(1)}) (x_2 + y_{\sigma(2)}) \cdots (x_n + y_{\sigma(n)}) = \sum_{I \subseteq [n]} \left( \prod_{i \in I} x_i \right) \left( \prod_{i \in [n] \setminus I} y_{\sigma(i)} \right)
\]
(where \([n]\) means the set \( \{1, 2, \ldots, n\} \)). Thus, (139) becomes
\[
\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} (x_1 + y_{\sigma(1)}) (x_2 + y_{\sigma(2)}) \cdots (x_n + y_{\sigma(n)})
\]
\[
= \sum_{\sigma \in S_n} (-1)^{\sigma} \sum_{I \subseteq [n]} \left( \prod_{i \in I} x_i \right) \left( \prod_{i \in [n] \setminus I} y_{\sigma(i)} \right)
\]
\[
= \sum_{I \subseteq [n]} \sum_{\sigma \in S_n} (-1)^{\sigma} \left( \prod_{i \in I} x_i \right) \left( \prod_{i \in [n] \setminus I} y_{\sigma(i)} \right) .
\]
We want to prove that this is 0. In order to do so, it clearly suffices to show that every \( I \subseteq [n] \) satisfies

\[
\sum_{\sigma \in S_n} (-1)^\sigma \left( \prod_{i \in I} x_i \right) \left( \prod_{i \in [n] \setminus I} y_{\sigma(i)} \right) = 0. \tag{140}
\]

So let us fix \( I \subseteq [n] \), and try to prove (140). We must be in one of the following two cases:

**Case 1:** The set \([n] \setminus I\) has at least two elements. In this case, let us pick two distinct elements \( a \) and \( b \) of this set, and split the set \( S_n \) into disjoint two-element subsets by pairing up every even permutation \( \sigma \in S_n \) with the odd permutation \( t_{a,b} \circ \sigma \) (where \( t_{a,b} \) is as defined in Definition 5.25). The addends on the left hand side of (140) corresponding to two permutations paired up cancel out each other, and thus the whole left hand side of (140) is 0. Thus, (140) is proven in Case 1.

**Case 2:** The set \([n] \setminus I\) has at most one element. In this case, the set \( I \) has at least two elements (it is here that we use \( n \geq 3 \)). Pick two distinct elements \( c \) and \( d \) of \( I \), and split the set \( S_n \) into disjoint two-element subsets by pairing up every even permutation \( \sigma \in S_n \) with the odd permutation \( \sigma \circ t_{c,d} \). Again, the addends on the left hand side of (140) corresponding to two permutations paired up cancel out each other, and thus the whole left hand side of (140) is 0. This proves (140) in Case 2.

We thus have proven (140) in both cases. So \( \det A = 0 \) is proven. This was a tricky argument, and shows the limits of the usefulness of (134).

We shall now discuss basic properties of the determinant.

**Exercise 21.** Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix. Assume that \( a_{i,j} = 0 \) for every \( (i,j) \in \{1,2,\ldots,n\}^2 \) satisfying \( i < j \). Show that

\[
\det A = a_{1,1}a_{2,2}\cdots a_{n,n}.
\]

**Definition 6.8.** An \( n \times n \)-matrix \( A \) satisfying the assumption of Exercise 21 is said to be lower-triangular (because its entries above the main diagonal are 0, and thus its nonzero entries are concentrated in the triangular region southwest of the main diagonal). Exercise 21 thus says that the determinant of a lower-triangular matrix is the product of its diagonal entries. For instance, \( \det \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & f \end{pmatrix} =acf \).
Example 6.9. Let \( n \in \mathbb{N} \). The \( n \times n \) identity matrix \( I_n \) is lower-triangular, and its diagonal entries are \( 1, 1, \ldots, 1 \). Hence, Exercise 21 shows that its determinant is \( \det (I_n) = 1 \cdot 1 \cdots 1 = 1 \).

Definition 6.10. The transpose of a matrix \( A = (a_{ij})_{1 \leq i \leq n, \ 1 \leq j \leq m} \) is defined to be the matrix \( (a_{ji})_{1 \leq j \leq m, \ 1 \leq i \leq n} \). It is denoted by \( A^T \). For instance, \( \begin{pmatrix} 1 & 2 & -1 \\ 4 & 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 0 \\ -1 & 1 \end{pmatrix} \).

Remark 6.11. I have seen various other notations for the transpose of a matrix \( A \). Some of them are \( A^t \) (with a lower case \( t \)) and \( T_A \) and \( t_A \).

Exercise 22. Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Show that \( \det (A^T) = \det A \).

The transpose of a lower-triangular \( n \times n \)-matrix is an upper-triangular \( n \times n \)-matrix (i.e., an \( n \times n \)-matrix whose entries below the main diagonal are 0). Thus, combining Exercise 21 with Exercise 22, we see that the determinant of an upper-triangular matrix is the product of its diagonal entries.

Here is yet another simple property of determinants that follows directly from their definition:

Proposition 6.12. Let \( n \in \mathbb{N} \) and \( \lambda \in \mathbb{K} \). Let \( A \) be an \( n \times n \)-matrix. Then, \( \det (\lambda A) = \lambda^n \det A \).

Proof of Proposition 6.12. Write \( A \) in the form \( A = (a_{ij})_{1 \leq i \leq n, \ 1 \leq j \leq n} \). Thus, \( \lambda A = (\lambda a_{ij})_{1 \leq i \leq n, \ 1 \leq j \leq n} \) (by the definition of \( \lambda A \)). Hence, (135) (applied to \( \lambda A \) and \( \lambda a_{ij} \) instead of \( A \) and \( a_{ij} \)) yields

\[
\det (\lambda A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} \left( \lambda a_{i,\sigma(i)} \right) = \sum_{\sigma \in S_n} (-1)^\sigma \lambda^n \prod_{i=1}^{n} a_{i,\sigma(i)}
\]

\[
= \lambda^n \prod_{i=1}^{n} a_{i,\sigma(i)} \quad \text{(by 135)}
\]

\[
= \lambda^n \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} a_{i,\sigma(i)} = \lambda^n \det A.
\]

Proposition 6.12 is thus proven. \( \square \)
Exercise 23. Let $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p$ be elements of $K$.

(a) Find a simple formula for the determinant

$$\det\begin{pmatrix} a & b & c & d \\ l & 0 & 0 & e \\ k & 0 & 0 & f \\ j & i & h & g \end{pmatrix}.$$ 

(b) Find a simple formula for the determinant

$$\det\begin{pmatrix} a & b & c & d & e \\ f & 0 & 0 & 0 & g \\ h & 0 & 0 & 0 & i \\ j & 0 & 0 & 0 & k \\ \ell & m & n & o & p \end{pmatrix}.$$

(Do not mistake the “o” for a “0”.)

[Hint: Part (b) is simpler than part (a).]

In the next exercises, we shall talk about rows and columns; let us first make some pedantic remarks about these notions.

If $n \in \mathbb{N}$, then an $n \times 1$-matrix is said to be a column vector of length $n$, whereas a $1 \times n$-matrix is said to be a row vector of length $n$. Column vectors and row vectors store exactly the same kind of data (namely, $n$ elements of $K$), so you might wonder why I make a difference between them (and also why I distinguish them from $n$-tuples of elements of $K$, which also contain precisely the same kind of data). The reason for this is that column vectors and row vectors behave differently under matrix multiplication: For example,

$$\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \end{pmatrix}$$

is not the same as

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac + bd \end{pmatrix}.$$ 

If we would identify column vectors with row vectors, then this would cause contradictions.

The reason to distinguish between row vectors and $n$-tuples is subtler: We have defined row vectors only for a commutative ring $K$, whereas $n$-tuples can be made out of elements of any set. As a consequence, the sum of two row vectors is well-defined (since row vectors are matrices and thus can be added entry by entry), whereas the sum of two $n$-tuples is not. Similarly, we can take the product $\lambda v$ of

---

128The word “length” here has nothing to do with the length of a segment in geometry. Probably, among the words used in mathematics, “length” is one of those with the most different meanings.
an element \( \lambda \in K \) with a row vector \( v \) (by multiplying every entry of \( v \) by \( \lambda \)), but such a thing does not make sense for general \( n \)-tuples. These differences between row vectors and \( n \)-tuples, however, cause no clashes of notation if we use the same notations for both types of object. Thus, we are often going to identify a row vector \( \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \) with the \( n \)-tuple \( (a_1, a_2, \ldots, a_n) \in K^n \). Thus, \( K^n \) becomes the set of all row vectors of length \( n \).

The column vectors of length \( n \) are in 1-to-1 correspondence with the row vectors of length \( n \), and this correspondence is given by taking the transpose: The column vector \( v \) corresponds to the row vector \( v^T \), and conversely, the row vector \( w \) corresponds to the column vector \( w^T \). In particular, every column vector \( \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \) can be rewritten in the form \( \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}^T = (a_1, a_2, \ldots, a_n)^T \). We shall often write it in the latter form, just because it takes up less space on paper.

The rows of a matrix are row vectors; the columns of a matrix are column vectors. Thus, terms like “the sum of two rows of a matrix \( A \)” or “\(-3\) times a column of a matrix \( A \)” make sense: Rows and columns are vectors, and thus can be added (when they have the same length) and multiplied by elements of \( K \).

Let \( n \in \mathbb{N} \) and \( j \in \{1, 2, \ldots, n\} \). If \( v \) is a column vector of length \( n \) (that is, an \( n \times 1 \)-matrix), then the \( j \)-th entry of \( v \) means the \((j, 1)\)-th entry of \( v \). If \( v \) is a row vector of length \( n \) (that is, a \( 1 \times n \)-matrix), then the \( j \)-th entry of \( v \) means the \((1, j)\)-th entry of \( v \). For example, the 2-nd entry of the row vector \( \begin{pmatrix} a & b & c \end{pmatrix} \) is \( b \).

**Exercise 24.** Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Prove the following:

(a) If \( B \) is an \( n \times n \)-matrix obtained from \( A \) by switching two rows, then \( \det B = - \det A \). (“Switching two rows” means “switching two distinct rows”, of course.)

(b) If \( B \) is an \( n \times n \)-matrix obtained from \( A \) by switching two columns, then \( \det B = - \det A \).

(c) If a row of \( A \) consists of zeroes, then \( \det A = 0 \).

(d) If a column of \( A \) consists of zeroes, then \( \det A = 0 \).

(e) If \( A \) has two equal rows, then \( \det A = 0 \).

(f) If \( A \) has two equal columns, then \( \det A = 0 \).

(g) Let \( \lambda \in K \) and \( k \in \{1, 2, \ldots, n\} \). If \( B \) is the \( n \times n \)-matrix obtained from \( A \) by multiplying the \( k \)-th row by \( \lambda \) (that is, multiplying every entry of the \( k \)-th row by \( \lambda \)), then \( \det B = \lambda \det A \).

(h) Let \( \lambda \in K \) and \( k \in \{1, 2, \ldots, n\} \). If \( B \) is the \( n \times n \)-matrix obtained from \( A \) by multiplying the \( k \)-th column by \( \lambda \), then \( \det B = \lambda \det A \).

\[ \text{Exercise 24.} \]

Some algebraists, instead, identify column vectors with \( n \)-tuples, so that \( K^n \) is then the set of all column vectors of length \( n \). This is a valid convention as well, but one must be careful not to use it simultaneously with the other convention (i.e., with the convention that row vectors are identified with \( n \)-tuples); this is why we will not use it.
(i) Let \( k \in \{1, 2, \ldots, n\} \). Let \( A' \) be an \( n \times n \)-matrix whose rows equal the corresponding rows of \( A \) except (perhaps) the \( k \)-th row. Let \( B \) be the \( n \times n \)-matrix obtained from \( A \) by adding the \( k \)-th row of \( A' \) to the \( k \)-th row of \( A \) (that is, by adding every entry of the \( k \)-th row of \( A' \) to the corresponding entry of the \( k \)-th row of \( A \)). Then, \( \det B = \det A + \det A' \).

(j) Let \( k \in \{1, 2, \ldots, n\} \). Let \( A' \) be an \( n \times n \)-matrix whose columns equal the corresponding columns of \( A \) except (perhaps) the \( k \)-th column. Let \( B \) be the \( n \times n \)-matrix obtained from \( A \) by adding the \( k \)-th column of \( A' \) to the \( k \)-th column of \( A \). Then, \( \det B = \det A + \det A' \).

Example 6.13. Let me visualize Exercise [24](i) on an example, as it has a somewhat daunting statement.

Set \( n = 3 \) and \( k = 2 \). Set \( A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \). Then, a matrix \( A' \) satisfying the conditions of Exercise [24](i) has the form \( A' = \begin{pmatrix} a & b & c \\ d' & e' & f' \\ g & h & i \end{pmatrix} \). For such a matrix \( A' \), we obtain \( B = \begin{pmatrix} a & b & c \\ d + d' & e + e' & f + f' \\ g & h & i \end{pmatrix} \). Exercise [24](i) then claims that \( \det B = \det A + \det A' \).

Parts (a), (c), (e), (g) and (i) of Exercise [24] are often united under the slogan “the determinant of a matrix is multilinear and alternating in its rows”\(^{130}\). Similarly, parts (b), (d), (f), (h) and (j) are combined under the slogan “the determinant of a matrix is multilinear and alternating in its columns”. Many texts on linear algebra (for example, \[HoffKun\]) use these properties as the definition of the determinant; this is a valid approach, but I prefer to use Definition 6.5 instead, since it is more explicit.

Exercise 25. Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Prove the following:

(a) If we add a scalar multiple of a row of \( A \) to another row of \( A \), then the determinant of \( A \) does not change. (A scalar multiple of a row vector \( v \) means a row vector of the form \( \lambda v \), where \( \lambda \in \mathbb{K} \).)

\(^{130}\)Specifically, parts (c), (g) and (i) say that it is “multilinear”, while parts (a) and (e) are responsible for the “alternating”.

\(^{131}\)More precisely, they define a determinant function to be a function \( F : \mathbb{K}^{n \times n} \to \mathbb{K} \) which is multilinear and alternating in the rows of a matrix (i.e., which satisfies parts (a), (c), (e), (g) and (i) of Exercise [24] if every appearance of “\( \det \)” is replaced by “\( F \)” in this Exercise) and which satisfies \( F(I_n) = 1 \). Then, they show that there is (for each \( n \in \mathbb{N} \)) exactly one determinant function \( F : \mathbb{K}^{n \times n} \to \mathbb{K} \). They then denote this function by \( \det \). This is a rather slick definition of a determinant, but it has the downside that it requires showing that there is exactly one determinant function (which is often not easier than our approach).
(b) If we add a scalar multiple of a column of \( A \) to another column of \( A \), then the determinant of \( A \) does not change. (A scalar multiple of a column vector \( v \) means a column vector of the form \( \lambda v \), where \( \lambda \in \mathbb{K} \).)

**Example 6.14.** Let us visualize Exercise 25 (a). Set \( n = 3 \) and \( A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \).

If we add \(-2\) times the second row of \( A \) to the first row of \( A \), then we obtain the matrix \( \begin{pmatrix} a + (-2)d & b + (-2)e & c + (-2)f \\ d & e & f \\ g & h & i \end{pmatrix} \). Exercise 25 (a) now claims that this new matrix has the same determinant as \( A \) (because \(-2\) times the second row of \( A \) is a scalar multiple of the second row of \( A \)).

Notice the word “another” in Exercise 25. Adding a scalar multiple of a row of \( A \) to the same row of \( A \) will likely change the determinant.

**Remark 6.15.** Exercise 25 lets us prove the claim of Example 6.7 in a much simpler way.

Namely, let \( n \) and \( x_1, x_2, \ldots, x_n \) and \( y_1, y_2, \ldots, y_n \) and \( A \) be as in Example 6.7. Assume that \( n \geq 3 \). We want to show that \( \det A = 0 \).

The matrix \( A \) has at least three rows (since \( n \geq 3 \)), and looks as follows:

\[
A = \begin{pmatrix}
x_1 + y_1 & x_1 + y_2 & x_1 + y_3 & x_1 + y_4 & \cdots & x_1 + y_n \\
x_2 + y_1 & x_2 + y_2 & x_2 + y_3 & x_2 + y_4 & \cdots & x_2 + y_n \\
x_3 + y_1 & x_3 + y_2 & x_3 + y_3 & x_3 + y_4 & \cdots & x_3 + y_n \\
x_4 + y_1 & x_4 + y_2 & x_4 + y_3 & x_4 + y_4 & \cdots & x_4 + y_n \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_n + y_1 & x_n + y_2 & x_n + y_3 & x_n + y_4 & \cdots & x_n + y_n
\end{pmatrix}
\]

(where the presence of terms like \( x_4 \) and \( y_4 \) does not mean that the variables \( x_4 \) and \( y_4 \) exist, in the same way as one can write “\( x_1, x_2, \ldots, x_k \)” even if \( k = 1 \) or \( k = 0 \)). Thus, if we subtract the first row of \( A \) from the second row of \( A \), then we obtain the matrix

\[
A' = \begin{pmatrix}
x_1 + y_1 & x_1 + y_2 & x_1 + y_3 & x_1 + y_4 & \cdots & x_1 + y_n \\
x_2 - x_1 & x_2 - x_1 & x_2 - x_1 & x_2 - x_1 & \cdots & x_2 - x_1 \\
x_3 + y_1 & x_3 + y_2 & x_3 + y_3 & x_3 + y_4 & \cdots & x_3 + y_n \\
x_4 + y_1 & x_4 + y_2 & x_4 + y_3 & x_4 + y_4 & \cdots & x_4 + y_n \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_n + y_1 & x_n + y_2 & x_n + y_3 & x_n + y_4 & \cdots & x_n + y_n
\end{pmatrix}
\]

(because \( x_2 + y_j - (x_1 + y_j) = x_2 - x_1 \) for every \( j \)). The transformation we just did (subtracting a row from another row) does not change the determinant of
the matrix (by Exercise 25 (a), because subtracting a row from another row is tantamount to adding the \((-1\))-multiple of the former row to the latter), and thus we have \(\det A' = \det A\).

We notice that each entry of the second row of \(A'\) equals \(x_2 - x_1\).

Next, we subtract the first row of \(A'\) from the third row of \(A'\), and obtain the matrix

\[
A'' = \begin{pmatrix}
x_1 + y_1 & x_1 + y_2 & x_1 + y_3 & x_1 + y_4 & \cdots & x_1 + y_n \\
x_2 - x_1 & x_2 - x_1 & x_2 - x_1 & x_2 - x_1 & \cdots & x_2 - x_1 \\
x_3 - x_1 & x_3 - x_1 & x_3 - x_1 & x_3 - x_1 & \cdots & x_3 - x_1 \\
x_4 + y_1 & x_4 + y_2 & x_4 + y_3 & x_4 + y_4 & \cdots & x_4 + y_n \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_n + y_1 & x_n + y_2 & x_n + y_3 & x_n + y_4 & \cdots & x_n + y_n
\end{pmatrix}.
\]

Again, the determinant is unchanged (because of Exercise 25 (a)), so we have \(\det A'' = \det A' = \det A\).

We notice that each entry of the second row of \(A''\) equals \(x_2 - x_1\) (indeed, these entries have been copied over from \(A'\)), and that each entry of the third row of \(A''\) equals \(x_3 - x_1\).

Next, we subtract the first column of \(A''\) from each of the other columns of \(A''\). This gives us the matrix

\[
A''' = \begin{pmatrix}
x_1 + y_1 & y_2 - y_1 & y_3 - y_1 & y_4 - y_1 & \cdots & y_n - y_1 \\
x_2 - x_1 & 0 & 0 & 0 & \cdots & 0 \\
x_3 - x_1 & 0 & 0 & 0 & \cdots & 0 \\
x_4 + y_1 & y_2 - y_1 & y_3 - y_1 & y_4 - y_1 & \cdots & y_n - y_1 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
x_n + y_1 & y_2 - y_1 & y_3 - y_1 & y_4 - y_1 & \cdots & y_n - y_1
\end{pmatrix}.
\] (141)

This step, again, has not changed the determinant (because Exercise 25 (b) shows that subtracting a column from another column does not change the determinant, and what we did was doing \(n - 1\) such transformations). Thus, \(\det A''' = \det A'' = \det A\).

Now, let us write the matrix \(A'''\) in the form \(A''' = (a''''_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}\). (Thus, \(a''''_{i,j}\) is the \((i,j)\)-th entry of \(A'''\) for every \((i,j)\)). Then, (134) (applied to \(A'''\) instead of \(A\)) yields

\[
\det A''' = \sum_{\sigma \in S_n} (-1)^{\sigma} a''''_{1,\sigma(1)}a''''_{2,\sigma(2)} \cdots a''''_{n,\sigma(n)}.
\] (142)

I claim that

\[
a''''_{1,\sigma(1)}a''''_{2,\sigma(2)} \cdots a''''_{n,\sigma(n)} = 0 \quad \text{for every } \sigma \in S_n.
\] (143)

**Proof of (143):** Let \(\sigma \in S_n\). Then, \(\sigma\) is injective, and thus \(\sigma(2) \neq \sigma(3)\). Therefore, at least one of the integers \(\sigma(2)\) and \(\sigma(3)\) must be \(\neq 1\) (because otherwise, we...
would have \( \sigma(2) = 1 = \sigma(3) \), contradicting \( \sigma(2) \neq \sigma(3) \). We WLOG assume that \( \sigma(2) \neq 1 \). But a look at (141) reveals that all entries of the second row of \( A''' \) are zero except for the first entry. Thus, \( a'''_{2,1} = 0 \) for every \( j \neq 1 \). Applied to \( j = \sigma(2) \), this yields \( a'''_{2,\sigma(2)} = 0 \) (since \( \sigma(2) \neq 1 \)). Hence, \( a'''_{1,\sigma(1)}a'''_{2,\sigma(2)} \cdots a'''_{n,\sigma(n)} = 0 \) (because if 0 appears as a factor in a product, then the whole product must be 0). This proves (143).

Now, (142) becomes

\[
\det A''' = \sum_{\sigma \in S_n} (-1)^\sigma a'''_{1,\sigma(1)}a'''_{2,\sigma(2)} \cdots a'''_{n,\sigma(n)} = \sum_{\sigma \in S_n} (-1)^\sigma 0 = 0. 
\]

(by (143))

Compared with \( \det A''' = \det A \), this yields \( \det A = 0 \). Thus, \( \det A = 0 \) is proven again.

**Remark 6.16.** Here is another example for the use of Exercise 25.

Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( K \). Let \( A \) be the matrix

\[
\begin{pmatrix}
    x_{\max\{i,j\}} \\
    x_2 & x_3 & x_4 \\
    x_3 & x_4 \\
    x_4 & x_4 \\
\end{pmatrix}
\]

(Recall that max \( S \) denotes the greatest element of a nonempty set \( S \).)

For example, if \( n = 4 \), then

\[
A = \begin{pmatrix}
    x_1 & x_2 & x_3 & x_4 \\
    x_2 & x_3 & x_4 \\
    x_3 & x_4 \\
    x_4 & x_4 \\
\end{pmatrix}
\]
(since we obtained the matrix $A'$ by subtracting the first row of $A$ from each of the other rows of $A$). Hence, for every $(i, j) \in \{1, 2, \ldots, n\}^2$ satisfying $1 < i \leq j$, we have

$$a'_{i,j} = x_{\max\{i,j\}} - x_{\max\{1,j\}} = x_j - x_i \quad \left(\text{since } \max\{i,j\} = j \text{ (because } i \leq j \right)$$

$$= 0. \quad (146)$$

This is the general explanation for the six 0's in (144). We notice also that the first row of the matrix $A'$ is $(x_1, x_2, \ldots, x_n)$.

Now, we want to transform $A'$ further. Namely, we first switch the first row with the second row; then we switch the second row (which used to be the first row) with the third row; then, the third row with the fourth row, and so on, until we finally switch the $(n-1)$-th row with the $n$-th row. As a result of these $n-1$ switches, the first row has moved all the way down to the bottom, past all the other rows. We denote the resulting matrix by $A''$. For instance, if $n = 4$, then

$$A'' = \begin{pmatrix} x_2 - x_1 & 0 & 0 & 0 \\ x_3 - x_1 & x_3 - x_2 & 0 & 0 \\ x_4 - x_1 & x_4 - x_2 & x_4 - x_3 & 0 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}. \quad (147)$$

This is a lower-triangular matrix. To see that this holds in the general case, we write the matrix $A''$ in the form $A'' = \left( a''_{i,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}$ (so that $a''_{i,j}$ is the $(i,j)$-th entry of $A''$ for every $(i,j)$). Then, for every $(i,j) \in \{1, 2, \ldots, n\}^2$, we have

$$a''_{i,j} = \begin{cases} a'_{i+1,j} & \text{if } i < n; \\ a'_{1,j} & \text{if } i = n \end{cases} \quad (148)$$

(because the first row of $A'$ has become the $n$-th row of $A''$, whereas every other row has moved up one step). In particular, for every $(i,j) \in \{1, 2, \ldots, n\}^2$ satisfying $1 \leq i < j \leq n$, we have

$$a''_{i,j} = \begin{cases} a'_{i+1,j} & \text{if } i < n; \\ a'_{1,j} & \text{if } i = n \end{cases} \quad (\text{since } i < j \leq n)$$

$$= 0 \quad \left(\text{by (146), applied to } i+1 \text{ instead of } i \right) \quad (\text{because } i < j \text{ yields } i+1 \leq j) \quad .$$

This shows that $A''$ is indeed lower-triangular. Hence, Exercise 21 (applied to $A''$ and $a''_{i,j}$ instead of $A$ and $a_{i,j}$) shows that $\det A'' = a''_{1,1} a''_{2,2} \cdots a''_{n,n}$.

Using (148) and (145), it is easy to see that every $i \in \{1, 2, \ldots, n\}$ satisfies

$$a''_{i,i} = \begin{cases} x_{i+1} - x_i & \text{if } i < n; \\ x_n & \text{if } i = n \end{cases} \quad . \quad (149)$$
Next, a lemma that will come handy in a more important proof:

**Lemma 6.17.** Let \( n \in \mathbb{N} \). Let \([n]\) denote the set \(\{1, 2, \ldots, n\}\). Let \( \kappa : [n] \to [n] \) be a map. Let \( B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix. Let \( B_\kappa \) be the \( n \times n \)-matrix

\[
(b_{\kappa(i),j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

(a) If \( \kappa \in S_n \), then \( \det(B_\kappa) = (-1)^\kappa \cdot \det B \).

(b) If \( \kappa \notin S_n \), then \( \det(B_\kappa) = 0 \).

**Remark 6.18.** Lemma 6.17(a) simply says that if we permute the rows of a square matrix, then its determinant gets multiplied by the sign of the permutation used.

For instance, let \( n = 3 \) and \( B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \). If \( \kappa \) is the permutation \((2, 3, 1)\) (in one-line notation), then \( B_\kappa = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \), and Lemma 6.17(a) says that

\[
\det(B_\kappa) = (-1)^\kappa \cdot \det B = \det B.
\]
Of course, a similar result holds for permutations of columns.

**Remark 6.19.** Exercise [24](a) is a particular case of Lemma [6.17](a). Indeed, if \( B \) is an \( n \times n \)-matrix obtained from \( A \) by switching the \( u \)-th and the \( v \)-th row (where \( u \) and \( v \) are two distinct elements of \( \{1, 2, \ldots, n\} \)), then \( B = \left( a_{i,u,\sigma(i),j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \) (where \( A \) is written in the form \( A = \left( a_{i,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \)).

**Proof of Lemma 6.17.** Recall that \( S_n \) is the set of all permutations of \( \{1, 2, \ldots, n\} \). In other words, \( S_n \) is the set of all permutations of \( [n] \) (since \( [n] = \{1, 2, \ldots, n\} \)). In other words, \( S_n \) is the set of all bijective maps \( [n] \to [n] \).

(a) Assume that \( \kappa \in S_n \). We define a map \( \Phi : S_n \to S_n \) by
\[
\Phi(\sigma) = \sigma \circ \kappa \quad \text{for every } \sigma \in S_n.
\]
We also define a map \( \Psi : S_n \to S_n \) by
\[
\Psi(\sigma) = \sigma \circ \kappa^{-1} \quad \text{for every } \sigma \in S_n.
\]
The maps \( \Phi \) and \( \Psi \) are mutually inverse.\(^{132}\) Hence, the map \( \Phi \) is a bijection.

We have \( B = \left( b_{i,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, (135) (applied to \( B \) and \( b_{i,j} \) instead of \( A \) and \( a_{i,j} \)) yields
\[
\det B = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{i,\sigma(i)} = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i \in [n]} b_{i,\sigma(i)} \quad \text{(151)}
\]
Now, \( B_\kappa = \left( b_{\kappa(i),j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, (135) (applied to \( B_\kappa \) and \( b_{\kappa(i),j} \) instead of \( A \) and \( a_{i,j} \)) yields
\[
\det (B_\kappa) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{\kappa(i),\sigma(i)} = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i \in [n]} b_{\kappa(i),\sigma(i)}
\]
\[
= \sum_{\sigma \in S_n} (-1)^{\Phi(\sigma)} \prod_{i \in [n]} b_{\kappa(i),\Phi(\sigma)(i)} \quad \text{(152)}
\]
\(^{132}\)Proof. Every \( \sigma \in S_n \) satisfies
\[
(\Psi \circ \Phi)(\sigma) = \Psi \left( \Phi(\sigma) \right) = \Psi(\sigma \circ \kappa) = \sigma \circ \kappa \circ \kappa^{-1} = \text{id} \quad \text{(by the definition of } \Psi \text{)}
\]
Thus, \( \Psi \circ \Phi = \text{id} \). Similarly, \( \Phi \circ \Psi = \text{id} \). Combined with \( \Psi \circ \Phi = \text{id} \), this yields that the maps \( \Phi \) and \( \Psi \) are mutually inverse, qed.
(here, we have substituted $\Phi (\sigma)$ for $\sigma$ in the sum, since $\Phi$ is a bijection).

But every $\sigma \in S_n$ satisfies $(-1)^{\Phi(\sigma)} = (-1)^{\kappa} \cdot (-1)^{\sigma} \quad \text{(135)}$ and
\[
\prod_{i \in [n]} b_{i,\sigma(i)} \quad \text{Thus, (152) becomes}
\]
\[
\det (B_\kappa) = \sum_{\sigma \in S_n} (-1)^{\Phi(\sigma)} \prod_{i \in [n]} b_{\kappa(i),\Phi(\sigma)(i)}(i) = \sum_{\sigma \in S_n} (-1)^{\kappa} \cdot (-1)^{\sigma} \prod_{i \in [n]} b_{i,\sigma(i)}
\]
\[
= (-1)^{\kappa} \cdot \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i \in [n]} b_{i,\sigma(i)} = (-1)^{\kappa} \cdot \det B.
\]
\[
\text{(by \ref{detB})}
\]

This proves Lemma 6.17 (a).

(b) Assume that $\kappa \notin S_n$.

The following fact is well-known: If $U$ is a finite set, then every injective map $U \to U$ is bijective. We can apply this to $U = [n]$, and thus conclude that every injective map $[n] \to [n]$ is bijective. Therefore, if the map $\kappa : [n] \to [n]$ were injective, then $\kappa$ would be bijective and therefore would be an element of $S_n$ (since $S_n$ is the set of all bijective maps $[n] \to [n]$); but this would contradict the fact that $\kappa \notin S_n$. Hence, the map $\kappa : [n] \to [n]$ cannot be injective. Therefore, there exist two distinct elements $a$ and $b$ of $[n]$ such that $\kappa(a) = \kappa(b)$. Consider these $a$ and $b$. Then, $\kappa \circ t_{a,b} = \kappa \quad \text{(136)}$ Exercise 16 (b) (applied to $i = a$ and $j = b$) yields $(-1)^{t_{a,b}} = -1$.

\textbf{Proof.} Let $\sigma \in S_n$. Then, $\Phi(\sigma) = \sigma \circ \kappa$, so that
\[
(-1)^{\Phi(\sigma)} = (-1)^{\sigma \circ \kappa} = (-1)^{\sigma} \cdot (-1)^{\kappa} \quad \text{(by \ref{Phi}, applied to $\tau = \kappa$)}
\]
\[
= (-1)^{\kappa} \cdot (-1)^{\sigma},
\]
\text{qed.}

\textbf{Proof.} Let $\sigma \in S_n$. We have $\Phi(\sigma) = \sigma \circ \kappa$. Thus, for every $i \in [n]$, we have $(\Phi(\sigma))(i) = (\sigma \circ \kappa)(i) = \sigma(\kappa(i))$. Hence, \[
\prod_{i \in [n]} b_{\kappa(i),\Phi(\sigma)(i)}(i) = \prod_{i \in [n]} b_{\kappa(i),\sigma(\kappa(i))}.
\]

But $\kappa \in S_n$. In other words, $\kappa$ is a permutation of the set $\{1,2,\ldots,n\} = [n]$, hence a bijection from $[n]$ to $[n]$. Therefore, we can substitute $\kappa(i)$ for $i$ in the product $\prod_{i \in [n]} b_{i,\sigma(i)}$. We thus obtain $\prod_{i \in [n]} b_{i,\sigma(i)} = \prod_{i \in [n]} b_{\kappa(i),\sigma(\kappa(i))}$. Comparing this with $\prod_{i \in [n]} b_{\kappa(i),\Phi(\sigma)(i)}(i) = \prod_{i \in [n]} b_{\kappa(i),\sigma(\kappa(i))}$, we obtain $\prod_{i \in [n]} b_{\kappa(i),\Phi(\sigma)(i)}(i) = \prod_{i \in [n]} b_{i,\sigma(i)}$, QED.

\textbf{Proof.} Let $U$ be a finite set, and let $f$ be an injective map $U \to U$. We must show that $f$ is bijective. Since $f$ is injective, we have $|f(U)| = |U|$. Thus, $f(U)$ is a subset of $U$ which has size $|U|$. But the only such subset is $U$ itself (since $U$ is a finite set). Therefore, $f(U)$ must be $U$ itself. In other words, the map $f$ is surjective. Hence, $f$ is bijective (since $f$ is injective and surjective), QED.

\textbf{Proof.} We are going to show that every $i \in [n]$ satisfies $(\kappa \circ t_{a,b})(i) = \kappa(i)$.

So let $i \in [n]$. We shall show that $(\kappa \circ t_{a,b})(i) = \kappa(i)$. 

Let $A_n$ be the set of all even permutations in $S_n$. Let $C_n$ be the set of all odd permutations in $S_n$.

We have $\sigma \circ t_{a,b} \in C_n$ for every $\sigma \in A_n$. Hence, we can define a map $\Phi: A_n \to C_n$ by
\[
\Phi(\sigma) = \sigma \circ t_{a,b} \quad \text{for every } \sigma \in A_n.
\]
Consider this map $\Phi$. Furthermore, we have $\sigma \circ (t_{a,b})^{-1} \in A_n$ for every $\sigma \in C_n$. Thus, we can define a map $\Psi: C_n \to A_n$ by
\[
\Psi(\sigma) = \sigma \circ (t_{a,b})^{-1} \quad \text{for every } \sigma \in C_n.
\]

The definition of $t_{a,b}$ shows that $t_{a,b}$ is the permutation in $S_n$ which switches $a$ with $b$ while leaving all other elements of $\{1, 2, \ldots, n\}$ unchanged. In other words, we have $t_{a,b}(a) = b$, and $t_{a,b}(b) = a$, and $t_{a,b}(j) = j$ for every $j \in [n] \setminus \{a, b\}$.

Now, we have $i \in [n]$. Thus, we are in one of the following three cases:

Case 1: We have $i = a$.
Case 2: We have $i = b$.
Case 3: We have $i \in [n] \setminus \{a, b\}$.

Let us first consider Case 1. In this case, we have $i = a$, so that $(\kappa \circ t_{a,b}) \left( i \atop = a \right) = (\kappa \circ t_{a,b}) (a) = \kappa (b)$. Compared with $\kappa \left( i \atop = a \right) = \kappa (a) = \kappa (b)$, this yields $\kappa \circ t_{a,b} (i) = \kappa (i)$. Thus, $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ is proven in Case 1.

Let us next consider Case 2. In this case, we have $i = b$, so that $(\kappa \circ t_{a,b}) \left( i \atop = b \right) = (\kappa \circ t_{a,b}) (b) = \kappa (a) = \kappa (b)$. Compared with $\kappa \left( i \atop = b \right) = \kappa (b)$, this yields $\kappa \circ t_{a,b} (i) = \kappa (i)$. Thus, $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ is proven in Case 2.

Let us finally consider Case 3. In this case, we have $i \in [n] \setminus \{a, b\}$. Hence, $t_{a,b} (i) = i$ for every $j \in [n] \setminus \{a, b\}$. Therefore, $(\kappa \circ t_{a,b}) (i) = \kappa \left( t_{a,b} (i) \atop = i \right) = \kappa (i)$. Thus, $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ is proven in Case 3.

We now have shown $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ in each of the three Cases 1, 2 and 3. Hence, $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ always holds.

Now, let us forget that we fixed $i$. We thus have shown that $(\kappa \circ t_{a,b}) (i) = \kappa (i)$ for every $i \in [n]$. In other words, $\kappa \circ t_{a,b} = \kappa$, qed.

**Proof.** Let $\sigma \in A_n$. Then, $\sigma$ is an even permutation in $S_n$ (since $A_n$ is the set of all even permutations in $S_n$). Hence, $(-1)^{\sigma_{\tau}} = 1$. Now, $[113]$ (applied to $\tau = t_{a,b}$) yields $(-1)^{\sigma_{t_{a,b}}} = (-1)^{(-1)^{\sigma_{t_{a,b}}} \cdot (-1)^{t_{a,b}}} = -1$. Thus, the permutation $\sigma \circ t_{a,b}$ is odd. Hence, $\sigma \circ t_{a,b}$ is an odd permutation in $S_n$. In other words, $\sigma \circ t_{a,b} \in C_n$ (since $C_n$ is the set of all odd permutations in $S_n$), qed.

**Proof.** Let $\sigma \in C_n$. Then, $\sigma$ is an odd permutation in $S_n$ (since $C_n$ is the set of all odd permutations in $S_n$). Hence, $(-1)^{\sigma_{\tau}} = -1$.

Applying $[114]$ to $t_{a,b}$ instead of $\sigma$, we obtain $(-1)^{t_{a,b}} = -1$. Now, $[113]$ (ap-
But I wanted to demonstrate a use of (114). Hence, the map \( \Psi \) is a bijection. Moreover, every permutation \( \sigma \in C_n \) satisfies

\[
\prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)} = \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}. \tag{153}
\]

We have \( B_\kappa = \left(b_{\kappa(i), j}\right)_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, (135) (applied to \( B_\kappa \) and \( b_{\kappa(i), j} \) instead

\[
\prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)} = \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}. \tag{153}
\]

\( \prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)} = \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}. \tag{153} \)

Proof of (153): Let \( \sigma \in C_n \). The map \( t_{a,b} \) is a permutation of \([n]\), thus a bijection \([n] \rightarrow [n]\). Hence, we can substitute \( t_{a,b}(i) \) for \( i \) in the product \( \prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)} \). Thus we obtain

\[
\prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)} = \prod_{i \in [n]} b_{\kappa(t_{a,b}(i)), (\Psi(\sigma))(t_{a,b}(i))} = \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}
\]

(since every \( i \in [n] \) satisfies \( \kappa(t_{a,b}(i)) = (\kappa \circ t_{a,b})(i) = \kappa(i) \) and

\[
(\Psi(\sigma))(t_{a,b}(i)) = (\sigma \circ (t_{a,b})^{-1})(t_{a,b}(i)) = \sigma \left( (t_{a,b})^{-1}(t_{a,b}(i)) \right) = \sigma(i)
\]

). This proves (153).
This proves Lemma 6.17 (b).

Now let us state a basic formula for products of sums in a commutative ring:

Lemma 6.20. For every \( n \in \mathbb{N} \), let \([n]\) denote the set \( \{1, 2, \ldots, n\} \).

Let \( n \in \mathbb{N} \). For every \( i \in [n] \), let \( p_{i,1}, p_{i,2}, \ldots, p_{i,m_i} \) be finitely many elements of \( K \). Then,

\[
\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} = \sum_{(k_1, k_2, \ldots, k_n) \in [m_1] \times [m_2] \times \cdots \times [m_n]} \prod_{i=1}^{n} p_{i,k_i}.
\]

(Pedantic remark: If \( n = 0 \), then the Cartesian product \([m_1] \times [m_2] \times \cdots \times [m_n]\) has no factors; it is what is called an empty Cartesian product. It is understood to be a 1-element set, and its single element is the 0-tuple \( () \) (also known as the empty list).)

Of \( A \) and \( a_{ij} \) yields

\[
\det (B) = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} b_{\kappa(i), \sigma(i)} = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}
\]

\[
= \sum_{\sigma \in S_n; \sigma \text{ is even}} (-1)^{\sigma} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)} + \sum_{\sigma \in S_n; \sigma \text{ is odd}} (-1)^{\sigma} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}
\]

\[
= \sum_{\sigma \in A_n} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)} + \sum_{\sigma \in C_n} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}
\]

since

\[
\sum_{\sigma \in A_n} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)} = \sum_{\sigma \in C_n} \prod_{i \in [n]} b_{\kappa(i), (\Psi(\sigma))(i)}
\]

\[
= \sum_{\sigma \in C_n} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)} \quad \text{(by (153))}
\]

\[
(\text{here, we have substituted } \Psi(\sigma) \text{ for } \sigma, \text{ since the map } \Psi \text{ is a bijection})
\]

\[
= \sum_{\sigma \in C_n} \prod_{i \in [n]} b_{\kappa(i), \sigma(i)}.
\]

This proves Lemma 6.17 (b). \( \square \)
I tend to refer to Lemma 6.20 as the product rule (since it is related to the product rule for joint probabilities); I think it has no really widespread name. However, it is a fundamental algebraic fact that is used very often and tacitly (I suspect that most mathematicians have never thought of it as being a theorem that needs to be proven). The idea behind Lemma 6.20 is that if you expand the product

\[
\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} = \prod_{i=1}^{n} (p_{i,1} + p_{i,2} + \cdots + p_{i,m_i}) = (p_{1,1} + p_{1,2} + \cdots + p_{1,m_1})(p_{2,1} + p_{2,2} + \cdots + p_{2,m_2}) \cdots (p_{n,1} + p_{n,2} + \cdots + p_{n,m_n}),
\]

then you get a sum of \(m_1 m_2 \cdots m_n\) terms, each of which has the form

\[
p_{1,k_1} p_{2,k_2} \cdots p_{n,k_n} = \prod_{i=1}^{n} p_{i,k_i}
\]

for some \((k_1, k_2, \ldots, k_n) \in [m_1] \times [m_2] \times \cdots \times [m_n]\). (More precisely, it is the sum of all such terms.) A formal proof of Lemma 6.20 could be obtained by induction over \(n\) using the distributivity axiom.\footnote{This and the observation that the \(n\)-tuples \((k_1, k_2, \ldots, k_n) \in [m_1] \times [m_2] \times \cdots \times [m_n]\) are in bijection with the pairs \(((k_1, k_2, \ldots, k_{n-1}), k_n)\) of an \((n-1)\)-tuple \((k_1, k_2, \ldots, k_{n-1}) \in [m_1] \times [m_2] \times \cdots \times [m_{n-1}]\) and an element \(k_n \in [m_n]\).} For the details (if you care about them), see the solution to the following exercise:

\[\textbf{Exercise 26.} \text{ Prove Lemma 6.20.}\]

We shall use a corollary of Lemma 6.20:

**Lemma 6.21.** For every \(n \in \mathbb{N}\), let \([n]\) denote the set \(\{1, 2, \ldots, n\}\).

Let \(n \in \mathbb{N}\) and \(m \in \mathbb{N}\). For every \(i \in [n]\), let \(p_{i,1}, p_{i,2}, \ldots, p_{i,m_i}\) be \(m_i\) elements of \(K\). Then,

\[
\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} = \sum_{\kappa: [n] \to [m]} \prod_{i=1}^{n} p_{i,\kappa(i)}.
\]

**Proof of Lemma 6.21.** For the sake of completeness, let us give this proof.

Lemma 6.20 (applied to \(m_i = m\) for every \(i \in [n]\)) yields

\[
\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} = \sum_{(k_1, k_2, \ldots, k_n) \in [m_1] \times [m_2] \times \cdots \times [m_n]} \prod_{i=1}^{n} p_{i,k_i}, \quad (154)
\]
Let \( \text{Map} ([n], [m]) \) denote the set of all functions from \([n]\) to \([m]\). Now, let \( \Phi \) be the map from \( \text{Map} ([n], [m]) \) to \([m] \times [m] \times \cdots \times [m] \) given by

\[
\Phi (\kappa) = (\kappa(1), \kappa(2), \ldots, \kappa(n)) \quad \text{for every } \kappa \in \text{Map} ([n], [m]).
\]

So the map \( \Phi \) takes a function \( \kappa \) from \([n]\) to \([m]\), and outputs the list \((\kappa(1), \kappa(2), \ldots, \kappa(n))\) of all its values. Clearly, the map \( \Phi \) is injective (since a function \( \kappa \in \text{Map} ([n], [m]) \) can be reconstructed from the list \((\kappa(1), \kappa(2), \ldots, \kappa(n)) = \Phi (\kappa)\)) and surjective (since every list of \( n \) elements of \([m]\) is the list of values of some function \( \kappa \in \text{Map} ([n], [m]) \)). Thus, \( \Phi \) is bijective. Therefore, we can substitute \( \Phi (\kappa) \) for \((k_1, k_2, \ldots, k_n)\) in the sum

\[
\sum_{(k_1, k_2, \ldots, k_n) \in [m] \times [m] \times \cdots \times [m]} \prod_{i=1}^{n} p_{i,k_i},
\]

In other words, we can substitute \((\kappa(1), \kappa(2), \ldots, \kappa(n))\) for \((k_1, k_2, \ldots, k_n)\) in this sum (since \( \Phi (\kappa) = (\kappa(1), \kappa(2), \ldots, \kappa(n)) \) for each \( \kappa \in \text{Map} ([n], [m]) \)). We thus obtain

\[
\sum_{(k_1, k_2, \ldots, k_n) \in [m] \times [m] \times \cdots \times [m]} \prod_{i=1}^{n} p_{i,k_i} = \sum_{\kappa \in \text{Map} ([n], [m])} \prod_{i=1}^{n} p_{i,\kappa(i)} = \sum_{\kappa: [n] \to [m]} \prod_{i=1}^{n} p_{i,\kappa(i)}.
\]

Thus, (154) becomes

\[
\prod_{i=1}^{n} \sum_{k=1}^{m} p_{i,k} = \sum_{(k_1, k_2, \ldots, k_n) \in [m] \times [m] \times \cdots \times [m]} \prod_{i=1}^{n} p_{i,k_i} = \sum_{\kappa: [n] \to [m]} \prod_{i=1}^{n} p_{i,\kappa(i)}.
\]

Lemma 6.21 is proven. \( \square \)

Now we are ready to prove what is probably the most important property of determinants:

**Theorem 6.22.** Let \( n \in \mathbb{N} \). Let \( A \) and \( B \) be two \( n \times n \)-matrices. Then,

\[
\det(AB) = \det A \cdot \det B.
\]

**Proof of Theorem 6.22** Write \( A \) and \( B \) in the forms \( A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \) and \( B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \). The definition of \( AB \) thus yields \( AB = \left( \sum_{k=1}^{n} a_{i,k} b_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \).
Therefore, (135) (applied to $AB$ and $\sum_{k=1}^{n} a_{i,k} b_{k,j}$ instead of $A$ and $a_{i,j}$) yields

$$
\det (AB) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} \left( \sum_{k=1}^{n} a_{i,k} b_{k,\sigma(i)} \right)
= \sum_{\kappa : [n] \to [n]} \prod_{i=1}^{n} \left( a_{i,\kappa(i)} b_{\kappa(i),\sigma(i)} \right)
$$

(by Lemma 6.21 applied to $m=n$ and $p_{i,k} = a_{i,k} b_{k,\sigma(i)}$)

$$
= \sum_{\sigma \in S_n} (-1)^\sigma \prod_{\kappa : [n] \to [n]} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \left( \prod_{i=1}^{n} b_{\kappa(i),\sigma(i)} \right)
= \sum_{\kappa : [n] \to [n]} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \left( \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{\kappa(i),\sigma(i)} \right).
$$

(155)

Now, for every $\kappa : [n] \to [n]$, we let $B_\kappa$ be the $n \times n$-matrix $\left( b_{\kappa(i),j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}$. Then, for every $\kappa : [n] \to [n]$, the equality (135) (applied to $B_\kappa$ and $b_{\kappa(i),j}$ instead of $A$ and $a_{i,j}$) yields

$$
\det (B_\kappa) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{\kappa(i),\sigma(i)}.
$$

(156)
Thus, (155) becomes
\[
\det(AB) = \sum_{\kappa: [n] \to [n]} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \left( \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} b_{\kappa(i),\sigma(i)} \right)
\]
\[
= \sum_{\kappa: [n] \to [n]} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \det(B_{\kappa})
\]
\[
= \sum_{\kappa: [n] \to [n]; \kappa \in S_n} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \frac{\det(B_{\kappa})}{\det(B_{\kappa})}
\]
\[
= \sum_{\kappa \in S_n} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \cdot (-1)^{\kappa} \cdot \det B
\]
\[
= \sum_{\kappa \in S_n} \left( \prod_{i=1}^{n} a_{i,\kappa(i)} \right) \cdot (-1)^{\kappa} \cdot \det B
\]
\[
= \left( \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} a_{i,\sigma(i)} \right) \cdot \det B = \det A \cdot \det B.
\]

This proves Theorem 6.22.

**Remark 6.23.** The analogue of Theorem 6.22 with addition instead of multiplication does not hold. If \(A\) and \(B\) are two \(n \times n\)-matrices for some \(n \in \mathbb{N}\), then \(\det(A + B)\) does usually not equal \(\det A + \det B\).

We shall now show several applications of Theorem 6.22. First, a simple corollary:
Corollary 6.24. Let \( n \in \mathbb{N} \).

(a) If \( B_1, B_2, \ldots, B_k \) are finitely many \( n \times n \)-matrices, then \( \det (B_1 B_2 \cdots B_k) = \prod_{i=1}^{k} \det (B_i) \).

(b) If \( B \) is any \( n \times n \)-matrix, and \( k \in \mathbb{N} \), then \( \det (B^k) = (\det B)^k \).

Proof of Corollary 6.24. Corollary 6.24 easily follows from Theorem 6.22 by induction over \( k \). (The induction base, \( k = 0 \), relies on the fact that the product of 0 matrices is \( I_n \) and has determinant \( \det (I_n) = 1 \).) We leave the details to the reader.

Example 6.25. Recall that the Fibonacci sequence is the sequence \( (f_0, f_1, f_2, \ldots) \) of integers which is defined recursively by \( f_0 = 0 \), \( f_1 = 1 \), and \( f_n = f_{n-1} + f_{n-2} \) for all \( n \geq 2 \). We shall prove that

\[
f_{n+1}f_{n-1} - f_n^2 = (-1)^n \quad \text{for every positive integer } n. \tag{157}
\]

(This is a classical fact known as the Cassini identity and easy to prove by induction, but we shall prove it differently to illustrate the use of determinants.)

Let \( B \) be the \( 2 \times 2 \)-matrix \( \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \) (over the ring \( \mathbb{Z} \)). It is easy to see that \( \det B = -1 \). But for every positive integer \( n \), we have

\[
B^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \tag{158}
\]

Indeed, (158) can be easily proven by induction over \( n \): For \( n = 1 \) it is clear by inspection; if it holds for \( n = N \), then for \( n = N + 1 \) it follows from

\[
B^{N+1} = B^n B^N = \begin{pmatrix} f_{N+1} & f_N \\ f_N & f_{N-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_{N+1} + f_N & f_N \end{pmatrix} \begin{pmatrix} f_N \end{pmatrix} \bigg( \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \bigg) \bigg( \begin{pmatrix} f_{N+1} & f_N \\ f_N & f_{N-1} \end{pmatrix} \bigg)
\]

(by the induction hypothesis)

\[
= \begin{pmatrix} f_{N+1} \cdot 1 + f_N \cdot 1 & f_{N+1} \cdot 1 + f_N \cdot 0 \\ f_N \cdot 1 + f_{N-1} \cdot 1 & f_N \cdot 1 + f_{N-1} \cdot 0 \end{pmatrix}
\]

(by the definition of a product of two matrices)

\[
= \begin{pmatrix} f_{N+1} + f_N & f_{N+1} \\ f_N + f_{N-1} & f_N \end{pmatrix} = \begin{pmatrix} f_{N+2} & f_{N+1} \\ f_{N+1} & f_N \end{pmatrix}
\]

(since \( f_{N+1} + f_N = f_{N+2} \) and \( f_{N+1} + f_{N-1} = f_{N+1} \)).

Now, let \( n \) be a positive integer. Then, (158) yields

\[
\det (B^n) = \det \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = f_{n+1}f_{n-1} - f_n^2.
\]
On the other hand, Corollary 6.24 (b) (applied to \(k = n\)) yields \(\det (B^n) = (-1)^n\). Hence, \(f_{n+1}f_{n-1} - f_n^2 = \det (B^n) = (-1)^n\). This proves (157).

We can generalize (157) as follows:

**Exercise 27.** Let \(a\) and \(b\) be two complex numbers. Let \((x_0, x_1, x_2, \ldots)\) be a sequence of complex numbers such that every \(n \geq 2\) satisfies

\[
x_n = ax_{n-1} + bx_{n-2}.
\]

(We called such sequences \("(a, b)\)-recurrent" in Definition 4.2.) Let \(k \in \mathbb{N}\). Prove that

\[
x_{n+1}x_{n-k-1} - x_nx_{n-k} = (-b)^{n-k-1}(x_{k+2}x_0 - x_{k+1}x_1).
\]

(160)

for every integer \(n > k\).

We notice that (157) can be obtained by applying (160) to \(a = 1, b = 1, x_i = f_i\) and \(k = 0\). Thus, (160) is a generalization of (157). Notice that you could have easily come up with the identity (160) by trying to generalize the proof of (157) we gave; in contrast, it is not that straightforward to guess the general formula (160) from the classical proof of (157) by induction. So the proof of (157) using determinants has at least the advantage of pointing to a generalization.

**Example 6.26.** Let \(n \in \mathbb{N}\). Let \(x_1, x_2, \ldots, x_n\) be \(n\) elements of \(K\), and let \(y_1, y_2, \ldots, y_n\) be \(n\) further elements of \(K\). Let \(A\) be the \(n \times n\)-matrix \((x_iy_j)_{1 \leq i \leq n, 1 \leq j \leq n}\). In Example 6.6 we have shown that \(\det A = 0\) if \(n \geq 2\). We can now prove this in a simpler way.

Namely, let \(n \geq 2\). Define an \(n \times n\)-matrix \(B\) by

\[
B = \begin{pmatrix}
x_1 & 0 & 0 & \cdots & 0 \\
x_2 & 0 & 0 & \cdots & 0 \\
x_3 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
x_n & 0 & 0 & \cdots & 0
\end{pmatrix}.
\]

(Thus, the first column of \(B\) is \((x_1, x_2, \ldots, x_n)^T\), while all other columns are filled with zeroes.) Define an \(n \times n\)-matrix \(C\) by

\[
C = \begin{pmatrix}
y_1 & y_2 & y_3 & \cdots & y_n \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{pmatrix}.
\]

(Thus, the first row of \(C\) is \((y_1, y_2, \ldots, y_n)\), while all other rows are filled with zeroes.)

The second row of \(C\) consists of zeroes (and this second row indeed exists, because \(n \geq 2\)). Thus, Exercise 24 (c) (applied to \(C\) instead of \(A\)) yields \(\det C = 0\).
Similarly, using Exercise 24 (d), we can show that \( \det B = 0 \). Now, Theorem 6.22 (applied to \( B \) and \( C \) instead of \( A \) and \( B \)) yields
\[
\det (BC) = \det B \cdot \det C = 0.
\]
But what is \( BC \)?

Write \( B \) in the form
\[
B = \begin{pmatrix} b_{i,j} \end{pmatrix}_{1 \leq i \leq n, 1 \leq j \leq n'}
\]
and write \( C \) in the form
\[
C = \begin{pmatrix} c_{i,j} \end{pmatrix}_{1 \leq i \leq n, 1 \leq j \leq n'}.
\]
Then, the definition of \( BC \) yields
\[
BC = \left( \sum_{k=1}^{n} b_{i,k} c_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Therefore, for every \((i, j) \in \{1, 2, \ldots, n\}^2\), the \((i, j)\)-th entry of the matrix \( BC \) is
\[
\sum_{k=1}^{n} b_{i,k} c_{k,j} = b_{i,1} \cdot c_{1,j} + \sum_{k=2}^{n} b_{i,k} \cdot c_{k,j} = x_i y_j + \sum_{k=2}^{n} 0 = x_i y_j.
\]

But this is the same as the \((i, j)\)-th entry of the matrix \( A \). Thus, every entry of \( BC \) equals the corresponding entry of \( A \). Hence, \( BC = A \), so that \( \det (BC) = \det A \).

Thus, \( \det A = \det (BC) = 0 \), just as we wanted to show.

**Example 6.27.** Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( \mathbb{K} \), and let \( y_1, y_2, \ldots, y_n \) be \( n \) further elements of \( \mathbb{K} \). Let \( A \) be the \( n \times n \)-matrix
\[
\begin{pmatrix}
(x_i + y_j)_{1 \leq i \leq n, 1 \leq j \leq n}
\end{pmatrix}.
\]
In Example 6.7, we have shown that \( \det A = 0 \) if \( n \geq 3 \).

We can now prove this in a simpler way. The argument is similar to Example 6.26, and so I will be very brief:

Let \( n \geq 3 \). Define an \( n \times n \)-matrix \( B \) by
\[
B = \begin{pmatrix}
x_1 & 1 & 0 & \cdots & 0 \\
x_2 & 1 & 0 & \cdots & 0 \\
x_3 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
x_n & 1 & 0 & \cdots & 0
\end{pmatrix}.
\]
(Thus, the first column of \( B \) is \((x_1, x_2, \ldots, x_n)^T\), the second column is \((1, 1, \ldots, 1)^T\), while all other columns are filled with zeroes.) Define an \( n \times n \)-matrix \( C \) by
\[
C = \begin{pmatrix}
y_1 & y_2 & y_3 & \cdots & y_n \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{pmatrix}.
\]
(Thus, the first row of \( C \) is \((1, 1, \ldots, 1)^T\), the second row is \((y_1, y_2, \ldots, y_n)^T\), while all other rows are filled with zeroes.) It is now easy to show that \( BC = A \) (check this!), but both \( \det B \) and \( \det C \) are 0 (due to having a column or a row filled with zeroes). Thus, again, we obtain \( \det A = 0 \).
Exercise 28. Let \( n \in \mathbb{N} \). Let \( A \) be the \( n \times n \)-matrix
\[
\begin{pmatrix}
0 & 1 & \cdots & n-1 \\
0 & 0 & \cdots & 0 \\
1 & 2 & \cdots & n \\
\vdots & \vdots & \ddots & \vdots \\
(n-1) & n & \cdots & 2n-2
\end{pmatrix}
\]
\(1 \leq \text{row} \leq n, 1 \leq \text{column} \leq n\).

(This matrix is a piece of Pascal’s triangle "rotated by 45°". For example, for \( n = 4 \), we have
\[
A = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 \\
1 & 3 & 6 & 10 \\
1 & 4 & 10 & 20
\end{pmatrix}.
\]

show that \( \det A = 1 \).

The matrix \( A \) in Exercise 28 is one of the so-called Pascal matrices; see [Edestra04] for an enlightening exposition of some of its properties (but beware of the fact that the very first page reveals a significant part of the solution of Exercise 28).

Remark 6.28. There exists a more general notion of a matrix, in which the rows and columns are indexed not necessarily by integers from 1 to \( n \) (for some \( n \in \mathbb{N} \)), but rather by arbitrary objects. For instance, this more general notion allows us to speak of a matrix with two rows labelled "spam" and "eggs", and with three columns labelled 0, 3 and \( \infty \). (It thus has 6 entries, such as the ("spam", 3)-th entry or the ("eggs", \( \infty \))-th entry.) This notion of matrices is more general and more flexible than the one used above (e.g., it allows for infinite matrices), although it has some drawbacks (e.g., notions such as "lower-triangular" are not defined per se, because there might be no canonical way to order the rows and the columns; also, infinite matrices cannot always be multiplied). We might want to define the determinant of such a matrix. Of course, this only makes sense when the rows of the matrix are indexed by the same objects as its columns (this essentially says that the matrix is a "square matrix" in a reasonably general sense). So, let \( X \) be a set, and \( A \) be a "generalized matrix" whose rows and columns are both indexed by the elements of \( X \). We want to define \( \det A \). We assume that \( X \) is finite (indeed, while \( \det A \) sometimes makes sense for infinite \( X \), this only happens under some rather restrictive conditions). Then, we can define \( \det A \) by
\[
\det A = \sum_{\sigma \in S_X} (-1)^\sigma \prod_{i \in X} a_{i,\sigma(i)},
\]
where \( S_X \) denotes the set of all permutations of \( X \). This relies on a definition of \((-1)^\sigma\) for every \( \sigma \in S_X \); fortunately, we have provided such a definition in Exercise [18].

We shall see more about determinants later. So far we have barely scratched the
surface. Huge collections of problems and examples on the computation of determinants can be found in [Prasolov] and [Kratt] (and, if you can be bothered with 100-years-old notation and level of rigor, in [Muir] – one of the most comprehensive collections of “forgotten tales” in mathematics).

Let us finish this section with a brief remark on the geometrical use of determinants.

**Remark 6.29.** Let us consider the Euclidean plane \( \mathbb{R}^2 \) with its Cartesian coordinate system and its origin 0. If \( A = (x_A, y_A) \) and \( B = (x_B, y_B) \) are two points on \( \mathbb{R}^2 \), then the area of the triangle \( 0AB \) is \( \frac{1}{2} \left| \det \begin{pmatrix} x_A & x_B \\ y_A & y_B \end{pmatrix} \right| \). The absolute value here reflects the fact that determinants can be negative, while areas must always be \( \geq 0 \) (although they can be 0 when 0, \( A \) and \( B \) are collinear); however, it makes working with areas somewhat awkward. This can be circumvented by the notion of a signed area. (The signed area of a triangle \( ABC \) is its regular area if the triangle is “directed clockwise”, and otherwise it is the negative of its area.)

The signed area of the triangle \( 0AB \) is \( \frac{1}{2} \det \begin{pmatrix} x_A & x_B \\ y_A & y_B \end{pmatrix} \). (Here, 0 stands for the origin; i.e., “the triangle \( 0AB \)” means the triangle with vertices at the origin, at \( A \) and at \( B \).)

If \( A = (x_A, y_A) \), \( B = (x_B, y_B) \) and \( C = (x_C, y_C) \) are three points in \( \mathbb{R}^2 \), then the signed area of triangle \( ABC \) is \( \frac{1}{2} \det \begin{pmatrix} x_A & x_B & x_C \\ y_A & y_B & y_C \end{pmatrix} \).

Similar formulas hold for tetrahedra: If \( A = (x_A, y_A, z_A) \), \( B = (x_B, y_B, z_B) \) and \( C = (x_C, y_C, z_C) \) are three points in \( \mathbb{R}^3 \), then the signed volume of the tetrahedron \( 0ABC \) is \( \frac{1}{6} \det \begin{pmatrix} x_A & x_B & x_C \\ y_A & y_B & y_C \\ z_A & z_B & z_C \end{pmatrix} \). (Again, take the absolute value for the non-signed volume.) There is a \( 4 \times 4 \) determinant formula for the signed volume of a general tetrahedron \( ABCD \).

One can generalize the notion of a triangle in \( \mathbb{R}^2 \) and the notion of a tetrahedron in \( \mathbb{R}^3 \) to a notion of a simplex in \( \mathbb{R}^n \). Then, one can try to define a notion of volume for these objects. Determinants provide a way to do this. (Obviously, they don’t allow you to define the volume of a general “convex body” like a sphere, and even for simplices it is not a-priori clear that they satisfy the standard properties that one would expect them to have – e.g., that the “volume” of a simplex does not change when one moves this simplex. But for the algebraic part of analytic geometry, they are mostly sufficient. To define “volumes” for general convex bodies, one needs calculus and the theory of integration in \( \mathbb{R}^n \); but this theory, too, uses determinants.)
6.5. The Cauchy-Binet formula

This section is devoted to the Cauchy-Binet formula: a generalization of Theorem 6.22 which is less well-known than the latter, but still comes useful. This formula appears in the literature in various forms; we follow the one on PlanetMath (although we use different notations).

First, we introduce a notation for “picking out some rows of a matrix and throwing away the rest” (and also the analogous thing for columns):

**Definition 6.30.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} \) be an \( n \times m \)-matrix.

(a) If \( i_1, i_2, \ldots, i_u \) are some elements of \( \{1, 2, \ldots, n\} \), then we let \( \text{rows}_{i_1,i_2,\ldots,i_u} A \) denote the \( u \times m \)-matrix \( (a_{ix,j})_{1 \leq x \leq u, 1 \leq j \leq m} \). For instance, if \( A = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \\ d & d' & d'' \end{pmatrix} \),

then \( \text{rows}_{3,1,4} A = \begin{pmatrix} c & c' & c'' \\ a & a' & a'' \\ d & d' & d'' \end{pmatrix} \). For every \( p \in \{1, 2, \ldots, u\} \), we have

\[
\begin{align*}
\text{rows}_{i_1,i_2,\ldots,i_u} A & = (a_{ip,1}, a_{ip,2}, \ldots, a_{ip,m}) \\
& = (\text{the } i_p\text{-th row of } A) \quad \left(\text{since } \text{rows}_{i_1,i_2,\ldots,i_u} A = (a_{ix,j})_{1 \leq x \leq u, 1 \leq j \leq m}\right) \quad \text{(161)}
\end{align*}
\]

Thus, \( \text{rows}_{i_1,i_2,\ldots,i_u} A \) is the \( u \times m \)-matrix whose rows (from top to bottom) are the rows labelled \( i_1, i_2, \ldots, i_u \) of the matrix \( A \).

(b) If \( j_1, j_2, \ldots, j_v \) are some elements of \( \{1, 2, \ldots, m\} \), then we let \( \text{cols}_{j_1,j_2,\ldots,j_v} A \) denote the \( n \times v \)-matrix \( (a_{ij})_{1 \leq i \leq n, 1 \leq y \leq v} \). For instance, if \( A = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix} \),

then \( \text{cols}_{3,2} A = \begin{pmatrix} a'' & a' & a' \\ b'' & b' & b' \\ c'' & c' & c' \end{pmatrix} \). For every \( q \in \{1, 2, \ldots, v\} \), we have

\[
\begin{align*}
\text{cols}_{j_1,j_2,\ldots,j_v} A & = (a_{1,jq}, a_{2,jq}, \ldots, a_{n,jq})^T \\
& = (\text{the } j_q\text{-th column of } A) \quad \left(\text{since } \text{cols}_{j_1,j_2,\ldots,j_v} A = (a_{ij})_{1 \leq i \leq n, 1 \leq y \leq v}\right) \quad \text{(162)}
\end{align*}
\]

Thus, \( \text{cols}_{j_1,j_2,\ldots,j_v} A \) is the \( n \times v \)-matrix whose columns (from left to right) are the columns labelled \( j_1, j_2, \ldots, j_v \) of the matrix \( A \).
Now we can state the **Cauchy-Binet formula**:

**Theorem 6.31.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an \( n \times m \)-matrix, and let \( B \) be an \( m \times n \)-matrix. Then,

\[
\det(AB) = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \det(\text{cols}_{g_1,g_2,\ldots,g_n} A) \cdot \det(\text{rows}_{g_1,g_2,\ldots,g_n} B) .
\]  

(163)

**Remark 6.32.** The summation sign \( \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \) in (163) is an abbreviation for

\[
\sum_{(g_1,g_2,\ldots,g_n) \in \{1,2,\ldots,m\}^n; \\
g_1 < g_2 < \cdots < g_n}
\]

(164)

In particular, if \( n = 0 \), then it signifies a summation over all 0-tuples of elements of \( \{1,2,\ldots,m\} \) (because in this case, the chain of inequalities \( g_1 < g_2 < \cdots < g_n \) is a tautology); such a sum always has exactly one addend (because there is exactly one 0-tuple).

When both \( n \) and \( m \) equal 0, then the notation \( \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \) is slightly confusing: It appears to mean an empty summation (because \( 1 \leq m \) does not hold). But as we said, we mean this notation to be an abbreviation for (164), which signifies a sum with exactly one addend. But this is enough pedantry for now; for \( n > 0 \), the notation \( \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \) fortunately means exactly what it seems to mean.

We shall soon give a detailed proof of Theorem 6.31; see [AigZie, Chapter 29, Theorem] for a different proof. Before we prove Theorem 6.31, let us give some examples for its use. First, here is a simple fact:

\[\text{Note that the formulation of Theorem 6.31 in [AigZie, Chapter 29, Theorem] is slightly different: In our notations, it says that if } A \text{ is an } n \times m \text{-matrix and if } B \text{ is an } m \times n \text{-matrix, then}
\[
\det(AB) = \sum_{|Z|=n; \\
Z \subseteq \{1,2,\ldots,m\}} \det(\text{cols}_Z A) \cdot \det(\text{rows}_Z B),
\]  

(165)

where the matrices \( \text{cols}_Z A \) and \( \text{rows}_Z B \) (for \( Z \) being a subset of \( \{1,2,\ldots,m\} \)) are defined as follows: Write the subset \( Z \) in the form \( \{z_1,z_2,\ldots,z_k\} \) with \( z_1 < z_2 < \cdots < z_k \), and set
\[
\text{cols}_Z A = \text{cols}_{z_1,z_2,\ldots,z_k} A \quad \text{and} \quad \text{rows}_Z B = \text{rows}_{z_1,z_2,\ldots,z_k} B.
\]

(Apart from this, [AigZie] Chapter 29, Theorem] also requires \( n \leq m \); but this requirement is useless.)

The equalities (163) and (165) are equivalent, because the \( n \)-tuples \( (g_1,g_2,\ldots,g_n) \in \{1,2,\ldots,m\}^n \) satisfying \( g_1 < g_2 < \cdots < g_n \) are in a bijection with the subsets \( Z \) of \( \{1,2,\ldots,m\} \) satisfying \( |Z| = n \). (This bijection sends an \( n \)-tuple \( (g_1,g_2,\ldots,g_n) \) to the subset \( \{g_1,g_2,\ldots,g_n\} \).)

The proof of (165) uses the **Lindström-Gessel-Viennot lemma** (which it calls the “lemma of Gessel-Viennot”) and is highly worth reading.)
Lemma 6.33. Let $n \in \mathbb{N}$.

(a) There exists exactly one $n$-tuple $(g_1, g_2, \ldots, g_n) \in \{1, 2, \ldots, n\}^n$ satisfying $g_1 < g_2 < \cdots < g_n$, namely the $n$-tuple $(1, 2, \ldots, n)$.

(b) Let $m \in \mathbb{N}$ be such that $m < n$. Then, there exists no $n$-tuple $(g_1, g_2, \ldots, g_n) \in \{1, 2, \ldots, m\}^n$ satisfying $g_1 < g_2 < \cdots < g_n$.

As for its intuitive meaning, Lemma 6.33 can be viewed as a “pigeonhole principle” for strictly increasing sequences: Part (b) says (roughly speaking) that there is no way to squeeze a strictly increasing sequence $(g_1, g_2, \ldots, g_n)$ of $n$ numbers into the set $\{1, 2, \ldots, m\}$ when $m < n$; part (a) says (again, informally) that the only such sequence for $m = n$ is $(1, 2, \ldots, n)$.

Exercise 29. Give a formal proof of Lemma 6.33. (Do not bother doing this if you do not particularly care about formal proofs and find Lemma 6.33 obvious enough.)

Example 6.34. Let $n \in \mathbb{N}$. Let $A$ and $B$ be two $n \times n$-matrices. It is easy to check that $\text{cols}_{1, 2, \ldots, n} A = A$ and $\text{rows}_{1, 2, \ldots, n} B = B$. Now, Theorem 6.31 (applied to $m = n$) yields

$$
\det(AB) = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq n} \det(\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det(\text{rows}_{g_1, g_2, \ldots, g_n} B). \quad (166)
$$

But Lemma 6.33 (a) yields that there exists exactly one $n$-tuple $(g_1, g_2, \ldots, g_n) \in \{1, 2, \ldots, n\}^n$ satisfying $g_1 < g_2 < \cdots < g_n$, namely the $n$-tuple $(1, 2, \ldots, n)$. Hence, the sum on the right hand side of (166) has exactly one addend: namely, the addend for $(g_1, g_2, \ldots, g_n) = (1, 2, \ldots, n)$. Therefore, this sum simplifies as follows:

$$
\sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq n} \det(\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det(\text{rows}_{g_1, g_2, \ldots, g_n} B)
= \det(\underbrace{\text{cols}_{1, 2, \ldots, n} A}_{= A}) \cdot \det(\underbrace{\text{rows}_{1, 2, \ldots, n} B}_{= B}) = \det A \cdot \det B.
$$

Hence, (166) becomes

$$
\det(AB) = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq n} \det(\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det(\text{rows}_{g_1, g_2, \ldots, g_n} B)
= \det A \cdot \det B.
$$

This, of course, is the statement of Theorem 6.22. Hence, Theorem 6.22 is a particular case of Theorem 6.31.
Example 6.35. Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \) be such that \( m < n \). Thus, Lemma 6.33 (b) shows that there exists no \( n \)-tuple \((g_1, g_2, \ldots, g_n) \in \{1, 2, \ldots, m\}^n\) satisfying \( g_1 < g_2 < \cdots < g_n \).

Now, let \( A \) be an \( n \times m \)-matrix, and let \( B \) be an \( m \times n \)-matrix. Then, Theorem 6.31 yields

\[
\det(AB) = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \det(\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det(\text{rows}_{g_1, g_2, \ldots, g_n} B)
\]

(\text{empty sum})

(\text{since there exists no } n\text{-tuple } (g_1, g_2, \ldots, g_n) \in \{1, 2, \ldots, m\}^n \text{ satisfying } g_1 < g_2 < \cdots < g_n)

= 0.

(167)

This identity allows us to compute \( \det A \) in Example 6.26 in a simpler way: Instead of defining two \( n \times n \)-matrices \( B \) and \( C \) by

\[
B = \begin{pmatrix}
x_1 & 0 & 0 & \cdots & 0 \\
x_2 & 0 & 0 & \cdots & 0 \\
x_3 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
x_n & 0 & 0 & \cdots & 0
\end{pmatrix}
\]

\[
C = \begin{pmatrix}
y_1 & y_2 & y_3 & \cdots & y_n \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{pmatrix}
\]

and \( A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \\ a_{4,1} & a_{4,2} \end{pmatrix} \), it suffices to define an \( n \times 1 \)-matrix \( B' \) by

\[
B' = (x_1, x_2, \ldots, x_n)^T
\]

and a \( 1 \times n \)-matrix \( C' \) by \( C' = (y_1, y_2, \ldots, y_n) \), and argue that \( A = B'C' \). (We leave the details to the reader.) Similarly, Example 6.27 could be dealt with.

Remark 6.36. The equality (167) can also be derived from Theorem 6.22. Indeed, let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \) be such that \( m < n \). Let \( A \) be an \( n \times m \)-matrix, and let \( B \) be an \( m \times n \)-matrix. Notice that \( n - m > 0 \) (since \( m < n \)). Let \( A' \) be the \( n \times n \)-matrix obtained from \( A \) by appending \( n - m \) new columns to the right of \( A \) and filling these columns with zeroes. (For example, if \( n = 4 \) and \( m = 2 \)

\[
A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \\ a_{4,1} & a_{4,2} \end{pmatrix}
\]

and \( A' = \begin{pmatrix} a_{1,1} & a_{1,2} & 0 & 0 \\ a_{2,1} & a_{2,2} & 0 & 0 \\ a_{3,1} & a_{3,2} & 0 & 0 \\ a_{4,1} & a_{4,2} & 0 & 0 \end{pmatrix} \).

Also, let \( B' \) be the \( n \times n \)-matrix obtained from \( B \) by appending \( n - m \) new rows to the bottom of \( B \) and filling these rows with zeroes. (For example, if \( n = 4 \) and \( m = 2 \) and \( B = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} \end{pmatrix} \), then \( B' = \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \).

Then, it is
easy to check that $AB = A'B'$ (in fact, just compare corresponding entries of $AB$ and $A'B'$). But recall that $n - m > 0$. Hence, the matrix $A'$ has a column consisting of zeroes (namely, its last column). Thus, Exercise 24 (d) (applied to $A'$ instead of $A$) shows that $\det(A') = 0$. Now,

$$\det\left(\begin{array}{c}
AB \\
=A'B'
\end{array}\right) = \det(A'B') = \det\left(\begin{array}{c}
A' \\
\end{array}\right) \cdot \det\left(\begin{array}{c}
B' \\
\end{array}\right) = 0$$

(by Theorem 6.22 applied to $A'$ and $B'$ instead of $A$ and $B$)

Thus, (167) is proven again.

Example 6.37. Let us see what Theorem 6.31 says for $n = 1$. Indeed, let $m \in \mathbb{N}$; let $A = (a_1, a_2, \ldots, a_m)$ be a $1 \times m$-matrix (i.e., a row vector of length $m$), and let $B = (b_1, b_2, \ldots, b_m)^T$ be an $m \times 1$-matrix (i.e., a column vector of length $m$). Then, $AB$ is the $1 \times 1$-matrix \( \left( \sum_{k=1}^{m} a_k b_k \right) \). Thus,

$$\det(AB) = \det\left( \sum_{k=1}^{m} a_k b_k \right) = \sum_{k=1}^{m} a_k b_k \quad \text{(by (136))}. \quad (168)$$

What would we obtain if we tried to compute $\det(AB)$ using Theorem 6.31? Theorem 6.31 (applied to $n = 1$) yields

$$\det(AB) = \sum_{1 \leq g_1 \leq m} \det\left( \begin{array}{c}
\text{cols}_{a_1} A \\
\end{array} = \left( a_{g_1} \right) \right) \cdot \det\left( \begin{array}{c}
\text{rows}_{b_1} B \\
\end{array} = \left( b_{g_1} \right) \right)$$

$$= \sum_{g_1=1}^{m} \det\left( a_{g_1} \right) \cdot \det\left( b_{g_1} \right) = \sum_{g_1=1}^{m} a_{g_1} \cdot b_{g_1}. \quad \text{(by (136))}$$

This is, of course, the same result as that of (168) (with the summation index $k$ renamed as $g_1$). So we did not gain any interesting insight from applying Theorem 6.31 to $n = 1$.

Example 6.38. Let us try a slightly less trivial case. Indeed, let $m \in \mathbb{N}$; let

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ a'_1 & a'_2 & \cdots & a'_m \end{pmatrix}$$
be a $2 \times m$-matrix, and let

$$B = \begin{pmatrix} b_1 & b'_1 \\ b_2 & b'_2 \\ \vdots & \vdots \\ b_m & b'_m \end{pmatrix}$$
be an
$m \times 2$-matrix. Then, $AB$ is the $2 \times 2$-matrix

$$
\begin{pmatrix}
\sum_{k=1}^{m} a_k b_k & \sum_{k=1}^{m} a_k b'_k \\
\sum_{k=1}^{m} a'_k b_k & \sum_{k=1}^{m} a'_k b'_k
\end{pmatrix}.
$$

Hence,

$$
\det(AB) = \det \left( \begin{pmatrix}
\sum_{k=1}^{m} a_k b_k & \sum_{k=1}^{m} a_k b'_k \\
\sum_{k=1}^{m} a'_k b_k & \sum_{k=1}^{m} a'_k b'_k
\end{pmatrix} \right)
$$

$$
= \left( \sum_{k=1}^{m} a_k b_k \right) \left( \sum_{k=1}^{m} a'_k b'_k \right) - \left( \sum_{k=1}^{m} a'_k b_k \right) \left( \sum_{k=1}^{m} a_k b'_k \right) \quad \text{(169)}
$$

On the other hand, Theorem 6.31 (now applied to $n = 2$) yields

$$
\det(AB) = \sum_{1 \leq g_1 < g_2 \leq m} \det(\text{cols}_{g_1 \ldots g_2} A) \cdot \det(\text{rows}_{g_1 \ldots g_2} B)
$$

$$
= \sum_{1 \leq i < j \leq m} \det\left( \begin{pmatrix}
\text{cols}_{i \ldots j} A
\end{pmatrix} \right) \cdot \det\left( \begin{pmatrix}
\text{rows}_{i \ldots j} B
\end{pmatrix} \right)
$$

$$
\quad \left( \text{here, we renamed the summation indices } g_1 \text{ and } g_2 \text{ as } i \text{ and } j, \text{ since double subscripts are annoying} \right)
$$

$$
= \sum_{1 \leq i < j \leq m} \det\left( \begin{pmatrix}
a_i & a_j \\
a'_i & a'_j
\end{pmatrix} \right) \cdot \det\left( \begin{pmatrix}
b_i & b'_i \\
b_j & b'_j
\end{pmatrix} \right)
$$

$$
\quad = a_i a'_j - a_i a'_j \cdot (b_i b'_j - b_i b'_j)
$$

Compared with (169), this yields

$$
\left( \sum_{k=1}^{m} a_k b_k \right) \left( \sum_{k=1}^{m} a'_k b'_k \right) - \left( \sum_{k=1}^{m} a'_k b_k \right) \left( \sum_{k=1}^{m} a_k b'_k \right)
$$

$$
\quad = \sum_{1 \leq i < j \leq m} (a_i a'_j - a_i a'_i) \cdot (b_i b'_j - b_i b'_i) \quad \text{(170)}
$$

This identity is called the Binet-Cauchy identity (I am not kidding – look it up on the Wikipedia). It is fairly easy to prove by direct computation; thus, using
Theorem 6.31 to prove it was quite an overkill. However, (170) might not be very easy to come up with, whereas deriving it from Theorem 6.31 is straightforward.

(And Theorem 6.31 is easier to memorize than (170).)

Here is a neat application of (170): If \(a_1, a_2, \ldots, a_m\) and \(a'_1, a'_2, \ldots, a'_m\) are real numbers, then (170) (applied to \(b_k = a_k\) and \(b'_k = a'_k\)) yields

\[
\left( \sum_{k=1}^{m} a_k a_k \right) \left( \sum_{k=1}^{m} a'_k a'_k \right) - \left( \sum_{k=1}^{m} a'_k a_k \right) \left( \sum_{k=1}^{m} a_k a'_k \right) = \sum_{1 \leq i < j \leq m} \left( a_i a'_j - a_i a'_j \right) \geq 0,
\]

so that

\[
\left( \sum_{k=1}^{m} a_k a_k \right) \left( \sum_{k=1}^{m} a'_k a'_k \right) \geq \left( \sum_{k=1}^{m} a'_k a_k \right) \left( \sum_{k=1}^{m} a_k a'_k \right) .
\]

In other words,

\[
\left( \sum_{k=1}^{m} a_k^2 \right) \left( \sum_{k=1}^{m} (a'_k)^2 \right) \geq \left( \sum_{k=1}^{m} a_k a'_k \right)^2 .
\]

This is the famous Cauchy-Schwarz inequality.

Let us now prepare for the proof of Theorem 6.31. First comes a fact which should be fairly clear:

**Proposition 6.39.** Let \(n \in \mathbb{N}\). Let \(a_1, a_2, \ldots, a_n\) be \(n\) integers.

(a) There exists a permutation \(\sigma \in S_n\) such that \(a_{\sigma(1)} \leq a_{\sigma(2)} \leq \cdots \leq a_{\sigma(n)}\).

(b) If \(\sigma \in S_n\) is such that \(a_{\sigma(1)} \leq a_{\sigma(2)} \leq \cdots \leq a_{\sigma(n)}\), then, for every \(i \in \{1, 2, \ldots, n\}\), the value \(a_{\sigma(i)}\) depends only on \(a_1, a_2, \ldots, a_n\) and \(i\) (but not on \(\sigma\)).

(c) Assume that the integers \(a_1, a_2, \ldots, a_n\) are distinct. Then, there is a unique permutation \(\sigma \in S_n\) such that \(a_{\sigma(1)} < a_{\sigma(2)} < \cdots < a_{\sigma(n)}\).

Let me explain why this proposition should be intuitively obvious. Proposition 6.39 (a) says that any list \((a_1, a_2, \ldots, a_n)\) of \(n\) integers can be sorted in weakly increasing order by means of a permutation \(\sigma \in S_n\). Proposition 6.39 (b) says that the result of this sorting process is independent of how the sorting happened (although the permutation \(\sigma\) will sometimes be non-unique). Proposition 6.39 (c) says that if the integers \(a_1, a_2, \ldots, a_n\) are distinct, then the permutation \(\sigma \in S_n\) which sorts the list \((a_1, a_2, \ldots, a_n)\) in increasing order is uniquely determined as well. We required \(a_1, a_2, \ldots, a_n\) to be \(n\) integers for the sake of simplicity, but we could just as well have required them to be elements of any totally ordered set (i.e., any set with a less-than relation satisfying some standard axioms).

The next fact looks slightly scary, but is still rather simple:

\[\text{See the solution of Exercise 50 further below for a formal proof of this proposition.}\]
Lemma 6.40. For every \( n \in \mathbb{N} \), let \([n]\) denote the set \( \{1, 2, \ldots, n\} \).

Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). We let \( E \) be the subset
\[
\{(k_1, k_2, \ldots, k_n) \in [m]^n \mid \text{the integers } k_1, k_2, \ldots, k_n \text{ are distinct}\}
\]
of \([m]^n\). We let \( I \) be the subset
\[
\{(k_1, k_2, \ldots, k_n) \in [m]^n \mid k_1 < k_2 < \ldots < k_n\}
\]
of \([m]^n\). Then, the map
\[
I \times S_n \rightarrow E,
((g_1, g_2, \ldots, g_n), \sigma) \mapsto (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)})
\]
is well-defined and is a bijection.

The intuition for Lemma 6.40 is that every \( n \)-tuple of distinct elements of \( \{1, 2, \ldots, m\} \) can be represented uniquely as a permuted version of a strictly increasing \( n \)-tuple of elements of \( \{1, 2, \ldots, m\} \), and therefore, specifying an \( n \)-tuple of distinct elements of \( \{1, 2, \ldots, m\} \) is tantamount to specifying a strictly increasing \( n \)-tuple of elements of \( \{1, 2, \ldots, m\} \) and a permutation \( \sigma \in S_n \) which says how this \( n \)-tuple is to be permuted. This is not a formal proof, but this should explain why Lemma 6.40 is usually applied throughout mathematics without even mentioning it as a statement. If desired, a formal proof of Lemma 6.40 can be obtained using Proposition 6.39.

Exercise 30. Prove Proposition 6.39 and Lemma 6.40. (Ignore this exercise if you find these two facts sufficiently obvious and are uninterested in the details of their proofs.)

Before we return to Theorem 6.31, let me make a digression about sorting:

Exercise 31. Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \) be such that \( n \geq m \). Let \( a_1, a_2, \ldots, a_n \) be \( n \) integers. Let \( b_1, b_2, \ldots, b_m \) be \( m \) integers. Assume that
\[
a_i \leq b_i \quad \text{for every } i \in \{1, 2, \ldots, m\}.
\]

\begin{align*}
\text{An } n \text{-tuple } (k_1, k_2, \ldots, k_n) \text{ is said to be strictly increasing if and only if } k_1 < k_2 < \cdots < k_n. \\
\text{For instance, the 4-tuple } (4, 1, 6, 2) \text{ of distinct elements of } \{1, 2, \ldots, 7\} \text{ can be specified by specifying the strictly increasing 4-tuple } (1, 2, 4, 6) \text{ (which is its sorted version) and the permutation } \pi \in S_4 \text{ which sends } 1, 2, 3, 4 \text{ to } 3, 1, 4, 2, \text{ respectively (that is, } \pi = (3, 1, 4, 2) \text{ in one-line notation).} \\
\text{In the terminology of Lemma 6.40 the map}
I \times S_n \rightarrow E, 
((g_1, g_2, \ldots, g_n), \sigma) \mapsto (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)})
\end{align*}

sends \((1, 2, 4, 6), \pi)\) to \((4, 1, 6, 2)\).

\begin{align*}
\text{Again, see the solution of Exercise 30 further below for such a proof.}
\end{align*}
Let $\sigma \in S_n$ be such that $a_{\sigma(1)} \leq a_{\sigma(2)} \leq \cdots \leq a_{\sigma(n)}$. Let $\tau \in S_m$ be such that $b_{\tau(1)} \leq b_{\tau(2)} \leq \cdots \leq b_{\tau(m)}$. Then,

$$a_{\sigma(i)} \leq b_{\tau(i)} \quad \text{for every } i \in \{1, 2, \ldots, m\}.$$  

Remark 6.41. Loosely speaking, Exercise 31 says the following: If two lists $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_m)$ of integers have the property that each entry of the first list is $\leq$ to the corresponding entry of the second list (as long as the latter is well-defined), then this property still holds after both lists are sorted in increasing order, provided that we have $n \geq m$ (that is, the first list is at least as long as the second list).

A consequence of Exercise 31 is the following curious fact, known as the “non-messing-up phenomenon” ([Tenner04, Theorem 1]): If we start with a matrix filled with integers, then sort the entries of each row of the matrix in increasing order, and then sort the entries of each column of the resulting matrix in increasing order, then the final matrix still has sorted rows (i.e., the entries of each row are still sorted). That is, the sorting of the columns did not “mess up” the sortedness of the rows. For example, if we start with the matrix

$$\begin{pmatrix} 1 & 3 & 2 & 5 \\ 2 & 1 & 4 & 2 \\ 3 & 1 & 6 & 0 \end{pmatrix},$$

then sorting the entries of each row gives us the matrix

$$\begin{pmatrix} 1 & 2 & 3 & 5 \\ 1 & 2 & 2 & 4 \\ 0 & 1 & 3 & 6 \end{pmatrix},$$

and then sorting the entries of each column results in the matrix

$$\begin{pmatrix} 0 & 1 & 2 & 4 \\ 1 & 2 & 3 & 5 \\ 1 & 2 & 3 & 6 \end{pmatrix}.$$  

The rows of this matrix are still sorted, as the “non-messing-up phenomenon” predicts. To prove this phenomenon in general, it suffices to show that any entry in the resulting matrix is $\leq$ to the entry directly below it (assuming that the latter exists); but this follows easily from Exercise 31.

We are now ready to prove Theorem 6.31.

Proof of Theorem 6.31. We shall use the notations of Lemma 6.40. Write the $n \times m$-matrix $A$ as $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$. Write the $m \times n$-matrix $B$ as $B = (b_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$. The definition of $AB$ thus yields $AB = \left( \sum_{k=1}^{m} a_{i,k}b_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}$. Therefore, (135) (applied to $AB$ and $\sum_{k=1}^{m} a_{i,k}b_{k,j}$ instead of $A$ and $a_{i,j}$) yields

$$\det(AB) = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} \left( \sum_{k=1}^{m} a_{i,k}b_{k,\sigma(i)} \right).$$  

(172)
But for every $\sigma \in S_n$, we have

$$\prod_{i=1}^{n} \left( \sum_{k=1}^{m} a_{i,k} b_{k,i,\sigma(i)} \right) = \sum_{(k_1,k_2,\ldots,k_n) \in [m]^n} \prod_{i=1}^{n} \left( a_{i,k_i} b_{k_i,\sigma(i)} \right) = \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right)$$

(by Lemma 6.20, applied to $m = n$ and $p_{i,k} = a_{i,k} b_{k,i,\sigma(i)}$)

$$= \sum_{(k_1,k_2,\ldots,k_n) \in [m]^n} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right).$$

Hence, (172) rewrites as

$$\det(AB) = \sum_{\sigma \in S_n} (-1)^\sigma \sum_{(k_1,k_2,\ldots,k_n) \in [m]^n} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right)$$

$$= \sum_{\sigma \in S_n} \sum_{(k_1,k_2,\ldots,k_n) \in [m]^n} (-1)^\sigma \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right)$$

$$= \sum_{(k_1,k_2,\ldots,k_n) \in [m]^n} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right).$$

(173)

But every $(k_1,k_2,\ldots,k_n) \in [m]^n$ satisfies

$$\sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{k_i,\sigma(i)} = \det(\text{rows}_{k_1,k_2,\ldots,k_n} B)$$

(174)
Hence, (173) becomes

\[ \det(AB) = \sum_{(k_1, k_2, \ldots, k_n) \in [m]^n} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \left( \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} b_{k_i,\sigma(i)} \right) = \det(\text{rows}_{k_1, k_2, \ldots, k_n} B) \]

\[ = \sum_{(k_1, k_2, \ldots, k_n) \in [m]^n} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \det(\text{rows}_{k_1, k_2, \ldots, k_n} B). \] \tag{175} \]

But for every \((k_1, k_2, \ldots, k_n) \in [m]^n\) satisfying \((k_1, k_2, \ldots, k_n) \not\in E\), we have

\[ \det(\text{rows}_{k_1, k_2, \ldots, k_n} B) = 0 \] \tag{176} \]

Therefore, in the sum on the right hand side of (175), all the addends corresponding to \((k_1, k_2, \ldots, k_n) \in [m]^n\) satisfying \((k_1, k_2, \ldots, k_n) \not\in E\) evaluate to 0. We can therefore remove all these addends from the sum. The remaining addends are those corresponding to \((k_1, k_2, \ldots, k_n) \in E\). Therefore, (175) becomes

\[ \det(AB) = \sum_{(k_1, k_2, \ldots, k_n) \in E} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \det(\text{rows}_{k_1, k_2, \ldots, k_n} B). \] \tag{177} \]

On the other hand, Lemma 6.40 yields that the map

\[ I \times S_n \rightarrow E, \]

\[(g_1, g_2, \ldots, g_n, \sigma) \mapsto (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)}) \]

Proof. Let \((k_1, k_2, \ldots, k_n) \in [m]^n\). Recall that \(B = (b_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}\). Hence, the definition of \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) gives us

\[ \text{rows}_{k_1, k_2, \ldots, k_n} B = (b_{k_i,j})_{1 \leq x \leq n, 1 \leq j \leq n} = (b_{k_i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \]

(here, we renamed the index \(x\) as \(i\)). Hence, (135) (applied to \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) and \(b_{i,j}\) instead of \(A\) and \(a_{i,j}\)) yields

\[ \det(\text{rows}_{k_1, k_2, \ldots, k_n} B) = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} b_{k_i,\sigma(i)}, \]

qed.

Proof of (176): Let \((k_1, k_2, \ldots, k_n) \in [m]^n\) be such that \((k_1, k_2, \ldots, k_n) \not\in E\). Then, the integers \(k_1, k_2, \ldots, k_n\) are not distinct (because \(E\) is the set of all \(n\)-tuples in \([m]^n\) whose entries are distinct). Thus, there exist two distinct elements \(p\) and \(q\) of \([n]\) such that \(k_p = k_q\). Consider these \(p\) and \(q\). But \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) is the \(n \times n\)-matrix whose rows (from top to bottom) are the rows labelled \(k_1, k_2, \ldots, k_n\) of the matrix \(B\). Since \(k_p = k_q\), this shows that the \(p\)-th row and the \(q\)-th row of the matrix \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) are equal. Hence, the matrix \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) has two equal rows (since \(p\) and \(q\) are distinct). Therefore, Exercise 24(e) (applied to \(\text{rows}_{k_1, k_2, \ldots, k_n} B\) instead of \(A\)) yields \(\det(\text{rows}_{k_1, k_2, \ldots, k_n} B) = 0\), qed.
is well-defined and is a bijection. Hence, we can substitute \((g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)})\) for \((k_1, k_2, \ldots, k_n)\) in the sum on the right hand side of (177). We thus obtain

\[
\sum_{(k_1, k_2, \ldots, k_n) \in E} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \det \left( \text{rows}_{k_1,k_2,\ldots,k_n} B \right)
\]

Thus, (177) becomes

\[
\det (AB) = \sum_{(k_1, k_2, \ldots, k_n) \in E} \left( \prod_{i=1}^{n} a_{i,k_i} \right) \det \left( \text{rows}_{k_1,k_2,\ldots,k_n} B \right)
\]

But every \((k_1, k_2, \ldots, k_n) \in [m]^n\) and every \(\sigma \in S_n\) satisfy

\[
\det \left( \text{rows}_{g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}} B \right) = (-1)^{\sigma} \cdot \det \left( \text{rows}_{k_1,k_2,\ldots,k_n} B \right)
\]

Hence, (178) becomes

\[
\det (AB) = \sum_{(g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}, \sigma) \in I \times S_n} \left( \prod_{i=1}^{n} a_{i,g_{\sigma(i)}} \right) \det \left( \text{rows}_{g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}} B \right)
\]

(178)

Proof of (179): Let \((k_1, k_2, \ldots, k_n) \in [m]^n\) and \(\sigma \in S_n\). We have \(\text{rows}_{k_1,k_2,\ldots,k_n} B = (b_{k,i})_{1 \leq i \leq n, 1 \leq j \leq n}\) (as we have seen in one of the previous footnotes) and \(\text{rows}_{g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}} B = (b_{g_{\sigma(i)}j})_{1 \leq i \leq n, 1 \leq j \leq n}\) (for similar reasons). Hence, we can apply Lemma 6.17 (a) to \(\sigma\), \(\text{rows}_{k_1,k_2,\ldots,k_n} B\) and \(\text{rows}_{g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}} B\) instead of \(\kappa, B\) and \(B_{\kappa}\). As a consequence, we obtain

\[
\det \left( \text{rows}_{g_{\sigma(1)}g_{\sigma(2)}\cdots g_{\sigma(n)}} B \right) = (-1)^{\sigma} \cdot \det \left( \text{rows}_{k_1,k_2,\ldots,k_n} B \right)
\]

This proves (179).
But every \((g_1, g_2, \ldots, g_n) \in \mathcal{I}\) satisfies \(\sum_{\sigma \in S_n} \left( \prod_{i=1}^{n} a_{i\sigma(i)} \right) (-1)^{\sigma} = \det (\text{cols}_{g_1, g_2, \ldots, g_n} A)\)\(^{150}\). Hence, \((180)\) becomes

\[
\det(AB) = \sum_{(g_1, g_2, \ldots, g_n) \in \mathcal{I}} \left( \sum_{\sigma \in S_n} \left( \prod_{i=1}^{n} a_{i\sigma(i)} \right) (-1)^{\sigma} \right) \cdot \det (\text{rows}_{g_1, g_2, \ldots, g_n} B)
\]

\[= \det(\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det (\text{rows}_{g_1, g_2, \ldots, g_n} B). \quad (181)\]

Finally, we recall that \(\mathcal{I}\) was defined as the set

\[
\{ (k_1, k_2, \ldots, k_n) \in [m]^n \mid k_1 < k_2 < \cdots < k_n \}.
\]

Thus, summing over all \((g_1, g_2, \ldots, g_n) \in \mathcal{I}\) means the same as summing over all \((g_1, g_2, \ldots, g_n) \in [m]^n\) satisfying \(g_1 < g_2 < \cdots < g_n\). In other words,

\[
\sum_{(g_1, g_2, \ldots, g_n) \in \mathcal{I}} = \sum_{(g_1, g_2, \ldots, g_n) \in [m]^n; g_1 < g_2 < \cdots < g_n} = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m}
\]

(\(^{181}\) an equality between summation signs – hopefully its meaning is obvious). Hence, \((181)\) becomes

\[
\det(AB) = \sum_{1 \leq g_1 < g_2 < \cdots < g_n \leq m} \det (\text{cols}_{g_1, g_2, \ldots, g_n} A) \cdot \det (\text{rows}_{g_1, g_2, \ldots, g_n} B).
\]

This proves Theorem \([6.31]\) \(\square\)

### 6.6. Prelude to Laplace expansion

Next we shall show a fact which will allow us to compute some determinants by induction:

\(^{150}\)Proof. Let \((g_1, g_2, \ldots, g_n) \in \mathcal{I}\). We have \(A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}\). Thus, the definition of \(\text{cols}_{g_1, g_2, \ldots, g_n} A\) yields

\[
\text{cols}_{g_1, g_2, \ldots, g_n} A = (a_{i\sigma(i)})_{1 \leq i \leq n, 1 \leq \sigma(y) \leq n} = (a_{i\sigma(i)})_{1 \leq i \leq n, 1 \leq \sigma \leq n}
\]

(here, we renamed the index \(y\) as \(j\)). Hence, \((135)\) (applied to \(\text{cols}_{g_1, g_2, \ldots, g_n} A\) and \(a_{i\sigma(i)}\) instead of \(A\) and \(a_{ij}\)) yields

\[
\det (\text{cols}_{g_1, g_2, \ldots, g_n} A) = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\sigma \in S_n} \left( \prod_{i=1}^{n} a_{i\sigma(i)} \right) (-1)^{\sigma},
\]

\(\text{qed.}\)
**Theorem 6.42.** Let $n$ be a positive integer. Let $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ be an $n \times n$-matrix. Assume that

$$a_{n,j} = 0 \quad \text{for every } j \in \{1, 2, \ldots, n - 1\}. \quad (182)$$

Then, $\det A = a_{n,n} \cdot \det \left( (a_{i,j})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \right)$.

The assumption (182) says that the last row of the matrix $A$ consists entirely of zeroes, apart from its last entry $a_{n,n}$ (which may and may not be 0). Theorem 6.42 states that, under this assumption, the determinant can be obtained by multiplying this last entry $a_{n,n}$ with the determinant of the $(n - 1) \times (n - 1)$-matrix obtained by removing both the last row and the last column from $A$. For example, for $n = 3$, Theorem 6.42 states that

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{pmatrix} = g \det \begin{pmatrix} a & b \\ d & e \end{pmatrix}.$$ 

Theorem 6.42 is a particular case of *Laplace expansion*, which is a general recursive formula for the determinants that we will encounter further below. But Theorem 6.42 already has noticeable applications of its own, which is why I have chosen to start with this particular case.

The proof of Theorem 6.42 essentially relies on the following fact:

**Lemma 6.43.** Let $n$ be a positive integer. Let $(a_{i,j})_{1 \leq i \leq n-1, 1 \leq j \leq n-1}$ be an $(n - 1) \times (n - 1)$-matrix. Then,

$$\sum_{\sigma \in S_n; \sigma(n) = n} (-1)^\sigma \prod_{i=1}^{n-1} a_{i,\sigma(i)} = \det \left( (a_{i,j})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \right).$$

**Proof of Lemma 6.43.** We define a subset $T$ of $S_n$ by

$$T = \{ \tau \in S_n \mid \tau(n) = n \}.$$ 

(In other words, $T$ is the set of all $\tau \in S_n$ such that if we write $\tau$ in one-line notation, then $\tau$ ends with an $n$.)

Now, we shall construct two mutually inverse maps between $S_{n-1}$ and $T$.

For every $\sigma \in S_{n-1}$, we define a map $\tilde{\sigma}: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by setting

$$\tilde{\sigma}(i) = \begin{cases} \sigma(i), & \text{if } i < n; \\ n, & \text{if } i = n \end{cases} \quad \text{for every } i \in \{1, 2, \ldots, n\}.$$
It is straightforward to see that this map $\hat{\sigma}$ is well-defined and belongs to $T$. Thus, we can define a map $\Phi : S_{n-1} \rightarrow T$ by setting

$$\Phi (\sigma) = \hat{\sigma} \quad \text{for every } \sigma \in S_{n-1}.$$  

Loosely speaking, for every $\sigma \in S_{n-1}$, the permutation $\Phi (\sigma) = \hat{\sigma} \in T$ is obtained by writing $\sigma$ in one-line notation and appending $n$ on its right. For example, if $n = 4$ and if $\sigma \in S_3$ is the permutation that is written as $(2,3,1)$ in one-line notation, then $\Phi (\sigma) = \hat{\sigma}$ is the permutation that is written as $(2,3,1,4)$ in one-line notation.

On the other hand, for every $\gamma \in T$, we define a map $\overline{\gamma} : \{1,2,\ldots,n-1\} \rightarrow \{1,2,\ldots,n-1\}$ by setting

$$\overline{\gamma} (i) = \gamma (i) \quad \text{for every } i \in \{1,2,\ldots,n-1\}.$$  

It is straightforward to see that this map $\overline{\gamma}$ is well-defined and belongs to $S_{n-1}$. Hence, we can define a map $\Psi : T \rightarrow S_{n-1}$ by setting

$$\Psi (\gamma) = \overline{\gamma} \quad \text{for every } \gamma \in T.$$  

Loosely speaking, for every $\gamma \in T$, the permutation $\Psi (\gamma) = \overline{\gamma} \in S_{n-1}$ is obtained by writing $\gamma$ in one-line notation and removing the $n$ (which is the rightmost entry in the one-line notation, because $\gamma (n) = n$). For example, if $n = 4$ and if $\gamma \in S_4$ is the permutation that is written as $(2,3,1,4)$ in one-line notation, then $\Psi (\gamma) = \overline{\gamma}$ is the permutation that is written as $(2,3,1)$ in one-line notation.

The maps $\Phi$ and $\Psi$ are mutually inverse. Thus, the map $\Phi$ is a bijection.

It is fairly easy to see that every $\sigma \in S_{n-1}$ satisfies

$$( -1 )^{\hat{\sigma}} = ( -1 )^{\sigma} \quad (183)$$

and

$$\prod_{i=1}^{n-1} a_i \hat{\sigma} (i) = \prod_{i=1}^{n-1} a_i \sigma (i) \quad (184)$$

151 This should be clear enough from the descriptions we gave using one-line notation. A formal proof is straightforward.

152 Proof of (183). Let $\sigma \in S_{n-1}$. We want to prove that $(-1)^{\hat{\sigma}} = (-1)^{\sigma}$. It is clearly sufficient to show that $\ell (\hat{\sigma}) = \ell (\sigma)$ (because $(-1)^{\hat{\sigma}} = (-1)^{\hat{\sigma}} (\hat{\sigma})$ and $(-1)^{\sigma} = (-1)^{\sigma} (\sigma)$). In order to do so, it is sufficient to show that the inversions of $\hat{\sigma}$ are precisely the inversions of $\sigma$ (because $\ell (\hat{\sigma})$ is the number of inversions of $\hat{\sigma}$, whereas $\ell (\sigma)$ is the number of inversions of $\sigma$).

If $(i,j)$ is an inversion of $\sigma$, then $(i,j)$ is an inversion of $\hat{\sigma}$ (because if $(i,j)$ is an inversion of $\sigma$, then both $i$ and $j$ are $< n$, and thus the definition of $\hat{\sigma}$ yields $\hat{\sigma} (i) = \sigma (i)$ and $\hat{\sigma} (j) = \sigma (j)$). In other words, every inversion of $\sigma$ is an inversion of $\hat{\sigma}$.

On the other hand, let $(u,v)$ be an inversion of $\hat{\sigma}$. We shall prove that $(u,v)$ is an inversion of $\sigma$.

Indeed, $(u,v)$ is an inversion of $\hat{\sigma}$. In other words, $(u,v)$ is a pair of integers satisfying $1 \leq u < v \leq n$ and $\hat{\sigma} (u) > \hat{\sigma} (v)$.

If we had $v = n$, then we would have $\hat{\sigma} (u) > \hat{\sigma} (n) = n$ (by the definition of $\hat{\sigma}$), which would contradict $\hat{\sigma} (u) \in \{1,2,\ldots,n\}$. Thus, we cannot have $v = n$. We therefore
Now,

\[
\sum_{\sigma \in S_n; \sigma(n) = n} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)}
= \sum_{\sigma \in \{\tau \in S_n \mid \tau(n) = n\}} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)}
\]

since \(\{\tau \in S_n \mid \tau(n) = n\} = T\)

\[
= \sum_{\sigma \in T} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)} = \sum_{\sigma \in S_{n-1}} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(\Phi(\sigma))(i)}
\]

(by (183))

This yields

\[
\begin{aligned}
\det \left( (a_{ij})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \right) &= \sum_{\sigma \in S_{n-1}} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)} \\
&= \sum_{\sigma \in S_{n-1}} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)}
\end{aligned}
\]

(by (135), applied to \(n-1\) and \(A\))

\[
\begin{aligned}
\sum_{\sigma \in S_n; \sigma(n) = n} (-1)^{\sigma} \prod_{i=1}^{n-1} a_{i,\sigma(i)} &= \det \left( (a_{ij})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \right) \\

\end{aligned}
\]

have \(v < n\), so that \(v \leq n-1\). Now, \(1 \leq u < v \leq n - 1\). Thus, both \(\sigma(u)\) and \(\sigma(v)\) are well-defined. The definition of \(\widehat{\sigma}\) yields \(\widehat{\sigma}(u) = \sigma(u)\) (since \(u \leq n - 1 < n\)) and \(\widehat{\sigma}(v) = \sigma(v)\) (since \(v \leq n - 1 < n\)), so that \(\sigma(u) = \widehat{\sigma}(u) > \widehat{\sigma}(v) = \sigma(v)\). Thus, \((u, v)\) is a pair of integers satisfying \(1 \leq u < v \leq n - 1\) and \(\sigma(u) > \sigma(v)\). In other words, \((u, v)\) is an inversion of \(\sigma\).

We thus have shown that every inversion of \(\widehat{\sigma}\) is an inversion of \(\sigma\). Combining this with the fact that every inversion of \(\sigma\) is an inversion of \(\widehat{\sigma}\), we thus conclude that the inversions of \(\widehat{\sigma}\) are precisely the inversions of \(\sigma\). As we have already said, this finishes the proof of (183).

Proof of (184): Let \(\sigma \in S_n\). The definition of \(\widehat{\sigma}\) yields \(\widehat{\sigma}(i) = \sigma(i)\) for every \(i \in \{1, 2, \ldots, n - 1\}\).

Thus, \(a_{i,\widehat{\sigma}(i)} = a_{i,\sigma(i)}\) for every \(i \in \{1, 2, \ldots, n - 1\}\). Hence, \(\prod_{i=1}^{n-1} a_{i,\widehat{\sigma}(i)} = \prod_{i=1}^{n-1} a_{i,\sigma(i)}\), qed.
This proves Lemma 6.43.

Proof of Theorem 6.42. Every permutation $\sigma \in S_n$ satisfying $\sigma(n) \neq n$ satisfies

$$a_{n,\sigma(n)} = 0 \quad (185)$$

Proof of (185): Let $\sigma \in S_n$ be a permutation satisfying $\sigma(n) \neq n$. Since $\sigma(n) \in \{1, 2, \ldots, n\}$ and $\sigma(n) \neq n$, we have $\sigma(n) \in \{1, 2, \ldots, n\} \setminus \{n\} = \{1, 2, \ldots, n-1\}$. Hence, (182) (applied to $j = \sigma(n)$) shows that $a_{n,\sigma(n)} = 0$, qed.

6.7. The Vandermonde determinant

An example for an application of Theorem 6.42 is the famous Vandermonde determinant:
**Theorem 6.44.** Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( K \). Then:

(a) We have

\[
\det \left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j).
\]

(b) We have

\[
\det \left( \left( x_j^{n-i} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j).
\]

(c) We have

\[
\det \left( \left( x_j^{j-1} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq j < i \leq n} (x_i - x_j).
\]

(d) We have

\[
\det \left( \left( x_i^{j-1} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq j < i \leq n} (x_i - x_j).
\]

**Remark 6.45.** For \( n = 4 \), the four matrices appearing in Theorem 6.44 are

\[
\begin{pmatrix}
    x_1^3 & x_1^2 & x_1 & 1 \\
    x_2^3 & x_2^2 & x_2 & 1 \\
    x_3^3 & x_3^2 & x_3 & 1 \\
    x_4^3 & x_4^2 & x_4 & 1 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
    x_1^3 & x_2^3 & x_3^3 & x_4^3 \\
    x_1^3 & x_2^3 & x_3^3 & x_4^3 \\
    x_1^3 & x_2^3 & x_3^3 & x_4^3 \\
    x_1^3 & x_2^3 & x_3^3 & x_4^3 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
    1 & x_1 & x_2 & x_3 & x_4 \\
    1 & x_2 & x_3 & x_4 & 1 \\
    1 & x_3 & x_4 & 1 & 1 \\
    1 & x_4 & 1 & 1 & 1 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
    1 & x_1^2 & x_1^3 & x_1 & 1 \\
    1 & x_2^2 & x_2^3 & x_2 & 1 \\
    1 & x_3^2 & x_3^3 & x_3 & 1 \\
    1 & x_4^2 & x_4^3 & x_4 & 1 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
    1 & 1 & 1 & 1 & 1 \\
    x_1 & x_2 & x_3 & x_4 & 1 \\
    x_2 & x_3 & x_4 & 1 & 1 \\
    x_3 & x_4 & 1 & 1 & 1 \\
    x_4 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

It is clear that the second of these four matrices is the transpose of the first; the
fourth is the transpose of the third; and the fourth is obtained from the second by rearranging the rows in opposite order. Thus, the four parts of Theorem 6.44 are rather easily seen to be equivalent. (We shall prove part (a) and derive the others from it.) Nevertheless it is useful to have seen them all.

Theorem 6.44 is a classical result (known as the Vandermonde determinant, although it is unclear whether it has been proven by Vandermonde): Almost all texts on linear algebra mention it (or, rather, at least one of its four parts), although some only prove it in lesser generality. It is a fundamental result that has various applications to abstract algebra, number theory, coding theory, combinatorics and numerical mathematics.

Theorem 6.44 has many known proofs. My favorite proof (of Theorem 6.44 (c) only, but as I said the other parts are easily seen to be equivalent) is given in [Gri10, Theorem 1]. In these notes, I will show another proof, which has the advantage of demonstrating how to use Theorem 6.42.

Example 6.46. Let $x, y, z \in K$. Let

$$A = \begin{pmatrix}
1 & x & x^2 \\
1 & y & y^2 \\
1 & z & z^2
\end{pmatrix}.$$ 

Then, (137) shows that

$$\det A = yz^2 + xy^2 \cdot 1 + x^2 \cdot 1z - 1y^2z - x \cdot 1z^2 - x^2y \cdot 1$$

$$= yz^2 + xy^2 + x^2z - y^2z - xz^2 - x^2y = yz (z - y) + zx (x - z) + xy (y - x).$$

(186)

On the other hand, Theorem 6.44 (c) (applied to $n = 3$, $x_1 = x$, $x_2 = y$ and $x_3 = z$) yields $\det A = (y - x) (z - x) (z - y)$. Compared with (186), this yields

$$(y - x) (z - x) (z - y) = yz (z - y) + zx (x - z) + xy (y - x).$$

(187)

You might have encountered this curious identity as a trick of use in contest problems. When $x, y, z$ are three distinct complex numbers, we can divide (187) by $(y - x) (z - x) (z - y)$, and obtain

$$1 = \frac{yz}{(y - x) (z - x)} + \frac{zx}{(z - y) (x - y)} + \frac{xy}{(x - z) (y - z)}.$$

Before we prove Theorem 6.44, let us see (in greater generality) what happens to the determinant of a matrix if we rearrange the rows in opposite order:

\[\text{For four combinatorial proofs, see } [\text{Gessel79}], [\text{Aigner07}, \S5.3], [\text{Loehr11}, \S12.9] \text{ and } [\text{BenDre07}]. \text{ (Specifically, } [\text{Gessel79}] \text{ and } [\text{BenDre07}] \text{ prove Theorem 6.44 (c), whereas } [\text{Aigner07}, \S5.3] \text{ and } [\text{Loehr11}, \S12.9] \text{ prove Theorem 6.44 (b). But as we will see, the four parts of Theorem 6.44 are easily seen to be equivalent to each other.)}\]
Lemma 6.47. Let $n \in \mathbb{N}$. Let $(a_{i,j})_{1 \leq i, j \leq n}$ be an $n \times n$-matrix. Then,

$$\det \left( \begin{pmatrix} a_{i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right) = (-1)^{n(n-1)/2} \det \left( \begin{pmatrix} a_{i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right).$$

Proof of Lemma 6.47. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. Define a permutation $w_0$ in $S_n$ as in Exercise 17. In the solution of Exercise 17, we have shown that $(-1)^{w_0} = (-1)^{n(n-1)/2}$.

Now, we can apply Lemma 6.17 (a) to $(a_{i,j})_{1 \leq i, j \leq n}$ instead of $B, \kappa$ and $B_x$. As a result, we obtain

$$\det \left( \begin{pmatrix} a_{w_0(i),j} \end{pmatrix}_{1 \leq i, j \leq n} \right) = \left( -1 \right)^{w_0} \cdot \det \left( \begin{pmatrix} a_{i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right) = (-1)^{n(n-1)/2} \det \left( \begin{pmatrix} a_{i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right). \quad (188)$$

But $w_0(i) = n + 1 - i$ for every $i \in \{1, 2, \ldots, n\}$ (by the definition of $w_0$). Thus, (188) rewrites as

$$\det \left( \begin{pmatrix} a_{n+1-i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right) = (-1)^{n(n-1)/2} \det \left( \begin{pmatrix} a_{i,j} \end{pmatrix}_{1 \leq i, j \leq n} \right).$$

This proves Lemma 6.47.

Proof of Theorem 6.44 (a) For every $u \in \{0, 1, \ldots, n\}$, let $A_u$ be the $u \times u$-matrix

$$\begin{pmatrix} x_i^{u-j} \end{pmatrix}_{1 \leq i \leq u, 1 \leq j \leq u}.$$

Now, let us show that

$$\det (A_u) = \prod_{1 \leq i < j \leq u} (x_i - x_j) \quad (189)$$

for every $u \in \{0, 1, \ldots, n\}$.

Proof of (189): We will prove (189) by induction over $u$:

Induction base: The matrix $A_0$ is a $0 \times 0$-matrix and thus has determinant $\det (A_0) = 1$. On the other hand, the product $\prod_{1 \leq i < j \leq 0} (x_i - x_j)$ is an empty product (i.e., a product of 0 elements of $\mathbb{K}$) and thus equals 1 as well. Hence, both $\det (A_0)$ and $\prod_{1 \leq i < j \leq 0} (x_i - x_j)$ equal 1. Thus, $\det (A_0) = \prod_{1 \leq i < j \leq 0} (x_i - x_j)$. In other words, (189) holds for $u = 0$. The induction base is thus complete.

Induction step: Let $U \in \{1, 2, \ldots, n\}$. Assume that (189) holds for $u = U - 1$. We need to prove that (189) holds for $u = U$.

Recall that $A_U = \begin{pmatrix} x_i^{U-j} \end{pmatrix}_{1 \leq i \leq U, 1 \leq j \leq U}$ (by the definition of $A_U$).

For every $(i, j) \in \{1, 2, \ldots, U\}^2$, define $b_{i,j} \in \mathbb{K}$ by

$$b_{i,j} = \begin{cases} x_i^{U-j} - x_i x_i^{U-j-1}, & \text{if } j < U; \\ 1, & \text{if } j = U. \end{cases}$$
Let $B$ be the $U \times U$-matrix $(b_{i,j})_{1 \leq i \leq U, 1 \leq j \leq U}$. For example, if $U = 4$, then

$$\begin{pmatrix}
  x_1^3 & x_1^2 & x_1 & 1 \\
  x_2^3 & x_2^2 & x_2 & 1 \\
  x_3^3 & x_3^2 & x_3 & 1 \\
  x_4^3 & x_4^2 & x_4 & 1 \\
\end{pmatrix} \quad \text{and} \quad
\begin{pmatrix}
  x_1^3 - x_4^2 x_1^2 & x_1^2 - x_4 x_1 & x_1 - x_4 & 1 \\
  x_2^3 - x_4^2 x_2^2 & x_2^2 - x_4 x_2 & x_2 - x_4 & 1 \\
  x_3^3 - x_4^2 x_3^2 & x_3^2 - x_4 x_3 & x_3 - x_4 & 1 \\
  x_4^3 - x_4^2 x_4^2 & x_4^2 - x_4 x_4 & x_4 - x_4 & 1 \\
\end{pmatrix}
= \begin{pmatrix}
  x_1^3 - x_4^2 x_1^2 & x_1^2 - x_4 x_1 & x_1 - x_4 & 1 \\
  x_2^3 - x_4^2 x_2^2 & x_2^2 - x_4 x_2 & x_2 - x_4 & 1 \\
  x_3^3 - x_4^2 x_3^2 & x_3^2 - x_4 x_3 & x_3 - x_4 & 1 \\
  0 & 0 & 0 & 1 \\
\end{pmatrix}.$$

We claim that $\det B = \det (A_U)$. Indeed, here are two ways to prove this:

First proof of $\det B = \det (A_U)$: Exercise 25 (b) shows that the determinant of a $U \times U$-matrix does not change if we subtract a multiple of one of its columns from another column. Now, let us subtract $x_U$ times the 2-nd column of $A_U$ from the 1-st column, then subtract $x_U$ times the 3-rd column of the resulting matrix from the 2-nd column, and so on, all the way until we finally subtract $x_U$ times the $U$-th column of the matrix from the $(U - 1)$-st column\footnote{So, all in all, we subtract the $x_U$-multiple of each column from its neighbor to its left, but the order in which we are doing it (namely, from left to right) is important: It means that the column we are subtracting is unchanged from $A_U$. (If we would be doing these subtractions from right to left instead, then the columns to be subtracting would be changed by the preceding steps.)}. The resulting matrix is $B$ (according to our definition of $B$). Thus, $\det B = \det (A_U)$ (since our subtractions never change the determinant). This proves $\det B = \det (A_U)$.

Second proof of $\det B = \det (A_U)$: Here is another way to prove that $\det B = \det (A_U)$, with some less handwaving.

For every $(i, j) \in \{1, 2, \ldots, U\}^2$, we define $c_{i,j} \in \mathbb{K}$ by

$$c_{i,j} = \begin{cases}
  1, & \text{if } i = j; \\
  -x_U, & \text{if } i = j + 1; \\
  0, & \text{otherwise}
\end{cases}.$$

Let $C$ be the $U \times U$-matrix $(c_{i,j})_{1 \leq i \leq U, 1 \leq j \leq U}$.

For example, if $U = 4$, then

$$C = \begin{pmatrix}
  1 & 0 & 0 & 0 \\
  -x_4 & 1 & 0 & 0 \\
  0 & -x_4 & 1 & 0 \\
  0 & 0 & -x_4 & 1
\end{pmatrix}.$$
The matrix \( C \) is lower-triangular, and thus Exercise 21 shows that its determinant is 
\[
\det C = c_{1,1} c_{2,2} \cdots c_{U,U} = 1.
\]

On the other hand, it is easy to see that \( B = A_U C \) (check this!). Thus, Theorem 6.22 yields 
\[
\det B = \det (A_U) \cdot \det C = \det (A_U).
\]
So we have proven \( \det B = \det (A_U) \) again.

[Remark: It is instructive to compare the two proofs of \( \det B = \det (A_U) \) given above. They are close kin, although they might look different at first. In the first proof, we argued that \( B \) can be obtained from \( A_U \) by subtracting multiples of some columns from others; in the second, we argued that \( B = A_U C \) for a specific lower-triangular matrix \( C \). But a look at the matrix \( C \) makes it clear that multiplying a \( U \times U \)-matrix with \( C \) on the right (i.e., transforming a \( U \times U \)-matrix \( X \) into the matrix \( XC \)) is tantamount to subtracting multiples of some columns from others, in the way we did it to \( A_U \) to obtain \( B \). So the main difference between the two proofs is that the first proof used a step-by-step procedure to obtain \( B \) from \( A_U \), whereas the second proof obtained \( B \) from \( A_U \) by a single-step operation (namely, multiplication by a matrix \( C \)).]

Next, we observe that for every \( j \in \{1, 2, \ldots, U - 1\} \), we have
\[
b_{U,j} = \begin{cases} 
x_{U}^{U-j} - x_{U} x_{U}^{U-j-1}, & \text{if } j < U; \\ 1, & \text{if } j = U \end{cases} 
\]
(by the definition of \( b_{U,j} \))
\[
= x_{U}^{U-j} - x_{U} x_{U}^{U-j-1} 
\]
(since \( j < U \) (since \( j \in \{1, 2, \ldots, U - 1\} \))
\[
= x_{U}^{U-j} - x_{U}^{U-j} = 0.
\]

Hence, Theorem 6.42 (applied to \( U, B \) and \( b_{i,j} \) instead of \( n, A \) and \( a_{i,j} \)) yields
\[
\det B = b_{U,U} \cdot \det \left( (b_{i,j})_{1 \leq i \leq U-1, 1 \leq j \leq U-1} \right). 
\]
(190)

Let \( B' \) denote the \((U - 1) \times (U - 1)\)-matrix \((b_{i,j})_{1 \leq i \leq U-1, 1 \leq j \leq U-1} \).

The definition of \( b_{U,U} \) yields
\[
b_{U,U} = \begin{cases} 
x_{U}^{U-U} - x_{U} x_{U}^{U-U-1}, & \text{if } U < U; \\ 1, & \text{if } U = U \end{cases} 
\]
(by the definition of \( b_{U,U} \))
\[
= 1 \quad \text{(since } U = U\).
\]

Thus, (190) becomes
\[
\det B = b_{U,U} \cdot \det \left( (b_{i,j})_{1 \leq i \leq U-1, 1 \leq j \leq U-1} \right) = \det (B').
\]
Compared with \( \det B = \det (A_U) \), this yields
\[
\det (A_U) = \det (B').
\] (191)

Now, let us take a closer look at \( B' \). Indeed, every \((i, j) \in \{1, 2, \ldots, U - 1\}^2\) satisfies
\[
b_{ij} = \begin{cases} 
x_i^{U-j} - x_Ux_i^{U-j-1}, & \text{if } j < U; \\
1, & \text{if } j = U 
\end{cases}
\]
(by the definition of \(b_{ij}\))
\[
= \begin{cases} 
x_i^{U-j} - x_Ux_i^{U-j-1} \\
= x_i^{U-j-1}
\end{cases}
\]
\[
= (x_i - x_U)x_i^{U-j-1} = (x_i - x_U)x_i^{(U-1)-j}. 
\]
(192)

Hence,
\[
B' = \begin{pmatrix}
\vdots \\
\vdots \\
\vdots
\end{pmatrix}
= \left( (x_i - x_U)x_i^{(U-1)-j} \right)_{1 \leq i \leq U-1, 1 \leq j \leq U-1}.
\]
(193)

On the other hand, the definition of \( A_{U-1} \) yields
\[
A_{U-1} = \left( x_i^{(U-1)-j} \right)_{1 \leq i \leq U-1, 1 \leq j \leq U-1}.
\]
(194)

Now, we claim that
\[
\det (B') = \det (A_{U-1}) \cdot \prod_{i=1}^{U-1} (x_i - x_U).
\]
(195)

Indeed, here are two ways to prove this:

First proof of (195): Comparing the formulas (193) and (194), we see that the matrix \( B' \) is obtained from the matrix \( A_{U-1} \) by multiplying the first row by \( x_1 - x_U \), the second row by \( x_2 - x_U \), and so on, and finally the \((U-1)\)-st row by \( x_{U-1} - x_U \). But every time we multiply a row of a \((U-1) \times (U-1)\)-matrix by some scalar \( \lambda \in \mathbb{K} \), the determinant of the matrix gets multiplied by \( \lambda \) (because of Exercise 24 (g)). Hence, the determinant of \( B' \) is obtained from that of \( A_{U-1} \) by first multiplying by \( x_1 - x_U \), then multiplying by \( x_2 - x_U \), and so on, and finally multiplying with \( x_{U-1} - x_U \). In other words,
\[
\det (B') = \det (A_{U-1}) \cdot \prod_{i=1}^{U-1} (x_i - x_U).
\]
This proves (195).

Second proof of (195): For every \((i, j) \in \{1, 2, \ldots, U - 1\}^2\), we define \(d_{ij} \in K\) by
\[
d_{ij} = \begin{cases} 
  x_i - x_U, & \text{if } i = j; \\
  0, & \text{otherwise.}
\end{cases}
\]

Let \(D\) be the \((U - 1) \times (U - 1)\)-matrix \((d_{ij})_{1 \leq i \leq U - 1, 1 \leq j \leq U - 1}\).

For example, if \(U = 4\), then
\[
D = \begin{pmatrix}
  x_1 - x_4 & 0 & 0 \\
  0 & x_2 - x_4 & 0 \\
  0 & 0 & x_3 - x_4
\end{pmatrix}.
\]

The matrix \(D\) is lower-triangular (actually, diagonal), and thus Exercise 21 shows that its determinant is \(\det D = (x_1 - x_U)(x_2 - x_U) \cdots (x_{U-1} - x_U) = \prod_{i=1}^{U-1} (x_i - x_U)\).

On the other hand, it is easy to see that \(B' = DA_{U-1}\) (check this!). Thus, Theorem 6.22 yields
\[
\det (B') = \det D \cdot \det (A_{U-1}) = \det (A_{U-1}) \cdot \prod_{i=1}^{U-1} (x_i - x_U).
\]

Thus, (195) is proven again.

[Remark: Again, our two proofs of (195) are closely related: the first one reveals \(B'\) as the result of a step-by-step process applied to \(A_{U-1}\), while the second shows how \(B'\) can be obtained from \(A_{U-1}\) by a single multiplication. However, here (in contrast to the proofs of \(\det B = \det (A_U)\)), the step-by-step process involves transforming rows (not columns), and the multiplication is a multiplication from the left (we have \(B' = DA_{U-1}\), not \(B' = A_{U-1}D\)).]

Now, (191) becomes
\[
\det (A_U) = \det (B') = \det (A_{U-1}) \cdot \prod_{i=1}^{U-1} (x_i - x_U).
\]

But we have assumed that (189) holds for \(u = U - 1\). In other words,
\[
\det (A_{U-1}) = \prod_{1 \leq i < j \leq U-1} (x_i - x_j) = \prod_{j=1}^{U-1} \prod_{i=1}^{j-1} (x_i - x_j).
\]

Thus, (196) is proven again.
Hence, (196) yields
\[ \det(A_U) = \det(A_{U-1}) \cdot \prod_{i=1}^{U-1} (x_i - x_U) \]
\[ = \prod_{j=1}^{U-1} \prod_{i=1}^{j-1} (x_i - x_j) \]
\[ = \left( \prod_{j=1}^{U-1} \prod_{i=1}^{j-1} (x_i - x_j) \right) \cdot \prod_{i=1}^{U-1} (x_i - x_U). \]

Compared with
\[ \prod_{1 \leq i < j \leq U} (x_i - x_j) = \prod_{j=1}^{U} \prod_{i=1}^{j-1} (x_i - x_j) = \left( \prod_{j=1}^{U-1} \prod_{i=1}^{j-1} (x_i - x_j) \right) \cdot \prod_{i=1}^{U-1} (x_i - x_U) \]

(here, we have split off the factor for \( j = U \) from the product),
this yields \( \det(A_U) = \prod_{1 \leq i < j \leq U} (x_i - x_j) \). In other words, (189) holds for \( u = U \).

This completes the induction step.

Now, (189) is proven by induction. Hence, we can apply (189) to \( u = n \). As the result, we obtain \( \det(A_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \). Since \( A_n = \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \) (by the definition of \( A_n \)), this rewrites as \( \det\left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \).

This proves Theorem 6.44 (a).

(b) The definition of the transpose of a matrix yields \( \left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right)^T = \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence,
\[ \det\left( \left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right)^T \right) = \det\left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \]
(by Theorem 6.44 (a)). Compared with
\[ \det\left( \left( \left( x_i^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right)^T \right) = \det\left( \left( x_j^{n-i} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) \]
(by Exercise 22, applied to \(A = \left( x_j^{n-i} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \), this yields
\[
\det \left( \left( x_j^{n-i} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]
This proves Theorem 6.44 (b).

(d) Applying Lemma 6.47 to \(a_{i,j} = x_j^{n-i} \), we obtain
\[
\det \left( \left( x_j^{n-(n+1-i)} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = (-1)^n \frac{n(n-1)/2}{\text{det} \left( \left( x_j^{n-i} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j)} .
\]
(by Theorem 6.44 (b))
\[
= (-1)^n \frac{n(n-1)/2}{\prod_{1 \leq i < j \leq n} (x_i - x_j)} .
\]
This rewrites as
\[
\det \left( \left( x_j^{i-1} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = (-1)^n \frac{n(n-1)/2}{\prod_{1 \leq i < j \leq n} (x_i - x_j)} \quad \text{(197)}
\]
(since every \((i,j) \in \{1,2,\ldots,n\}^2 \) satisfies \(x_j^{n-(n+1-i)} = x_j^{i-1} \)).

Now, in the solution to Exercise 17 we have shown that the number of all pairs \((i,j) \) of integers satisfying \(1 \leq i < j \leq n \) is \(n(n-1)/2 \). In other words,
\[
\left( \text{the number of all } (i,j) \in \{1,2,\ldots,n\}^2 \text{ such that } i < j \right) = n(n-1)/2 . \quad \text{(198)}
\]
Now,
\[
\prod_{1 \leq i < j \leq n} (x_i - x_j) = \prod_{1 \leq i < j \leq n} (x_i - x_j) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \quad \text{(here, we renamed the index } (j,i) \text{ as } (i,j) \text{ in the product)}
\]
\[
= \prod_{1 \leq i < j \leq n} ((-1)^n (x_i - x_j))
\]
\[
= (-1)^n \left( \text{the number of all } (i,j) \in \{1,2,\ldots,n\}^2 \text{ such that } i < j \right) \prod_{1 \leq i < j \leq n} (x_i - x_j)
\]
(by (198))
\[
= (-1)^n(n-1)/2 \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]
Compared with (197), this yields \(\det \left( \left( x_j^{i-1} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \right) = \prod_{1 \leq i < j \leq n} (x_i - x_j)\).
This proves Theorem 6.44 (d).

(c) We can derive Theorem 6.44 (c) from Theorem 6.44 (d) in the same way as we derived part (b) from (a).
Remark 6.48. One consequence of Theorem 6.44 is a new solution to Exercise 19 (a):

Namely, let \( n \in \mathbb{N} \) and \( \sigma \in S_n \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( C \) (or of any commutative ring). Then, Theorem 6.44 (a) yields

\[
\det \left( \begin{pmatrix} x_{i-j}^{n-j} & \text{if } j > 1; \\ x_i^n & \text{if } j = 1 \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]

On the other hand, Theorem 6.44 (a) (applied to \( x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)} \) instead of \( x_1, x_2, \ldots, x_n \)) yields

\[
\det \left( \begin{pmatrix} x_{\sigma(i)}^{n-j} & \text{if } j > 1; \\ x_i^n & \text{if } j = 1 \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \prod_{1 \leq i < j \leq n} \left( x_{\sigma(i)} - x_{\sigma(j)} \right) .
\] (199)

But Lemma 6.17 (a) (applied to \( B = \left( x_{i-j}^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \), \( \kappa = \sigma \) and \( B_\kappa = \left( x_{\sigma(i)}^{n-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \)) yields

\[
\det \left( \begin{pmatrix} x_{\sigma(i)}^{n-j} & \text{if } j > 1; \\ x_i^n & \text{if } j = 1 \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = (-1)^{\sigma} \cdot \det \left( \begin{pmatrix} x_{i-j}^{n-j} & \text{if } j > 1; \\ x_i^n & \text{if } j = 1 \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \\
= (-1)^{\sigma} \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]

Compared with (199), this yields

\[
\prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = (-1)^{\sigma} \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]

Thus, Exercise 19 (a) is solved. However, Exercise 19 (b) cannot be solved this way.

Exercise 32. Let \( n \) be a positive integer. Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( K \). Prove that

\[
\det \left( \begin{pmatrix} x_{i-j}^{n-j} & \text{if } j > 1; \\ x_i^n & \text{if } j = 1 \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = (x_1 + x_2 + \cdots + x_n) \prod_{1 \leq i < j \leq n} (x_i - x_j) .
\]
(For example, when \( n = 4 \), this states that)

\[
\begin{vmatrix}
  x_1^4 & x_1^3 & x_1 & 1 \\
  x_2^4 & x_2^3 & x_2 & 1 \\
  x_3^4 & x_3^3 & x_3 & 1 \\
  x_4^4 & x_4^3 & x_4 & 1 \\
\end{vmatrix}
\]

\[
= (x_1 + x_2 + x_3 + x_4) (x_1 - x_2) (x_1 - x_3) (x_1 - x_4) (x_2 - x_3) (x_2 - x_4) (x_3 - x_4).
\]

**Remark 6.49.** We can try to generalize Vandermonde’s determinant. Namely, let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( \mathbb{K} \). Let \( a_1, a_2, \ldots, a_n \) be \( n \) nonnegative integers. Let \( A \) be the \( n \times n \)-matrix

\[
\begin{pmatrix}
  x_1^{a_1} & x_1^{a_2} & \cdots & x_1^{a_n} \\
  x_2^{a_1} & x_2^{a_2} & \cdots & x_2^{a_n} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_n^{a_1} & x_n^{a_2} & \cdots & x_n^{a_n}
\end{pmatrix}
\]

What can we say about \( \det A \)?

Theorem 6.44 says that if \((a_1, a_2, \ldots, a_n) = (n-1, n-2, \ldots, 0)\), then \( \det A = \prod_{1 \leq i < j \leq n} (x_i - x_j) \).

Exercise 32 says that if \( n > 0 \) and \((a_1, a_2, \ldots, a_n) = (n, n-2, n-3, \ldots, 0)\), then \( \det A = (x_1 + x_2 + \cdots + x_n) \prod_{1 \leq i < j \leq n} (x_i - x_j) \).

This suggests a general pattern: We would suspect that for every \((a_1, a_2, \ldots, a_n)\), there is a polynomial \( P_{(a_1, a_2, \ldots, a_n)} \) in \( n \) indeterminates \( X_1, X_2, \ldots, X_n \) such that

\[
\det A = P_{(a_1, a_2, \ldots, a_n)} (x_1, x_2, \ldots, x_n) \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j).
\]

It turns out that this is true. Moreover, this polynomial \( P_{(a_1, a_2, \ldots, a_n)} \) is:

- zero if two of \( a_1, a_2, \ldots, a_n \) are equal;
- homogeneous of degree \( a_1 + a_2 + \cdots + a_n - \binom{n}{2} \);
- symmetric in \( X_1, X_2, \ldots, X_n \).
For example,

\[ P_{(n-1,n-2,...,0)} = 1; \]
\[ P_{(n,n-2,n-3,...,0)} = \sum_{i=1}^{n} X_i = X_1 + X_2 + \cdots + X_n; \]
\[ P_{(n-1,n-k+1,n-k-1,n-k-2,...,0)} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k} \]
for every \( k \in \{0, 1, \ldots, n\}; \)
\[ P_{(n+1,n-2,n-3,...,0)} = \sum_{1 \leq i \leq j \leq n} X_i X_j; \]
\[ P_{(n+1,n-1,n-3,n-4,...,0)} = \sum_{1 \leq i < j \leq n} \left( X_i^2 X_j + X_i X_j^2 \right) + 2 \sum_{1 \leq i < j < k \leq n} X_i X_j X_k. \]

But this polynomial \( P_{(a_1,a_2,...,a_n)} \) can actually be described rather explicitly for general \((a_1, a_2, \ldots, a_n)\); it is a so-called Schur polynomial (at least when \( a_1 > a_2 > \cdots > a_n \); otherwise it is either zero or ± a Schur polynomial). See [Stembr], The Bi-Alternant Formula], [Stan11, Theorem 7.15.1] or [Leeuwen] for the details. (Notice that [Leeuwen] uses the notation \( \varepsilon(\sigma) \) for the sign of a permutation \( \sigma \).

The theory of Schur polynomials shows, in particular, that all coefficients of the polynomial \( P_{(a_1,a_2,...,a_n)} \) have equal sign (which is positive if \( a_1 > a_2 > \cdots > a_n \)).

**Remark 6.50.** There are plenty other variations on the Vandermonde determinant. For instance, one can try replacing the powers \( x_i^{i-1} \) by binomial coefficients \( \binom{x_i}{j-1} \) in Theorem 6.44 (c), at least when these binomial coefficients are well-defined (e.g., when the \( x_1, x_2, \ldots, x_n \) are complex numbers). The result is rather nice: If \( x_1, x_2, \ldots, x_n \) are any \( n \) complex numbers, then

\[ \prod_{1 \leq i < j \leq n} \frac{x_i - x_j}{i - j} = \det \left( \binom{x_i}{j-1} \right)_{1 \leq i \leq n, 1 \leq j \leq n}. \]

(This is proven, e.g., in [Gri10, Corollary 11] and [AndDos] §9, Example 5.) This has the surprising consequence that, whenever \( x_1, x_2, \ldots, x_n \) are \( n \) integers, the product \( \prod_{1 \leq i < j \leq n} \frac{x_i - x_j}{i - j} \) is itself an integer (because it is the determinant of a matrix whose entries are integers). This is a nontrivial result! (A more elementary proof appears in [AndDos] §3, Example 8.)

Another “secret integer” (i.e., rational number which turns out to be an integer for non-obvious reasons) is

\[ \frac{H(a) H(b) H(c) H(a+b+c)}{H(b+c) H(c+a) H(a+b)}. \]

(200)
where $a, b, c$ are three nonnegative integers, and where $H(n)$ (for $n \in \mathbb{N}$) denotes the hyperfactorial of $n$, defined by

$$H(n) = \prod_{k=0}^{n-1} k! = 0! \cdot 1! \cdots (n-1)!.$$ 

I am aware of two proofs of the fact that (200) gives an integer for every $a, b, c \in \mathbb{N}$: One proof is combinatorial, and argues that (200) is the number of plane partitions inside an $a \times b \times c$-box (see [Stan01] last equality in §7.21] for a proof), or, equivalently, the number of rhombus tilings of a hexagon with sidelengths $a, b, c, a, b, c$ (see [Eisenk] for a precise statement). Another proof (see [Gri10, Theorem 0]) exhibits (200) as the determinant of a matrix, again using the Vandermonde determinant!

(None of the references to [Gri10] makes any claim of precedence; actually, I am rather sure of the opposite, i.e., that none of my proofs in [Gri10] are new.)

For some more exercises related to Vandermonde determinants, see [Prasolov, Chapter 1, problems 1.12–1.22]. Here comes one of them:

**Exercise 33.** Let $n$ be a positive integer. Let $x_1, x_2, \ldots, x_n$ be $n$ elements of $\mathbb{K}$. Let $y_1, y_2, \ldots, y_n$ be $n$ elements of $\mathbb{K}$.

(a) For every $m \in \{0, 1, \ldots, n-2\}$, prove that

$$\det \left( \begin{pmatrix} (x_i + y_j)^m \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = 0.$$

(b) Prove that

$$\det \left( \begin{pmatrix} (x_i + y_j)^{n-1} \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \prod_{k=0}^{n-1} \binom{n-1}{k} \left( \prod_{1 \leq i < j \leq n} (x_i - x_j) \right) \left( \prod_{1 \leq i < j \leq n} (y_j - y_i) \right).$$

[Hint: Use the binomial theorem.]

(c) Let $(p_0, p_1, \ldots, p_{n-1}) \in \mathbb{K}^n$ be an $n$-tuple of elements of $\mathbb{K}$. Let $P(X) \in \mathbb{K}[X]$ be the polynomial $\sum_{k=0}^{n-1} p_k X^k$. Prove that

$$\det \left( \begin{pmatrix} (P(x_i + y_j)) \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = p_{n-1}^{n} \prod_{k=0}^{n-1} \binom{n-1}{k} \left( \prod_{1 \leq i < j \leq n} (x_i - x_j) \right) \left( \prod_{1 \leq i < j \leq n} (y_j - y_i) \right).$$

Notice how Exercise 33(a) generalizes Example 6.7 (for $n \geq 3$).
6.8. Invertible elements in commutative rings, and fields

We shall now interrupt our study of determinants for a moment. Let us define the notion of inverses in $\mathbb{K}$. (Recall that $\mathbb{K}$ is a commutative ring.)

**Definition 6.51.** Let $a \in \mathbb{K}$. Then, an element $b \in \mathbb{K}$ is said to be an *inverse* of $a$ if it satisfies $ab = 1$ and $ba = 1$.

Of course, the two conditions $ab = 1$ and $ba = 1$ in Definition 6.51 are equivalent, since $ab = ba$ for every $a \in \mathbb{K}$ and $b \in \mathbb{K}$. Nevertheless, we have given both conditions, because this way the similarity between the inverse of an element of $\mathbb{K}$ and the inverse of a map becomes particularly clear.

For example, the element 1 of $\mathbb{Z}$ is its own inverse (since $1 \cdot 1 = 1$), and the element $-1$ of $\mathbb{Z}$ is its own inverse as well (since $(-1) \cdot (-1) = 1$). These elements 1 and $-1$ are the only elements of $\mathbb{Z}$ which have an inverse in $\mathbb{Z}$. However, in the larger commutative ring $\mathbb{Q}$, every nonzero element $a$ has an inverse (namely, $\frac{1}{a}$).

**Proposition 6.52.** Let $a \in \mathbb{K}$. Then, there exists at most one inverse of $a$ in $\mathbb{K}$.

**Proof of Proposition 6.52.** Let $b$ and $b'$ be any two inverses of $a$ in $\mathbb{K}$. Since $b$ is an inverse of $a$ in $\mathbb{K}$, we have $ab = 1$ and $ba = 1$ (by the definition of an “inverse of $a$”). Since $b'$ is an inverse of $a$ in $\mathbb{K}$, we have $ab' = 1$ and $b'a = 1$ (by the definition of an “inverse of $a$”). Now, comparing $b \cdot \underline{ab'} = b$ with $\underline{ba} \cdot b' = b'$, we obtain $b = b'$.

Let us now forget that we fixed $b$ and $b'$. We thus have shown that if $b$ and $b'$ are two inverses of $a$ in $\mathbb{K}$, then $b = b'$. In other words, any two inverses of $a$ in $\mathbb{K}$ are equal. In other words, there exists at most one inverse of $a$ in $\mathbb{K}$. This proves Proposition 6.52.

**Definition 6.53.** (a) An element $a \in \mathbb{K}$ is said to be *invertible* (or, more precisely, *invertible in $\mathbb{K}$*) if and only if there exists an inverse of $a$ in $\mathbb{K}$. In this case, this inverse of $a$ is unique (by Proposition 6.52), and thus will be called the inverse of $a$ and denoted by $a^{-1}$.

(b) It is clear that the unity 1 of $\mathbb{K}$ is invertible (having inverse 1). Also, the product of any two invertible elements $a$ and $b$ of $\mathbb{K}$ is again invertible (having inverse $(ab)^{-1} = a^{-1}b^{-1}$).

(c) If $a$ and $b$ are two elements of $\mathbb{K}$ such that $a$ is invertible (in $\mathbb{K}$), then we write $\frac{b}{a}$ (or $b/a$) for the product $ba^{-1}$. These fractions behave just as fractions of integers behave: For example, if $a, b, c, d$ are four elements of $\mathbb{K}$ such that $a$ and $c$ are invertible, then $\frac{b}{a} + \frac{d}{c} = \frac{bc + da}{ac}$ and $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$ (and the product $ac$ is indeed invertible, so that the fractions $\frac{bc + da}{ac}$ and $\frac{bd}{ac}$ actually make sense).
Of course, the meaning of the word “invertible” depends on the ring $K$. For example, the integer 2 is invertible in $\mathbb{Q}$ (because $\frac{1}{2}$ is an inverse of 2 in $\mathbb{Q}$), but not invertible in $\mathbb{Z}$ (since it has no inverse in $\mathbb{Z}$). Thus, it is important to say “invertible in $K$” unless the context makes it clear what $K$ is.

One can usually work with invertible elements in commutative rings in the same way as one works with nonzero rational numbers. For example, if $a$ is an invertible element of $K$, then we can define $a^n$ not only for all $n \in \mathbb{N}$, but also for all $n \in \mathbb{Z}$ (by setting $a^n = (a^{-1})^{-n}$ for all negative integers $n$). Of course, when $n = -1$, this is consistent with our notation $a^{-1}$ for the inverse of $a$.

Next, we define the notion of a field.

**Definition 6.54.** A commutative ring $K$ is said to be a field if it satisfies the following two properties:

- We have $0_K \neq 1_K$ (that is, $K$ is not a trivial ring).
- Every element of $K$ is either zero or invertible.

For example, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, whereas polynomial rings such as $\mathbb{Q}[x]$ or $\mathbb{R}[a,b]$ are not fields. For $n$ being a positive integer, the ring $\mathbb{Z}/n\mathbb{Z}$ (that is, the ring of residue classes of integers modulo $n$) is a field if and only if $n$ is a prime number.

Linear algebra (i.e., the study of matrices and linear transformations) becomes much easier (in many aspects) when $K$ is a field. This is one of the main reasons why most courses on linear algebra work over fields only (or begin by working over fields and only later move to the generality of commutative rings). In these

---

157 We are going to use the following simple fact: A commutative ring $K$ is a trivial ring if and only if $0_K = 1_K$.

**Proof.** Assume that $K$ is a trivial ring. Thus, $K$ has only one element. Hence, both $0_K$ and $1_K$ have to equal this one element. Therefore, $0_K = 1_K$.

Now, forget that we assumed that $K$ is a trivial ring. We thus have proven that

$$\text{if } K \text{ is a trivial ring, then } 0_K = 1_K. \quad (201)$$

Conversely, assume that $0_K = 1_K$. Then, every $a \in K$ satisfies $a = a \cdot 1_K = a \cdot 0_K = 0_K \in \{0_K\}$. In other words, $K \subseteq \{0_K\}$. Combining this with $\{0_K\} \subseteq K$, we obtain $K = \{0_K\}$. Hence, $K$ has only one element. In other words, $K$ is a trivial ring.

Now, forget that we assumed that $0_K = 1_K$. We thus have proven that

$$\text{if } 0_K = 1_K, \text{ then } K \text{ is a trivial ring.}$$

Combining this with (201), we conclude that $K$ is a trivial ring if and only if $0_K = 1_K$.

158 For example, the polynomial $x$ is not invertible in $\mathbb{Q}[x]$.

159 Many properties of a matrix over a field (such as its rank) are not even well-defined over an arbitrary commutative ring.
notes we are almost completely limiting ourselves to the parts of matrix theory which work over any commutative ring. Nevertheless, let us comment on how determinants can be computed fast when $\mathbb{K}$ is a field.

**Remark 6.55.** Assume that $\mathbb{K}$ is a field. If $A$ is an $n \times n$-matrix over $\mathbb{K}$, then the determinant of $A$ can be computed using (134)... but in practice, you probably do not want to compute it this way, since the right hand side of (134) contains a sum of $n!$ terms.

It turns out that there is an algorithm to compute $\det A$, which is (usually) a lot faster. It is a version of the Gaussian elimination algorithm commonly used for solving systems of linear equations.

Let us illustrate it on an example: Set

$n = 4$, $\mathbb{K} = \mathbb{Q}$ and $A = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & -1 & 0 & 2 \\ 2 & 4 & -2 & 3 \\ 5 & 1 & 3 & 5 \end{pmatrix}$.

We want to find $\det A$.

Exercise 25(b) shows that if we add a scalar multiple of a column of a matrix to another column of this matrix, then the determinant of the matrix does not change. Now, by adding appropriate scalar multiples of the fourth column of $A$ to the first three columns of $A$, we can make sure that the first three entries of the fourth row of $A$ become zero: Namely, we have to

- add $(-1)$ times the fourth column of $A$ to the first column of $A$;
- add $(-1/5)$ times the fourth column of $A$ to the second column of $A$;
- add $(-3/5)$ times the fourth column of $A$ to the third column of $A$.

These additions can be performed in any order, since none of them “interacts” with any other (more precisely, none of them uses any entries that another of them changes). As we know, none of these additions changes the determinant of the matrix.

Having performed these three additions, we end up with the matrix

$$A' = \begin{pmatrix} 1 & 2 & 3 & 0 \\ -2 & -7/5 & -6/5 & 2 \\ -1 & 17/5 & -19/5 & 3 \\ 0 & 0 & 0 & 5 \end{pmatrix}.$$

We have $\det(A') = \det A$ (because $A'$ was obtained from $A$ by three operations which do not change the determinant). Moreover, the fourth row of $A'$ contains only one nonzero entry – namely, its last entry. In other words, if we write $A'$
in the form \( A' = (a'_{ij})_{1 \leq i \leq 4, 1 \leq j \leq 4} \), then \( a'_{4,j} = 0 \) for every \( j \in \{1, 2, 3\} \). Thus, Theorem 6.42 (applied to 4, \( A' \) and \( a'_{ij} \) instead of \( n, A \) and \( a_{ij} \)) shows that

\[
\det(A') = a'_{4,4} \cdot \det\left(\begin{array}{ccc}
1 & 2 & 3 \\
-2 & -7/5 & -6/5 \\
-1 & 17/5 & -19/5
\end{array}\right)
\]

\[
= 5 \cdot \det\left(\begin{array}{ccc}
1 & 2 & 3 \\
-2 & -7/5 & -6/5 \\
-1 & 17/5 & -19/5
\end{array}\right).
\]

Comparing this with \( \det(A') = \det A \), we obtain

\[
\det A = 5 \cdot \det\left(\begin{array}{ccc}
1 & 2 & 3 \\
-2 & -7/5 & -6/5 \\
-1 & 17/5 & -19/5
\end{array}\right).
\]

Thus, we have reduced the problem of computing \( \det A \) (the determinant of a 4 \( \times \) 4-matrix) to the problem of computing \( \det\left(\begin{array}{ccc}
1 & 2 & 3 \\
-2 & -7/5 & -6/5 \\
-1 & 17/5 & -19/5
\end{array}\right) \) (the determinant of a 3 \( \times \) 3-matrix). Likewise, we can try to reduce the latter problem to the computation of the determinant of a 2 \( \times \) 2-matrix, and then further to the computation of the determinant of a 1 \( \times \) 1-matrix. (In our example, we obtain \( \det A = -140 \) at the end.)

This looks like a viable algorithm (which is, furthermore, fairly fast: essentially as fast as Gaussian elimination). But does it always work? It turns out that it almost always works. There are cases in which it can get “stuck”, and it needs to be modified to deal with these cases.

Namely, what can happen is that the \((n, n)\)-th entry of the matrix \( A \) could be 0.

\[
\begin{pmatrix}
1 & 2 & 3 & 0 \\
0 & -1 & 0 & 2 \\
2 & 4 & -2 & 3 \\
5 & 1 & 3 & 0
\end{pmatrix}
\]

Again, let us observe this on an example: Set \( n = 4 \) and \( A = \begin{pmatrix}
1 & 2 & 3 & 0 \\
0 & -1 & 0 & 2 \\
2 & 4 & -2 & 3 \\
5 & 1 & 3 & 0
\end{pmatrix} \).

Then, we cannot turn the first three entries of the fourth row of \( A \) into zeroes by adding appropriate multiples of the fourth column to the first three columns. (Whatever multiples we add, the fourth row stays unchanged.) However, we can now switch the second row of \( A \) with the fourth row. This operation produces
the matrix \( B = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 5 & 1 & 3 & 0 \\ 2 & 4 & -2 & 3 \\ 0 & -1 & 0 & 2 \end{pmatrix} \), which satisfies \( \det B = - \det A \) (by Exercise 24(a)). Thus, it suffices to compute \( \det B \); and this can be done as above.

The reason why we switched the second row of \( A \) with the fourth row is that the last entry of the second row of \( A \) was nonzero. In general, we need to find a \( k \in \{1, 2, \ldots, n\} \) such that the last entry of the \( k \)-th row of \( A \) is nonzero, and switch the \( k \)-th row of \( A \) with the \( n \)-th row. But what if no such \( k \) exists? In this case, we need another way to compute \( \det A \). It turns out that this is very easy: If there is no \( k \in \{1, 2, \ldots, n\} \) such that the last entry of the \( k \)-th row of \( A \) is nonzero, then the last column of \( A \) consists of zeroes, and thus Exercise 24(d) shows that \( \det A = 0 \).

When \( K \) is not a field, this algorithm breaks (or, at least, can break). Indeed, it relies on the fact that the \( (n, n) \)-th entry of the matrix \( A \) is either zero or invertible. Over a commutative ring \( \mathbb{K} \), it might be neither. For example, if we had tried to work with \( \mathbb{K} = \mathbb{Z} \) (instead of \( \mathbb{K} = \mathbb{Q} \)) in our above example, then we would not be able to add \((-1/5)\) times the fourth column of \( A \) to the second column of \( A \) (because \(-1/5 \notin \mathbb{Z} = \mathbb{K}\)). Fortunately, of course, \( \mathbb{Z} \) is a subset of \( \mathbb{Q} \) (and its operations + and \( \cdot \) are consistent with those of \( \mathbb{Q} \)), so that we can just perform the whole algorithm over \( \mathbb{Q} \) instead of \( \mathbb{Z} \). However, we aren’t always in luck: Some commutative rings \( \mathbb{K} \) cannot be “embedded” into fields in the way \( \mathbb{Z} \) is embedded into \( \mathbb{Q} \). (For instance, \( \mathbb{Z}/4\mathbb{Z} \) cannot be embedded into a field.)

Nevertheless, there are reasonably fast algorithms for computing determinants over any commutative ring; see [Rote, §2].

### 6.9. The Cauchy determinant

Now, we can state another classical formula for a determinant: the Cauchy determinant. In one of its many forms, it says the following:

**Exercise 34.** Let \( n \in \mathbb{N} \). Let \( x_1, x_2, \ldots, x_n \) be \( n \) elements of \( \mathbb{K} \). Let \( y_1, y_2, \ldots, y_n \) be \( n \) elements of \( \mathbb{K} \). Assume that \( x_i + y_j \) is invertible in \( \mathbb{K} \) for every \((i, j) \in \{1, 2, \ldots, n\}^2\). Then, prove that

\[
\det \left( \frac{1}{x_i + y_j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \frac{\prod_{1 \leq i < j \leq n} ((x_i - x_j)(y_i - y_j))}{\prod_{(i, j) \in \{1, 2, \ldots, n\}^2} (x_i + y_j)}.
\]

There is a different version of the Cauchy determinant floating around in literature; it differs from Exercise 34 in that each “\( x_i + y_j \)” is replaced by “\( x_i - y_j \)” , and in that “\( y_i - y_j \)” is replaced by “\( y_j - y_i \)” . Of course, this version is nothing else than the result of applying Exercise 34 to \(-y_1, -y_2, \ldots, -y_n\) instead of \( y_1, y_2, \ldots, y_n \).
Exercise 35. Let \( n \) be a positive integer. Let \( (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix such that \( a_{n,n} \) is invertible (in \( K \)). Prove that

\[
\det \left( (a_{i,j}a_{n,n} - a_{i,n}a_{n,j})_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \right) = a_{n,n}^{n-2} \cdot \det \left( (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \right). \tag{203}
\]

Exercise 35 is known as the Chio pivotal condensation theorem.

Remark 6.56. Exercise 35 gives a way to reduce the computation of an \( n \times n \)-determinant (the one on the right hand side of (203)) to the computation of an \( (n-1) \times (n-1) \)-determinant (the one on the left hand side), provided that \( a_{n,n} \) is invertible. If this reminds you of Remark 6.55, you are thinking right...

Remark 6.57. Exercise 35 holds even without the assumption that \( a_{n,n} \) be invertible, as long as we assume (instead) that \( n \geq 2 \). (If we don’t assume that \( n \geq 2 \), then the \( a_{n,n}^{n-2} \) on the right hand side of (203) will not be defined for non-invertible \( a_{n,n} \).) Proving this is beyond these notes, though.

The next exercises are just diversions; they have nothing to do with invertibility or with the Cauchy determinant.

Exercise 36. Let \( n \in \mathbb{N} \). Let \( (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix. Let \( b_1, b_2, ..., b_n \) be \( n \) elements of \( K \). Prove that

\[
\sum_{k=1}^{n} \det \left( (a_{i,j}b_{\delta_{j,k}})_{1 \leq i \leq n, 1 \leq j \leq n} \right) = (b_1 + b_2 + \cdots + b_n) \det \left( (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \right),
\]

where \( \delta_{j,k} \) means the nonnegative integer \( \begin{cases} 1, & \text{if } j = k; \\ 0, & \text{if } j \neq k \end{cases} \). Equivalently (in more reader-friendly terms): Prove that

\[
\det \begin{pmatrix}
a_{1,1}b_1 & a_{1,2} & \cdots & a_{1,n} \\
a_{2,1}b_2 & a_{2,2} & \cdots & a_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n,1}b_n & a_{n,2} & \cdots & a_{n,n}
\end{pmatrix}
+ \det \begin{pmatrix}
a_{1,1} & a_{1,2}b_1 & \cdots & a_{1,n} \\
a_{2,1} & a_{2,2}b_2 & \cdots & a_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n,1} & a_{n,2}b_n & \cdots & a_{n,n}
\end{pmatrix}
+ \cdots + \det \begin{pmatrix}
a_{1,1} & a_{1,2} & \cdots & a_{1,n}b_1 \\
a_{2,1} & a_{2,2} & \cdots & a_{2,n}b_2 \\
\vdots & \vdots & \ddots & \vdots \\
a_{n,1} & a_{n,2} & \cdots & a_{n,n}b_n
\end{pmatrix}
= (b_1 + b_2 + \cdots + b_n) \det \begin{pmatrix}
a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\
a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n,1} & a_{n,2} & \cdots & a_{n,n}
\end{pmatrix}. 
\]
Exercise 37. Let \( n \in \mathbb{N} \). Let \( a_1, a_2, \ldots, a_n \) be \( n \) elements of \( K \). Let \( x \in K \). Prove that
\[
\det \begin{pmatrix}
    x & a_1 & a_2 & \cdots & a_{n-1} & a_n \\
    a_1 & x & a_2 & \cdots & a_{n-1} & a_n \\
    a_1 & a_2 & x & \cdots & a_{n-1} & a_n \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_1 & a_2 & a_3 & \cdots & x & a_n \\
    a_1 & a_2 & a_3 & \cdots & a_n & x
\end{pmatrix} = (x + \sum_{i=1}^{n} a_i) \prod_{i=1}^{n} (x - a_i).
\]

Exercise 38. Let \( n > 1 \) be an integer. Let \( a_1, a_2, \ldots, a_n \) be \( n \) elements of \( K \). Let \( b_1, b_2, \ldots, b_n \) be \( n \) elements of \( K \). Let \( A \) be the \( n \times n \)-matrix
\[
\begin{pmatrix}
    a_j, & \text{if } i = j; \\
    b_j, & \text{if } i \equiv j + 1 \mod n; \\
    0, & \text{otherwise}
\end{pmatrix}
\]
\[
\begin{pmatrix}
    a_1 & 0 & 0 & \cdots & 0 & b_n \\
    b_1 & a_2 & 0 & \cdots & 0 & 0 \\
    0 & b_2 & a_3 & \cdots & 0 & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    0 & 0 & 0 & \cdots & a_{n-1} & 0 \\
    0 & 0 & 0 & \cdots & b_{n-1} & a_n
\end{pmatrix}.
\]
Prove that
\[
\det A = a_1 a_2 \cdots a_n + (-1)^{n-1} b_1 b_2 \cdots b_n.
\]

Remark 6.58. If we replace \( "i \equiv j + 1 \mod n" \) by \( "i \equiv j + 2 \mod n" \) in Exercise 38, then the pattern can break. For instance, for \( n = 4 \) we have
\[
\det \begin{pmatrix}
    a_1 & 0 & b_3 & 0 \\
    0 & a_2 & 0 & b_4 \\
    b_1 & 0 & a_3 & 0 \\
    0 & b_2 & 0 & a_4
\end{pmatrix} = (a_2 a_4 - b_2 b_4) (a_1 a_3 - b_1 b_3),
\]
which is not of the form \( a_1 a_2 a_3 a_4 \pm b_1 b_2 b_3 b_4 \) anymore. Can you guess for which \( d \in \{1, 2, \ldots, n - 1\} \) we can replace \( "i \equiv j + 1 \mod n" \) by \( "i \equiv j + d \mod n" \) in Exercise 38 and still get a formula of the form \( \det A = a_1 a_2 \cdots a_n \pm b_1 b_2 \cdots b_n \)?

6.10. Laplace expansion

We shall now state Laplace expansion in full. We begin with an example:
Example 6.59. Let $A = (a_{ij})_{1 \leq i \leq 3, 1 \leq j \leq 3}$ be a $3 \times 3$-matrix. From (137), we obtain

$$
\det A = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1}.
$$

(204)

On the right hand side of this equality, we have six terms, each of which contains either $a_{2,1}$ or $a_{2,2}$ or $a_{2,3}$. Let us combine the two terms containing $a_{2,1}$ and factor out $a_{2,1}$, then do the same with the two terms containing $a_{2,2}$, and with the two terms containing $a_{2,3}$. As a result, (204) becomes

$$
\det A = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,1}a_{2,3}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1} = a_{2,1} \left( a_{1,3}a_{3,2} - a_{1,2}a_{3,3} \right) + a_{2,2} \left( a_{1,1}a_{3,3} - a_{1,3}a_{3,1} \right) + a_{2,3} \left( a_{1,2}a_{3,1} - a_{1,1}a_{3,2} \right)
$$

(205)

This is a nice formula with an obvious pattern: The right hand side can be rewritten as $\sum_{q=1}^{3} a_{2,q} \det (B_{2,q})$, where $B_{2,q} = \begin{pmatrix} a_{1,q+2} & a_{1,q+1} \\ a_{3,q+2} & a_{3,q+1} \end{pmatrix}$ (where we set $a_{i,4} = a_{i,1}$ and $a_{i,5} = a_{i,2}$ for all $i \in \{1, 2, 3\}$). Notice the cyclic symmetry (with respect to the index of the column) in this formula! Unfortunately, in this exact form, the formula does not generalize to bigger matrices (or even to smaller: the analogue for a $2 \times 2$-matrix would be $\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = -a_{2,1}a_{1,2} + a_{2,2}a_{1,1}$, which has a minus sign unlike $\sum_{q=1}^{3} a_{2,q} \det (B_{2,q})$).

However, we can slightly modify our formula, sacrificing the cyclic symmetry but making it generalize. Namely, let us rewrite $a_{1,3}a_{3,2} - a_{1,2}a_{3,3}$ as
Let us first define a notation: $A_i$ where $p$ is the $i$-th column. Of course, you could also have guessed $C_i$. The formula (207) is what is usually called the Laplace expansion with respect to the $i$-th column. This formula (unlike (205)) involves powers of $-1$, but it can be generalized.

How? First, we notice that we can find a similar formula by factoring out $a_{1,1}, a_{1,2}, a_{1,3}$ (instead of $a_{2,1}, a_{2,2}, a_{2,3}$); this formula will be

$$
\det A = \sum_{q=1}^{3} (-1)^q a_{1,q} \det (C_{1,q}) ,
$$

where $C_{1,q}$ means the matrix obtained from $A$ by crossing out the 1-st row and the $q$-th column. This formula, and (206), suggest the following generalization: If $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ is an $n \times n$-matrix, and if $p \in \{1, 2, \ldots, n\}$, then

$$
\det A = \sum_{q=1}^{n} (-1)^{p+q} a_{p,q} \det (C_{p,q}) ,
$$

where $C_{p,q}$ means the matrix obtained from $A$ by crossing out the $p$-th row and the $q$-th column. (The only part of this formula which is not easy to guess is $(-1)^{p+q}$; you might need to compute several particular cases to guess this pattern. Of course, you could also have guessed $(-1)^{q-p}$ or $(-1)^{q-p}$ instead, because $(-1)^{p+q} = (-1)^{p-q} = (-1)^{q-p}$.)

The formula (207) is what is usually called the Laplace expansion with respect to the $p$-th row. We will prove it below (Theorem 6.64 (a)), and we will also prove an analogous “Laplace expansion with respect to the $q$-th column” (Theorem 6.64 (b)).

Let us first define a notation:
Definition 6.60. Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m} \) be an \( n \times m \)-matrix. Let \( i_1, i_2, \ldots, i_u \) be some elements of \( \{1, 2, \ldots, n\} \); let \( j_1, j_2, \ldots, j_v \) be some elements of \( \{1, 2, \ldots, m\} \). Then, we define \( \text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} A \) to be the \( u \times v \)-matrix 
\[
\begin{pmatrix}
(a_{ij})_{1 \leq i \leq u, 1 \leq j \leq v}
\end{pmatrix}
\]

When \( i_1 < i_2 < \cdots < i_u \) and \( j_1 < j_2 < \cdots < j_v \), the matrix \( \text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} A \) can be obtained from \( A \) by crossing out all rows other than the \( i_1 \)-th, the \( i_2 \)-th, etc., the \( i_u \)-th row and crossing out all columns other than the \( j_1 \)-th, the \( j_2 \)-th, etc., the \( j_v \)-th column. Thus, in this case, \( \text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} A \) is called a submatrix of \( A \).

For example, if \( n = 3, m = 4 \) and \( A = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & \ell \end{pmatrix} \), then \( \text{sub}_{1,3}^{2,3,4} A = \begin{pmatrix} b & c & d \\ j & k & \ell \end{pmatrix} \) (this is a submatrix of \( A \)) and \( \text{sub}_{2,3}^{3,1,1} A = \begin{pmatrix} g & e & e \\ k & i & i \end{pmatrix} \) (this is not, in general, a submatrix of \( A \)).

The following properties follow trivially from the definitions:

Proposition 6.61. Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an \( n \times m \)-matrix. Recall the notations introduced in Definition 6.30.

(a) We have \( \text{sub}_{1,2,\ldots,m}^{1,2,\ldots,m} A = A \).

(b) If \( i_1, i_2, \ldots, i_u \) are some elements of \( \{1, 2, \ldots, n\} \), then

\[
\text{rows}_{i_1, i_2, \ldots, i_u} A = \text{sub}_{i_1, i_2, \ldots, i_u}^{1,2,\ldots,m} A.
\]

(c) If \( j_1, j_2, \ldots, j_v \) are some elements of \( \{1, 2, \ldots, m\} \), then

\[
\text{cols}_{j_1, j_2, \ldots, j_v} A = \text{sub}_{1,2,\ldots,n}^{j_1, j_2, \ldots, j_v} A.
\]

(d) Let \( i_1, i_2, \ldots, i_u \) be some elements of \( \{1, 2, \ldots, n\} \); let \( j_1, j_2, \ldots, j_v \) be some elements of \( \{1, 2, \ldots, m\} \). Then,

\[
\text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} A = \text{rows}_{i_1, i_2, \ldots, i_u} \left( \text{cols}_{j_1, j_2, \ldots, j_v} A \right) = \text{cols}_{j_1, j_2, \ldots, j_v} \left( \text{rows}_{i_1, i_2, \ldots, i_u} A \right).
\]

(e) Let \( i_1, i_2, \ldots, i_u \) be some elements of \( \{1, 2, \ldots, n\} \); let \( j_1, j_2, \ldots, j_v \) be some elements of \( \{1, 2, \ldots, m\} \). Then,

\[
\left( \text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} A \right)^T = \text{sub}_{i_1, i_2, \ldots, i_u}^{j_1, j_2, \ldots, j_v} \left( A^T \right).
\]

Definition 6.62. Let \( n \in \mathbb{N} \). Let \( a_1, a_2, \ldots, a_n \) be \( n \) objects. Let \( i \in \{1, 2, \ldots, n\} \). Then, \((a_1, a_2, \ldots, \hat{a}_i, \ldots, a_n)\) shall mean the list \((a_1, a_2, \ldots, a_{i-1}, a_{i+1}, a_{i+2}, \ldots, a_n)\).
(that is, the list \( (a_1, a_2, \ldots, a_n) \) with its \( i \)-th entry removed). (Thus, the “hat” over the \( a_i \) means that this \( a_i \) is being omitted from the list.)

For example, \( (1^2, 2^2, \ldots, 5^2, \ldots, 8^2) = (1^2, 2^2, 3^2, 4^2, 6^2, 7^2, 8^2) \).

**Definition 6.63.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an \( n \times m \)-matrix. For every \( i \in \{1, 2, \ldots, n\} \) and \( j \in \{1, 2, \ldots, m\} \), we let \( A_{\sim i, \sim j} \) be the \((n-1) \times (m-1)\)-matrix sub\( _{1,2,\ldots,\hat{i},\ldots,n}^{1,2,\ldots,\hat{j},\ldots,m} \) \( A \). (Thus, \( A_{\sim i, \sim j} \) is the matrix obtained from \( A \) by crossing out the \( i \)-th row and the \( j \)-th column.)

For example, if \( n = m = 3 \) and \( A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \), then \( A_{\sim 1, \sim 2} = \begin{pmatrix} d & f \\ g & i \end{pmatrix} \) and \( A_{\sim 3, \sim 2} = \begin{pmatrix} a & c \\ d & f \end{pmatrix} \).

The notation \( A_{\sim i, \sim j} \) introduced in Definition 6.63 is not very standard; but there does not seem to be a standard one.

Now we can finally state Laplace expansion:

**Theorem 6.64.** Let \( n \in \mathbb{N} \). Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix.

(a) For every \( p \in \{1, 2, \ldots, n\} \), we have

\[
\det A = \sum_{q=1}^{n} (-1)^{p+q} a_{p,q} \det (A_{\sim p, \sim q}).
\]

(b) For every \( q \in \{1, 2, \ldots, n\} \), we have

\[
\det A = \sum_{p=1}^{n} (-1)^{p+q} a_{p,q} \det (A_{\sim p, \sim q}).
\]

Theorem 6.64 (a) is known as the Laplace expansion along the \( p \)-th row (or Laplace expansion with respect to the \( p \)-th row), whereas Theorem 6.64 (b) is known as the Laplace expansion along the \( q \)-th column (or Laplace expansion with respect to the \( q \)-th column). Notice that Theorem 6.64 (a) is equivalent to the formula (207), because the \( A_{\sim p, \sim q} \) in Theorem 6.64 (a) is precisely what we called \( C_{p,q} \) in (207).

We prepare the field for the proof of Theorem 6.64 with a few lemmas.

**Lemma 6.65.** For every \( n \in \mathbb{N} \), let \( [n] \) denote the set \( \{1, 2, \ldots, n\} \).

Let \( n \in \mathbb{N} \). For every \( p \in [n] \), we define a permutation \( g_p \in S_n \) by \( g_p = \text{cyc}_{p,p+1,\ldots,n} \) (where we are using the notations of Definition 5.29).
(a) We have \((g_p(1), g_p(2), \ldots, g_p(n-1)) = (1, 2, \ldots, \hat{p}, \ldots, n)\) for every \(p \in [n]\).

(b) We have \((-1)^{g_p} = (-1)^{n-p}\) for every \(p \in [n]\).

(c) Let \(p \in [n]\). We define a map

\[ g_p' : [n-1] \to [n] \setminus \{p\} \]

by

\[ (g_p'(i) = g_p(i) \quad \text{for every } i \in [n-1]) \]

This map \(g_p'\) is well-defined and bijective.

(d) Let \(p \in [n]\) and \(q \in [n]\). We define a map

\[ T : \{\tau \in S_n \mid \tau(n) = n\} \to \{\tau \in S_n \mid \tau(p) = q\} \]

by

\[ (T(\sigma) = g_q \circ \sigma \circ (g_p)^{-1} \quad \text{for every } \sigma \in \{\tau \in S_n \mid \tau(n) = n\}) \]

Then, this map \(T\) is well-defined and bijective.

\[ \text{Proof of Lemma 6.65} \]

(a) This is trivial.

(b) Let \(p \in [n]\). Exercise 20 (d) (applied to \(k = p + 1\) and \((i_1, i_2, \ldots, i_k) = (p, p+1, \ldots, n)\)) yields

\[ (-1)^{\text{cyc}_{p,p+1,\ldots,n}} = (-1)^{n-(p+1)-1} = (-1)^{n-p-2} = (-1)^{n-p}. \]

Now, \(g_p = \text{cyc}_{p,p+1,\ldots,n}\), so that \((-1)^{g_p} = (-1)^{\text{cyc}_{p,p+1,\ldots,n}} = (-1)^{n-p}\). This proves Lemma 6.65 (b).

(c) We have \(g_p(n) = p\) (since \(g_p = \text{cyc}_{p,p+1,\ldots,n}\)). Also, \(g_p\) is injective (since \(g_p\) is a permutation). Therefore, for every \(i \in [n-1]\), we have

\[ g_p(i) \neq g_p(n) \quad \text{(since } i \neq n \text{ (because } i \in [n-1]\text{) and since } g_p \text{ is injective)} \]

\[ = p, \]

so that \(g_p(i) \in [n] \setminus \{p\}\). This shows that the map \(g_p'\) is well-defined.

To prove that \(g_p'\) is bijective, we can construct its inverse. Indeed, for every \(i \in [n] \setminus \{p\}\), we have

\[ (g_p)^{-1}(i) \neq n \quad \text{(since } i \neq p = g_p(n)) \]

and thus \((g_p)^{-1}(i) \in [n-1]\). Hence, we can define a map \(h : [n] \setminus \{p\} \to [n-1]\) by

\[ (h(i) = (g_p)^{-1}(i) \quad \text{for every } i \in [n] \setminus \{p\}) \]

---
It is straightforward to check that the maps $g'_p$ and $h$ are mutually inverse. Thus, $g'_p$ is bijective. Lemma 6.65(c) is thus proven.

(d) We have $g_p(n) = p$ (since $g_p = cyc_{p,p+1,...,n}$) and $g_q(n) = q$ (similarly). Hence, $(g_p)^{-1}(p) = n$ (since $g_p(n) = p$) and $(g_q)^{-1}(q) = n$ (since $g_q(n) = q$).

For every $\sigma \in \{ \tau \in S_n \mid \tau(n) = n \}$, we have $\sigma(n) = n$ and thus

$$(g_q \circ \sigma \circ (g_p)^{-1})(p) = g_q \left( \sigma \left( \begin{array}{c} g_p^{-1}(p) \\ =n \end{array} \right) \right) = g_q \left( \sigma(n) \right) = g_q(n) = q$$

and therefore $g_q \circ \sigma \circ (g_p)^{-1} \in \{ \tau \in S_n \mid \tau(p) = q \}$. Thus, the map $T$ is well-defined.

We can also define a map

$$Q : \{ \tau \in S_n \mid \tau(p) = q \} \rightarrow \{ \tau \in S_n \mid \tau(n) = n \}$$

by

$$Q(\sigma) = (g_q)^{-1} \circ \sigma \circ g_p \quad \text{for every } \sigma \in \{ \tau \in S_n \mid \tau(p) = q \}.$$

The well-definedness of $Q$ can be checked similarly to how we proved the well-definedness of $T$. It is straightforward to verify that the maps $Q$ and $T$ are mutually inverse. Thus, $T$ is bijective. This completes the proof of Lemma 6.65(d).

Our next step towards the proof of Theorem 6.64 is the following lemma:

**Lemma 6.66.** Let $n \in \mathbb{N}$. Let $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ be an $n \times n$-matrix. Let $p \in \{1, 2, \ldots, n\}$ and $q \in \{1, 2, \ldots, n\}$. Then,

$$\sum_{\sigma \in S_n; \sigma(p) = q} (-1)^\sigma \prod_{i \in \{1, 2, \ldots, n\}; \sigma(i) = i} a_{i,\sigma(i)} = (-1)^{p+q} \det(A_{p,\bar{q}}) \cdot$$

**Proof of Lemma 6.66.** Let us use all notations introduced in Lemma 6.65.

We have $p \in \{1, 2, \ldots, n\} = [n]$. Hence, $g_p$ is well-defined. Similarly, $g_q$ is well-defined. We have

$$(g_p(1), g_p(2), \ldots, g_p(n-1)) = (1, 2, \ldots, \hat{p}, \ldots, n) \quad (208)$$

(by Lemma 6.65(a)) and

$$(g_q(1), g_q(2), \ldots, g_q(n-1)) = (1, 2, \ldots, \hat{q}, \ldots, n) \quad (209)$$
(by Lemma 6.65 (a), applied to q instead of p). Now, the definition of $A_{\sim p, \sim q}$ yields

$$A_{\sim p, \sim q} = \text{sub}_{1,2,\ldots,n}^{1,2,\ldots,n} A = \text{sub}_{p, q}^{\sigma(1), \sigma(2), \ldots, \sigma(n-1)}_{p, q} A \text{ (by (208) and (209))}$$

$$= \left( a_{\sigma(p)(x), \sigma(q)(y)} \right)_{1 \leq x \leq n - 1, 1 \leq y \leq n - 1} \text{ (by the definition of sub}_{p, q}^{\sigma(1), \sigma(2), \ldots, \sigma(n-1)}_{p, q} A)$$

$$= \left( a_{\sigma(p)(i), \sigma(q)(j)} \right)_{1 \leq i \leq n - 1, 1 \leq j \leq n - 1} \text{ (210)}$$

(here, we renamed the index $(x, y)$ as $(i, j)$).

Also, $[n]$ is nonempty (since $p \in [n]$), and thus we have $n > 0$.

Now, let us recall the map $T : \{ \tau \in S_n \mid \tau(n) = n \} \rightarrow \{ \tau \in S_n \mid \tau(p) = q \}$ defined in Lemma 6.65 (d). Lemma 6.65 (d) says that this map $T$ is well-defined and bijective. Every $\sigma \in \{ \tau \in S_n \mid \tau(n) = n \}$ satisfies

$$(-1)^{T(\sigma)} = (-1)^{p+q} \cdot (-1)^{\sigma} \text{ (211)}$$
161 and

\[ \prod_{i \in \{1, 2, \ldots, n\}, i \neq p} a_{i, (T(\sigma))(i)} = \prod_{i=1}^{n-1} a_{g_p(i), g_q(\sigma(i))} \]  

(212)

162

Proof of (211). Let \( \sigma \in \{ \tau \in S_n \mid \tau(n) = n \} \). Applying Lemma 6.65 (b) to \( q \) instead of \( p \), we obtain \((-1)^{\delta_q} = (-1)^{n-q} = (-1)^{n+q} \) (since \( n-q \equiv n+q \) mod 2).

The definition of \( T(\sigma) \) yields \( T(\sigma) = g_q \circ \sigma \circ (g_p)^{-1} \). Thus,

\[ T(\sigma) \circ g_p = g_q \circ \sigma \circ (g_p)^{-1} \circ g_p = g_q \circ \sigma , \]

so that

\[ (-1)^{T(\sigma)g_p} = (-1)^{\delta_q} \cdot (-1)^{\tau} \] (by (113), applied to \( g_q \) and \( \sigma \) instead of \( \sigma \) and \( \tau \))

\[ = (-1)^{n+q} \cdot (-1)^{\sigma} . \]

Compared with

\[ (-1)^{T(\sigma)g_p} = (-1)^{T(\sigma)} \cdot (-1)^{\delta_q} \] (by (113), applied to \( T(\sigma) \) and \( g_p \) instead of \( \sigma \) and \( \tau \))

\[ = (-1)^{T(\sigma)} \cdot (-1)^{n-p} , \]

this yields

\[ (-1)^{T(\sigma)} \cdot (-1)^{n-p} = (-1)^{n+q} \cdot (-1)^{\sigma} . \]

We can divide both sides of this equality by \((-1)^{n-p}\) (since \((-1)^{n-p} \in \{1, -1\} \) is clearly an invertible integer), and thus we obtain

\[ (-1)^{T(\sigma)} = \frac{(-1)^{n+q} \cdot (-1)^{\sigma}}{(-1)^{n-p}} = \frac{(-1)^{n+q} \cdot (-1)^{\delta_q}}{(-1)^{n-p}} \cdot (-1)^{\sigma} = (-1)^{p+q} \cdot (-1)^{\sigma} \]

(since \((-1)^{n-p} = (-1)^{p+q} \)

This proves (211).

162 Proof of (212). Let \( \sigma \in \{ \tau \in S_n \mid \tau(n) = n \} \). Let us recall the map \( g'_p : [n-1] \to [n] \setminus \{p\} \) introduced in Lemma 6.65 (f). Lemma 6.65 (e) says that this map \( g'_p \) is well-defined and bijective. In other words, \( g'_p \) is a bijection.

Let \( i \in [n-1] \). Then, \( g'_p(i) = g_p(i) \) (by the definition of \( g'_p \)). Also, the definition of \( T \) yields \( T(\sigma) = g_q \circ \sigma \circ (g_p)^{-1} \), so that

\[ \left( T(\sigma) \right) \left( g'_p(i) \right) = \left( g_q \circ \sigma \circ (g_p)^{-1} \right) \left( g_p(i) \right) = g_q \left( \sigma \left( \frac{(g_p)^{-1} \left( g_p(i) \right)}{g_p(i)} \right) \right) = g_q \left( \sigma \left( i \right) \right) . \]
From $g'_p(i) = g_p(i)$ and $(T(\sigma))(g'_p(i)) = g_q(\sigma(i))$, we obtain

$$a_{g'_p(i), T(\sigma)}(g'_p(i)) = a_{g_p(i), g_q(\sigma(i))}.$$  \hspace{1cm} (213)

Now, let us forget that we fixed $i$. We thus have proven (213) for every $i \in [n - 1]$. But now, we have

$$\prod_{i \in \{1, 2, \ldots, n\}; \ i \neq p} a_i(T(\sigma))(i)$$

$$= \prod_{i \in [n]; \ i \neq p} a_i(T(\sigma))(i) = \prod_{i \in [n \setminus \{p\}]} a_i(T(\sigma))(i) = \prod_{i \in [n-1]} a_{g'_p(i), T(\sigma)}(g'_p(i))$$

\hspace{1cm} (by (213))

$$= \prod_{i=1}^{n-1} a_{g_p(i), g_q(\sigma(i))}.$$  

This proves (212).
Now,
\[
\sum_{\sigma \in S_n; \sigma'(p)=q} (-1)^\sigma \prod_{i\in\{1,2,\ldots,n\}; i\neq p} a_{i,\sigma'(i)} = \sum_{\sigma \in \{\tau \in S_n \mid \tau(p)=q\}} \sum_{\tau \in S_n; \tau(n)=n} (-1)^{T(\sigma)} \prod_{i\in\{1,2,\ldots,n\}; i\neq p} a_{i,T(\sigma)(i)} = \sum_{\sigma \in S_n; \sigma(n)=n} (-1)^{p+q} \prod_{i=1}^{n-1} a_{g_p(i),g_q(\sigma(i))}
\]
\[\text{here, we have substituted } T(\sigma) \text{ for } \sigma \text{ in the sum, since the map } T: \{\tau \in S_n \mid \tau(n)=n\} \to \{\tau \in S_n \mid \tau(p)=q\} \text{ is a bijection.}
\]
\[(\sum_{\sigma \in S_n; \sigma(n)=n} (-1)^{p+q} (-1)^{n-1} \prod_{i=1}^{n-1} a_{g_p(i),g_q(\sigma(i))} = \sum_{\sigma \in S_n; \sigma(n)=n} (-1)^{p+q} \prod_{i=1}^{n-1} a_{g_p(i),g_q(\sigma(i))} = \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} \text{ (by Lemma 6.43, applied to } a_{g_p(i),g_q(j)} \text{ instead of } a_{i,j})
\]
\[= (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1} = (-1)^{p+q} \det\left(\begin{array}{c}
\end{array}\right)_{1 \leq i \leq n-1, 1 \leq j \leq n-1}
\]

This proves Lemma 6.66.

Now, we can finally prove Theorem 6.64.
Proof of Theorem 6.64 (a) Let $p \in \{1, 2, \ldots, n\}$. From (135), we obtain

$$\det A = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} a_{i, \sigma(i)}$$

$$= \sum_{q \in \{1, 2, \ldots, n\}} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^\sigma \prod_{i \in \{1, 2, \ldots, n\} \setminus \{p\}} a_{i, \sigma(i)}$$

because for every $\sigma \in S_n$, there exists exactly one $q \in \{1, 2, \ldots, n\}$ satisfying $\sigma(p) = q$

$$= \sum_{q \in \{1, 2, \ldots, n\}} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^\sigma \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)}$$

(here, we have split off the factor for $i=p$ from the product)

$$= \sum_{q=1}^{n} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^\sigma a_{p, q} \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)}$$

$$= \sum_{q=1}^{n} a_{p, q} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^\sigma \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)}$$

$$= (-1)^{p+q} \det(A_{\sim p, \sim q})$$

(by Lemma 6.66)

$$= \sum_{q=1}^{n} a_{p, q} (-1)^{p+q} \det(A_{\sim p, \sim q}) = \sum_{q=1}^{n} (-1)^{p+q} a_{p, q} \det(A_{\sim p, \sim q}) .$$

This proves Theorem 6.64 (a).
(b) Let \( q \in \{1, 2, \ldots, n\} \). From (135), we obtain

\[
\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} a_{i, \sigma(i)} = \sum_{p \in \{1, 2, \ldots, n\}} \sum_{\sigma \in S_n; \sigma^{-1}(q) = p} (-1)^{\sigma} \prod_{i \in \{1, 2, \ldots, n\}} a_{i, \sigma(i)}
\]

because for every \( \sigma \in S_n \), there exists exactly one \( p \in \{1, 2, \ldots, n\} \) satisfying \( \sigma^{-1}(q) = p \)

\[
= \sum_{p \in \{1, 2, \ldots, n\}} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^{\sigma} \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{p, \sigma(p)} = a_{p, q} \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)} \quad \text{(since \( \sigma(p) = q \))}
\]

(here, we have split off the factor for \( i = p \) from the product)

\[
= \sum_{p=1}^{n} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^{\sigma} a_{p, q} \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)} = a_{p, q} \sum_{\sigma \in S_n; \sigma(p) = q} (-1)^{\sigma} \prod_{i \in \{1, 2, \ldots, n\}; i \neq p} a_{i, \sigma(i)}
\]

(by Lemma 6.66)

\[
= n \cdot a_{p, q} \cdot (-1)^{p+q} \det (A_{\sim p, \sim q})
\]

\[
= \sum_{p=1}^{n} a_{p, q} (-1)^{p+q} \det (A_{\sim p, \sim q}) = \sum_{p=1}^{n} (-1)^{p+q} a_{p, q} \det (A_{\sim p, \sim q}).
\]

This proves Theorem 6.64 (b). \( \square \)

The reader can easily see how Theorem 6.64 (b) could be (alternatively) proven using Theorem 6.64 (a) and Exercise 22 and how Theorem 6.42 could be seen as a
particular case of Theorem 6.64 (a).

**Remark 6.67.** Some books use Laplace expansion to define the notion of a determinant. For example, one can define the determinant of a square matrix recursively, by setting the determinant of the $0 \times 0$-matrix to be 1, and defining the determinant of an $n \times n$-matrix $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ (with $n > 0$) to be

$$
\sum_{q=1}^{n} (-1)^{1+q} a_{1,q} \det (A_{1,\sim q}) \quad (\text{assuming that determinants of } (n-1) \times (n-1)\text{-matrices such as } A_{1,\sim q} \text{ are already defined}).
$$

Of course, this leads to the same notion of determinant as the one we are using, because of Theorem 6.64 (a).

### 6.11. Tridiagonal determinants

In this section, we shall study the so-called tridiagonal matrices: a class of matrices whose all entries are zero everywhere except in the “direct proximity” of the diagonal (more specifically: on the diagonal and “one level below and one level above”). We shall find recursive formulas for the determinants of these matrices. These formulas are a simple example of an application of Laplace expansion, but also interesting in their own right.

**Definition 6.68.** Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be $n$ elements of $\mathbb{K}$. Let $b_1, b_2, \ldots, b_{n-1}$ be $n-1$ elements of $\mathbb{K}$ (where we take the position that “$-1$ elements of $\mathbb{K}$” means “no elements of $\mathbb{K}$”). Let $c_1, c_2, \ldots, c_{n-1}$ be $n-1$ elements of $\mathbb{K}$. We now set

$$
A = \begin{pmatrix}
    a_1 & b_1 & 0 & \cdots & 0 & 0 & 0 \\
    c_1 & a_2 & b_2 & \cdots & 0 & 0 & 0 \\
    0 & c_2 & a_3 & \cdots & 0 & 0 & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
    0 & 0 & 0 & \cdots & a_{n-2} & b_{n-2} & 0 \\
    0 & 0 & 0 & \cdots & c_{n-2} & a_{n-1} & b_{n-1} \\
    0 & 0 & 0 & \cdots & 0 & c_{n-1} & a_n
\end{pmatrix}.
$$

(More formally,

$$
A = \begin{pmatrix}
    a_i, & \text{if } i = j; \\
    b_i, & \text{if } i = j - 1; \\
    c_i, & \text{if } i = j + 1; \\
    0, & \text{otherwise}
\end{pmatrix}_{1 \leq i \leq n, 1 \leq j \leq n}
$$

)

The matrix $A$ is called a tridiagonal matrix.

We shall keep the notations $n, a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_{n-1}, c_1, c_2, \ldots, c_{n-1}$ and $A$ fixed for the rest of Section 6.11.
Playing around with small examples, one soon notices that the determinants of tridiagonal matrices are too complicated to have neat explicit formulas in full generality. For \( n \in \{0,1,2,3\} \), the determinants look as follows:

\[
\begin{align*}
\det A &= \det (\text{the } 0 \times 0\text{-matrix}) = 1 \quad \text{if } n = 0; \\
\det A &= \det (a_1) = a_1 \quad \text{if } n = 1; \\
\det A &= \det \begin{pmatrix} a_1 & b_1 \\ c_1 & a_2 \end{pmatrix} = a_1a_2 - b_1c_1 \quad \text{if } n = 2; \\
\det A &= \det \begin{pmatrix} a_1 & b_1 & 0 \\ c_1 & a_2 & b_2 \\ 0 & c_2 & a_3 \end{pmatrix} = a_1a_2a_3 - a_1b_2c_2 - a_3b_1c_1 \quad \text{if } n = 3.
\end{align*}
\]

(And these formulas get more complicated the larger \( n \) becomes.) However, the many zeroes present in a tridiagonal matrix make it easy to find a recursive formula for its determinant using Laplace expansion:

**Proposition 6.69.** For every two elements \( x \) and \( y \) of \( \{0,1,\ldots,n\} \) satisfying \( x \leq y \), we let \( A_{x,y} \) be the \((y - x) \times (y - x)\)-matrix

\[
\begin{pmatrix}
  a_{x+1} & b_{x+1} & 0 & \cdots & 0 & 0 & 0 \\
  c_{x+1} & a_{x+2} & b_{x+2} & \cdots & 0 & 0 & 0 \\
  0 & c_{x+2} & a_{x+3} & \cdots & 0 & 0 & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
  0 & 0 & 0 & \cdots & a_{y-2} & b_{y-2} & 0 \\
  0 & 0 & 0 & \cdots & c_{y-2} & a_{y-1} & b_{y-1} \\
  0 & 0 & 0 & \cdots & 0 & c_{y-1} & a_y
\end{pmatrix} = \text{sub}^{x+1,x+2,\ldots,y}_{x+1,x+2,\ldots,y} A.
\]

(a) We have \( \det (A_{x,x}) = 1 \) for every \( x \in \{0,1,\ldots,n\} \).

(b) We have \( \det (A_{x,x+1}) = a_{x+1} \) for every \( x \in \{0,1,\ldots,n-1\} \).

(c) For every \( x \in \{0,1,\ldots,n\} \) and \( y \in \{0,1,\ldots,n\} \) satisfying \( x \leq y - 2 \), we have

\[
\det (A_{x,y}) = a_y \det (A_{x,y-1}) - b_{y-1}c_{y-1} \det (A_{x,y-2}).
\]

(d) For every \( x \in \{0,1,\ldots,n\} \) and \( y \in \{0,1,\ldots,n\} \) satisfying \( x \leq y - 2 \), we have

\[
\det (A_{x,y}) = a_{x+1} \det (A_{x+1,y}) - b_{x+1}c_{x+1} \det (A_{x+2,y}).
\]

(e) We have \( A = A_{0,n} \).
Proof of Proposition 6.69 (e) The definition of $A_{0,n}$ yields 

$$A_{0,n} = \begin{pmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 & 0 \\ c_1 & a_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_2 & a_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & \cdots & c_{n-2} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & c_{n-1} & a_n \end{pmatrix} = A.$$ 

This proves Proposition 6.69 (e).

(a) Let $x \in \{0,1,\ldots,n\}$. Then, $A_{x,x}$ is an $(x-x) \times (x-x)$-matrix, thus a $0 \times 0$-matrix. Hence, its determinant is $\det(A_{x,x}) = 1$. This proves Proposition 6.69 (a).

(b) Let $x \in \{0,1,\ldots,n-1\}$. The definition of $A_{x,x+1}$ shows that $A_{x,x+1}$ is the $1 \times 1$-matrix $\begin{pmatrix} a_{x+1} \end{pmatrix}$. Hence, $\det(A_{x,x+1}) = \det( a_{x+1} ) = a_{x+1}$. This proves Proposition 6.69 (b).

(c) Let $x \in \{0,1,\ldots,n\}$ and $y \in \{0,1,\ldots,n\}$ be such that $x \leq y - 2$. We have 

$$A_{x,y} = \begin{pmatrix} a_{x+1} & b_{x+1} & 0 & \cdots & 0 & 0 & 0 \\ c_{x+1} & a_{x+2} & b_{x+2} & \cdots & 0 & 0 & 0 \\ 0 & c_{x+2} & a_{x+3} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{y-2} & b_{y-2} & 0 \\ 0 & 0 & 0 & \cdots & c_{y-2} & a_{y-1} & b_{y-1} \\ 0 & 0 & 0 & \cdots & 0 & c_{y-1} & a_y \end{pmatrix}. \quad (214)$$ 

This is a $(y-x) \times (y-x)$-matrix. If we cross out its $(y-x)$-th row (i.e., its last row) and its $(y-x)$-th column (i.e., its last column), then we obtain $A_{x,y-1}$. In other words, $(A_{x,y})_{(y-x),(y-x)} = A_{x,y-1}$. 

Let us write the matrix $A_{x,y}$ in the form $A_{x,y} = (u_{i,j})_{1 \leq i \leq y-x, 1 \leq j \leq y-x}$. Thus, 

$$(u_{y-x,1}, u_{y-x,2}, \ldots, u_{y-x,y-x}) = (\text{the last row of the matrix } A_{x,y}) = (0, 0, \ldots, 0, c_{y-1}, a_y).$$ 

In other words, we have 

$$u_{y-x,q} = 0 \quad \text{for every } q \in \{1,2,\ldots,y-x-2\}, \quad (215)$$

and 

$$u_{y-x,y-x-1} = c_{y-1}, \quad u_{y-x,y-x} = a_y.$$ 

Now, Laplace expansion along the $(y-x)$-th row (or, more precisely, Theorem
6.64 (a), applied to \( y - x, A_{x,y}, u_{i,j} \) and \( y - x \) instead of \( n, A, a_{i,j} \) and \( p \) yields

\[
\det(A_{x,y}) = \sum_{q=1}^{y-x} (-1)^{(y-x)+q} u_{y-x,q} \det \left( (A_{x,y})_{(y-x), q} \right)
\]

\[
= \sum_{q=1}^{y-x-2} (-1)^{(y-x)+q} u_{y-x,q} \det \left( (A_{x,y})_{(y-x), q} \right)
\]

(by [215])

\[
+ (-1)^{(y-x)+(y-x-1)} u_{y-x,y-x-1} \det \left( (A_{x,y})_{(y-x), (y-x-1)} \right)
\]

\[
+ (-1)^{(y-x)+(y-x)} u_{y-x,y-x} \det \left( (A_{x,y})_{(y-x), (y-x)} \right)
\]

(since \( y - x \geq 2 \) (since \( x \leq y - 2 \))

\[
= \sum_{q=1}^{y-x-2} (-1)^{(y-x)+q} 0 \det \left( (A_{x,y})_{(y-x), q} \right)
\]

\[
- c_{y-1} \det \left( (A_{x,y})_{(y-x), (y-x-1)} \right) + a_y \det \left( A_{x,y-1} \right)
\]

\[
= -c_{y-1} \det \left( (A_{x,y})_{(y-x), (y-x-1)} \right) + a_y \det \left( A_{x,y-1} \right).
\]  \hspace{1cm} (216)

Now, let \( B = \left( A_{x,y} \right)_{(y-x), (y-x-1)} \). Thus, (216) becomes

\[
\det(A_{x,y}) = -c_{y-1} \det \left( (A_{x,y})_{(y-x), (y-x-1)} \right) + a_y \det \left( A_{x,y-1} \right)
\]

\[
= -c_{y-1} \det B + a_y \det \left( A_{x,y-1} \right).
\]  \hspace{1cm} (217)

Now,

\[
B = \left( A_{x,y} \right)_{(y-x), (y-x-1)}
\]

\[
= \begin{pmatrix}
    a_{x+1} & b_{x+1} & 0 & \cdots & 0 & 0 & 0 \\
    c_{x+1} & a_{x+2} & b_{x+2} & \cdots & 0 & 0 & 0 \\
    0 & c_{x+2} & a_{x+3} & \cdots & 0 & 0 & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
    0 & 0 & 0 & \cdots & a_{y-3} & b_{y-3} & 0 \\
    0 & 0 & 0 & \cdots & c_{y-3} & a_{y-2} & 0 \\
    0 & 0 & 0 & \cdots & 0 & c_{y-2} & b_{y-1}
\end{pmatrix}
\]

(because of (214)).

\hspace{1cm} (218)
Now, let us write the matrix $B$ in the form $B = (v_{i,j})_{1 \leq i \leq y-x-1, 1 \leq j \leq y-x-1}$. Thus,

$$(v_{1,y-x-1}, v_{2,y-x-1}, \ldots, v_{y-x-1,y-x-1})^T$$

= (the last column of the matrix $B$) = $(0, 0, \ldots, b_{y-1})^T$

(because of (218)). In other words, we have

$$v_{y-x-1,y-x-1} = b_{y-1}.$$

Now, Laplace expansion along the $(y-x-1)$-th column (or, more precisely, Theorem 6.64 (b), applied to $y-x-1$, $B$, $v_{i,j}$ and $y-x-1$ instead of $n$, $A$, $a_{i,j}$ and $q$) yields

$$\det B = \sum_{p=1}^{y-x-1} (-1)^{p+(y-x-1)} v_{p,y-x-1} \det \left( B_{\sim p,\sim (y-x-1)} \right)$$

$$= \sum_{p=1}^{y-x-2} (-1)^{p+(y-x-1)} v_{p,y-x-1} \det \left( B_{\sim p,\sim (y-x-1)} \right)$$

(by (219))

$$\begin{aligned}
+ (\underbrace{-1}_{=1} (y-x-1) + (y-x-1) \underbrace{v_{y-x-1,y-x-1}}_{=b_{y-1}}) \det \left( B_{\sim (y-x-1),\sim (y-x-1)} \right)
\end{aligned}$$

(since $y-x-1 \geq 1$ (since $x \leq y-2$))

$$= \sum_{p=1}^{y-x-2} (-1)^{p+(y-x-1)} 0 \det \left( B_{\sim p,\sim (y-x-1)} \right) + b_{y-1} \det \left( B_{\sim (y-x-1),\sim (y-x-1)} \right)$$

$$= b_{y-1} \det \left( B_{\sim (y-x-1),\sim (y-x-1)} \right).$$

Finally, a look at (218) reveals that

$$B_{\sim (y-x-1),\sim (y-x-1)} = \begin{pmatrix}
 a_{x+1} & b_{x+1} & 0 & \cdots & 0 & 0 & 0 \\
 c_{x+1} & a_{x+2} & b_{x+2} & \cdots & 0 & 0 & 0 \\
 0 & c_{x+2} & a_{x+3} & \cdots & 0 & 0 & 0 \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
 0 & 0 & 0 & \cdots & a_{y-4} & b_{y-4} & 0 \\
 0 & 0 & 0 & \cdots & c_{y-4} & a_{y-3} & b_{y-3} \\
 0 & 0 & 0 & \cdots & 0 & c_{y-3} & a_{y-2}
\end{pmatrix} = A_{x,y-2}.$$

Hence, (220) becomes

$$\det B = b_{y-1} \det \left( B_{\sim (y-x-1),\sim (y-x-1)} \right) = b_{y-1} \det (A_{x,y-2}).$$
Therefore, (217) becomes

\[
\det(A_{x,y}) = -c_{y-1} \det \begin{bmatrix} B \end{bmatrix} + a_y \det(A_{x,y-1}) = b_{y-1} \det(A_{x,y-2}) = a_y \det(A_{x,y-1}) - b_{y-1}c_{y-1} \det(A_{x,y-2}).
\]

This proves Proposition 6.69 (c).

(d) The proof of Proposition 6.69 (d) is similar to the proof of Proposition 6.69 (c). The main difference is that we now have to perform Laplace expansion along the 1-st row (instead of the \((y - x)\)-th row) and then Laplace expansion along the 1-st column (instead of the \((y - x - 1)\)-th column).

Proposition 6.69 gives us two fast recursive algorithms to compute \(\det A\):

The first algorithm proceeds by recursively computing \(\det(A_{0,m})\) for every \(m \in \{0, 1, \ldots, n\}\). This is done using Proposition 6.69 (a) (for \(m = 0\)), Proposition 6.69 (b) (for \(m = 1\)) and Proposition 6.69 (c) (to find \(\det(A_{0,m})\) for \(m \geq 2\) in terms of \(\det(A_{0,m-1})\) and \(\det(A_{0,m-2})\)). The final value \(\det(A_{0,n})\) is \(\det A\) (by Proposition 6.69 (e)).

The second algorithm proceeds by recursively computing \(\det(A_{m,n})\) for every \(m \in \{0, 1, \ldots, n\}\). This recursion goes backwards: We start with \(m = n\) (where we use Proposition 6.69 (a)), then turn to \(m = n - 1\) (using Proposition 6.69 (b)), and then go further and further down (using Proposition 6.69 (d) to compute \(\det(A_{m,n})\) in terms of \(\det(A_{m+1,n})\) and \(\det(A_{m+2,n})\)).

So we have two different recursive algorithms leading to one and the same result. Whenever you have such a thing, you can package up the equivalence of the two algorithms as an exercise, and try to make it less easy by covering up the actual goal of the algorithms (in our case, computing \(\det A\)). In our case, this leads to the following exercise:

**Exercise 39.** Let \(n \in \mathbb{N}\). Let \(a_1, a_2, \ldots, a_n\) be \(n\) elements of \(K\). Let \(b_1, b_2, \ldots, b_{n-1}\) be \(n - 1\) elements of \(K\).

Define a sequence \((u_0, u_1, \ldots, u_n)\) of elements of \(K\) recursively by setting \(u_0 = 1\), \(u_1 = a_1\) and

\[ u_i = a_i u_{i-1} - b_{i-1} u_{i-2} \quad \text{for every } i \in \{2, 3, \ldots, n\}. \]

Define a sequence \((v_0, v_1, \ldots, v_n)\) of elements of \(K\) recursively by setting \(v_0 = 1\), \(v_1 = a_n\) and

\[ v_i = a_{n-i+1} v_{i-1} - b_{n-i+1} v_{i-2} \quad \text{for every } i \in \{2, 3, \ldots, n\}. \]

Prove that \(u_n = v_n\).
This exercise generalizes [IMO Shortlist 2013 problem A1].

Our recursive algorithms for computing \( \det A \) also yield another observation:
The determinant \( \det A \) depends not on the \(( n - 1 )\) elements
\( b_1, b_2, \ldots, b_{n-1}, c_1, c_2, \ldots, c_{n-1} \) but only on the products
\( b_1 c_1, b_2 c_2, \ldots, b_{n-1} c_{n-1} \).

**Exercise 40.** Define \( A_{x,y} \) as in Proposition [6.69]. Prove that
\[
\frac{\det A}{\det (A_{1,n})} = a_1 - \frac{b_1 c_1}{a_2 - \frac{b_2 c_2}{a_3 - \frac{b_3 c_3}{\ldots - \frac{b_{n-2} c_{n-2}}{a_{n-1} - \frac{b_{n-1} c_{n-1}}{a_n}}}}}
\]
provided that all denominators in this equality are invertible.

**Exercise 41.** Assume that \( a_i = 1 \) for all \( i \in \{1, 2, \ldots, n\} \). Also, assume that
\( b_i = 1 \) and \( c_i = -1 \) for all \( i \in \{1, 2, \ldots, n - 1\} \). Let \((f_0, f_1, f_2, \ldots)\) be the Fibonacci sequence (defined as in Chapter [4]). Show that \( \det A = f_{n+1} \).

**Remark 6.70.** Consider once again the Fibonacci sequence \((f_0, f_1, f_2, \ldots)\) (defined as in Chapter [4]). Let \( n \) be a positive integer. Combining the results of Exercise

\[\text{[163] I have a suspicion that [IMO Shortlist 2009 problem C3] also can be viewed as an equality between two recursive ways to compute a determinant, but this determinant seems to be harder to find (I don’t think it can be obtained from Proposition [6.69]}.\]
and Exercise 41 (the details are left to the reader), we obtain the equality

\[
\frac{f_{n+1}}{f_n} = 1 - \frac{1}{1 - \frac{1}{1 - \frac{1}{\ddots}}}
\]

(with \(n - 1\) fractions in total)

\[
= 1 + \frac{1}{1 + \frac{1}{\ddots}}
\]

(with \(n - 1\) fractions in total).

If you know some trivia about the golden ratio, you might recognize this as a part of the continued fraction for the golden ratio \(\phi\). The whole continued fraction for \(\phi\) is

\[
\phi = 1 + \frac{1}{1 + \frac{1}{\ddots}}
\]

(with infinitely many fractions).

This hints at the fact that \(\lim_{n \to \infty} \frac{f_{n+1}}{f_n} = \phi\). (This is easy to prove without continued fractions, of course.)

6.12. On block-triangular matrices

**Definition 6.71.** Let \(n, n', m\) and \(m'\) be four nonnegative integers.

Let \(A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}\) be an \(n \times m\)-matrix.

Let \(B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m'}\) be an \(n \times m'\)-matrix.

Let \(C = (c_{ij})_{1 \leq i \leq n', 1 \leq j \leq m}\) be an \(n' \times m\)-matrix.

Let \(D = (d_{ij})_{1 \leq i \leq n', 1 \leq j \leq m'}\) be an \(n' \times m'\)-matrix.
Then, \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) will mean the \((n + n') \times (m + m')\)-matrix

\[
\begin{pmatrix}
a_{1,1} & a_{1,2} & \cdots & a_{1,m} & b_{1,1} & b_{1,2} & \cdots & b_{1,m'} \\
a_{2,1} & a_{2,2} & \cdots & a_{2,m} & b_{2,1} & b_{2,2} & \cdots & b_{2,m'} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
a_{n,1} & a_{n,2} & \cdots & a_{n,m} & b_{n,1} & b_{n,2} & \cdots & b_{n,m'} \\
c_{1,1} & c_{1,2} & \cdots & c_{1,m} & d_{1,1} & d_{1,2} & \cdots & d_{1,m'} \\
c_{2,1} & c_{2,2} & \cdots & c_{2,m} & d_{2,1} & d_{2,2} & \cdots & d_{2,m'} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
c_{n',1} & c_{n',2} & \cdots & c_{n',m} & d_{n',1} & d_{n',2} & \cdots & d_{n',m'}
\end{pmatrix}
\]

(Formally speaking, this means that

\[
\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a_{i,j} & \text{if } i \leq n \text{ and } j \leq m; \\
b_{i,j-m} & \text{if } i \leq n \text{ and } j > m; \\
c_{i-n,j} & \text{if } i > n \text{ and } j \leq m; \\
d_{i-n,j-m} & \text{if } i > n \text{ and } j > m \end{pmatrix}_{1 \leq i \leq n+n', 1 \leq j \leq m+m'}
\]

Less formally, we can say that \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) is the matrix obtained by gluing the matrices \( A, B, C \) and \( D \) to form one big \((n + n') \times (m + m')\)-matrix, where the right border of \( A \) is glued together with the left border of \( B \), the bottom border of \( A \) is glued together with the top border of \( C \), etc.)

Do not get fooled by the notation \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \): It is (in general) not a 2 \times 2-matrix, but an \((n + n') \times (m + m')\)-matrix, and its entries are not \( A, B, C \) and \( D \) but the entries of \( A, B, C \) and \( D \).

\[\textbf{Example 6.72.}\] If \( A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, C = \begin{pmatrix} c_1 & c_2 \end{pmatrix} \) and \( D = \begin{pmatrix} d \end{pmatrix} \),

then \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & b_1 \\ a_{2,1} & a_{2,2} & b_2 \\ c_1 & c_2 & d \end{pmatrix} \).

The notation \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) introduced in Definition 6.71 is a particular case of a more general notation – the block-matrix construction – for gluing together multiple ma-
trices with matching dimensions. We shall only need the particular case that is Definition 6.71 however.

**Definition 6.73.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Recall that \( \mathbb{K}^{n \times m} \) is the set of all \( n \times m \)-matrices.

We use \( 0_{n \times m} \) (or sometimes just \( 0 \)) to denote the \( n \times m \) zero matrix. (As we recall, this is the \( n \times m \)-matrix whose all entries are \( 0 \); in other words, this is the \( n \times m \)-matrix \((0)_{1 \leq i \leq n, 1 \leq j \leq m}\).

**Exercise 42.** Let \( n, n', m, m', \ell \) and \( \ell' \) be six nonnegative integers. Let \( A \in \mathbb{K}^{n \times m} \), \( B \in \mathbb{K}^{n' \times m'} \), \( C \in \mathbb{K}^{n' \times m'} \), \( D \in \mathbb{K}^{n' \times \ell'} \), \( A' \in \mathbb{K}^{m \times \ell} \), \( B' \in \mathbb{K}^{m \times \ell} \), \( C' \in \mathbb{K}^{m' \times \ell} \) and \( D' \in \mathbb{K}^{m' \times \ell'} \). Then, prove that

\[
\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} = \begin{pmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{pmatrix}.
\]

**Remark 6.74.** The intuitive meaning of Exercise 42 is that the product of two matrices in “block-matrix notation” can be computed by applying the usual multiplication rule “on the level of blocks”, without having to fall back to multiplying single entries. However, when applying Exercise 42 do not forget to check that its conditions are satisfied. Let me give an example and a non-example:

**Example:** If \( A = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \\ b_{3,1} & b_{3,2} \end{pmatrix}, C = \begin{pmatrix} c \end{pmatrix}, D = \begin{pmatrix} d_1 & d_2 \end{pmatrix}, A' = \begin{pmatrix} a'_1 & a'_2 \end{pmatrix}, B' = \begin{pmatrix} b'_1 & b'_2 \end{pmatrix}, C' = \begin{pmatrix} c'_{1,1} & c'_{1,2} \\ c'_{2,1} & c'_{2,2} \end{pmatrix} \) and \( D' = \begin{pmatrix} d'_{1,1} & d'_{1,2} \\ d'_{2,1} & d'_{2,2} \end{pmatrix} \),

\[
\begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,y} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,y} \\ \vdots & \vdots & \ddots & \vdots \\ A_{x,1} & A_{x,2} & \cdots & A_{x,y} \end{pmatrix}
\]

whenever you have given two nonnegative integers \( x \) and \( y \), an \( x \)-tuple \((n_1, n_2, \ldots, n_x) \in \mathbb{N}^x \), a \( y \)-tuple \((m_1, m_2, \ldots, m_y) \in \mathbb{N}^y \), and an \( n_i \times m_j \)-matrix \( A_{i,j} \) for every \( i \in \{1, 2, \ldots, x\} \) and every \( j \in \{1, 2, \ldots, y\} \). I guess you can guess the definition of this matrix. So you start with an \( x \times y \)-matrix of matrices and glue them together to an \((n_1 + n_2 + \cdots + n_x) \times (m_1 + m_2 + \cdots + m_y)\)-matrix (provided that the dimensions of these matrices allow them to be glued – e.g., you cannot glue a \( 2 \times 3 \)-matrix to a \( 4 \times 6 \)-matrix along its right border, nor on any other border).

It is called “block-matrix construction” because the original matrices \( A_{i,j} \) appear as “blocks” in the big matrix (222). Most authors define block matrices to be matrices which are “partitioned” into blocks as in (222); this is essentially our construction in reverse: Instead of gluing several “small” matrices into a big one, they study big matrices partitioned into many small matrices. Of course, the properties of their “block matrices” are equivalent to those of our “block-matrix construction”.

---

164This construction defines an \((n_1 + n_2 + \cdots + n_x) \times (m_1 + m_2 + \cdots + m_y)\)-matrix.
then Exercise 42 can be applied (with \( n = 3, n' = 1, m = 1, m' = 2, \ell = 2 \) and \( \ell' = 2 \)), and thus we obtain
\[
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix}
\begin{pmatrix}
A' & B' \\
C' & D'
\end{pmatrix}
= 
\begin{pmatrix}
AA' + BC' & AB' + BD' \\
CA' + DC' & CB' + DD'
\end{pmatrix}.
\]

**Non-example:** If
\[
A = \begin{pmatrix}
a_1 \\
a_2
\end{pmatrix},
B = \begin{pmatrix}
b_{1,1} & b_{1,2} \\
b_{2,1} & b_{2,2}
\end{pmatrix},
C = \begin{pmatrix}
c_1 \\
c_2
\end{pmatrix},
D = \begin{pmatrix}
d_{1,1} & d_{1,2} \\
d_{2,1} & d_{2,2}
\end{pmatrix},
A' = \begin{pmatrix}
a'_{1,1} & a'_{1,2} \\
a'_{2,1} & a'_{2,2}
\end{pmatrix},
B' = \begin{pmatrix}
b'_{1,1} & b'_{1,2} \\
b'_{2,1} & b'_{2,2}
\end{pmatrix},
C' = \begin{pmatrix}
c'_{1} \\
c'_{2}
\end{pmatrix}
\]
and
\[
D' = \begin{pmatrix}
d'_{1} & d'_{2}
\end{pmatrix},
\]
then Exercise 42 cannot be applied, because there exist no \( n, m, \ell \in \mathbb{N} \) such that \( A \in \mathbb{K}^{n \times m} \) and \( A' \in \mathbb{K}^{m \times \ell} \). (Indeed, the number of columns of \( A \) does not equal the number of rows of \( A' \), but these numbers would both have to be \( m \).) The matrices \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) and \( \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \) still exist in this case, and can even be multiplied, but their product is not given by a simple formula such as the one in Exercise 42. Thus, beware of seeing Exercise 42 as a panacea for multiplying matrices blockwise.

**Exercise 43.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Let \( B \) be an \( n \times m \)-matrix. Let \( D \) be an \( m \times m \)-matrix. Prove that
\[
\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det A \cdot \det D.
\]

**Example 6.75.** Exercise 43 (applied to \( n = 2 \) and \( m = 3 \)) yields
\[
\det \begin{pmatrix}
a_{1,1} & a_{1,2} & b_{1,1} & b_{1,2} & b_{1,3} \\
a_{2,1} & a_{2,2} & b_{2,1} & b_{2,2} & b_{2,3} \\
0 & 0 & c_{1,1} & c_{1,2} & c_{1,3} \\
0 & 0 & c_{2,1} & c_{2,2} & c_{2,3} \\
0 & 0 & c_{3,1} & c_{3,2} & c_{3,3}
\end{pmatrix}
= \det \begin{pmatrix}
a_{1,1} & a_{1,2} \\
a_{2,1} & a_{2,2}
\end{pmatrix} \cdot \det \begin{pmatrix}
c_{1,1} & c_{1,2} & c_{1,3} \\
c_{2,1} & c_{2,2} & c_{2,3} \\
c_{3,1} & c_{3,2} & c_{3,3}
\end{pmatrix}.
\]

**Remark 6.76.** Not every determinant of the form \( \det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \) can be computed using Exercise 43. In fact, Exercise 43 requires \( A \) to be an \( n \times n \)-matrix and \( D \) to be an \( m \times m \)-matrix; thus, both \( A \) and \( D \) have to be square matrices in order for Exercise 43 to be applicable. For instance, Exercise 43 cannot be applied to compute
\[
\det \begin{pmatrix}
a_1 & b_{1,1} & b_{1,2} \\
a_2 & b_{2,1} & b_{2,2} \\
0 & c_1 & c_2
\end{pmatrix}.
\]
Remark 6.77. You might wonder whether Exercise 43 generalizes to a formula for \( \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) when \( A \in K^{n \times n}, B \in K^{n \times m}, C \in K^{m \times n} \) and \( D \in K^{m \times m} \).

The general answer is “No”. However, when \( D \) is invertible, there exists such a formula (involving the Schur complement). Curiously, there is also a formula for the case when \( n = m \) and \( CD = DC \) (see [Silvest, Theorem 3]).

We notice that Exercise 43 allows us to solve Exercise 23 in a new way.

Exercise 44. Invent and solve an exercise on computing determinants.

6.13. The adjugate matrix

We start this section with a variation on Theorem 6.64:

Proposition 6.78. Let \( n \in \mathbb{N} \). Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) be an \( n \times n \)-matrix. Let \( r \in \{1,2,\ldots,n\} \).

(a) For every \( p \in \{1,2,\ldots,n\} \) satisfying \( p \neq r \), we have

\[
0 = \sum_{q=1}^{n} (-1)^{p+q} a_{r,q} \det(A_{\sim p,\sim q}).
\]

(b) For every \( q \in \{1,2,\ldots,n\} \) satisfying \( q \neq r \), we have

\[
0 = \sum_{p=1}^{n} (-1)^{p+q} a_{r,q} \det(A_{\sim p,\sim q}).
\]

Proof of Proposition 6.78. (a) Let \( p \in \{1,2,\ldots,n\} \) be such that \( p \neq r \).

Let \( C \) be the \( n \times n \)-matrix obtained from \( A \) by replacing the \( p \)-th row of \( A \) by the \( r \)-th row of \( A \). Thus, the \( p \)-th and the \( r \)-th rows of \( C \) are equal. Therefore, the matrix \( C \) has two equal rows (since \( p \neq r \)). Hence, \( \det C = 0 \) (by Exercise 24(e), applied to \( C \) instead of \( A \)).

Let us write the \( n \times n \)-matrix \( C \) in the form \( C = (c_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \).

The \( p \)-th row of \( C \) equals the \( r \)-th row of \( A \) (by the construction of \( C \)). In other words,

\[
c_{p,q} = a_{r,q} \quad \text{for every } q \in \{1,2,\ldots,n\}.
\]

(223)

On the other hand, the matrix \( C \) equals the matrix \( A \) in all rows but the \( p \)-th one (again, by the construction of \( C \)). Hence, if we cross out the \( p \)-th rows in both \( C \) and \( A \), then the matrices \( C \) and \( A \) become equal. Therefore,

\[
C_{\sim p,\sim q} = A_{\sim p,\sim q} \quad \text{for every } q \in \{1,2,\ldots,n\}
\]

(224)
(because the construction of $C_{\sim p, \sim q}$ from $C$ involves crossing out the $p$-th row, and so does the construction of $A_{\sim p, \sim q}$ from $A$).

Now, $\det C = 0$, so that

$$0 = \det C = \sum_{q=1}^{n} (-1)^{p+q} c_{p,q} \det \begin{pmatrix} C_{\sim p, \sim q} \end{pmatrix}$$

(by Theorem 6.64 (a), applied to $C$ and $c_{ij}$ instead of $A$ and $a_{ij}$)

$$= \sum_{q=1}^{n} (-1)^{p+q} a_{r,q} \det \begin{pmatrix} A_{\sim p, \sim q} \end{pmatrix}.$$

This proves Proposition 6.78 (a).

(b) This proof is rather similar to the proof of Proposition 6.78 (a), except that rows are now replaced by columns. We leave the details to the reader.  

We now can define the “adjugate” of a matrix:

**Definition 6.79.** Let $n \in \mathbb{N}$. Let $A$ be an $n \times n$-matrix. We define a new $n \times n$-matrix $\text{adj} \ A$ by

$$\text{adj} \ A = \left( (-1)^{i+j} \det \begin{pmatrix} A_{\sim j, \sim i} \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.$$

This matrix $\text{adj} \ A$ is called the **adjugate** of the matrix $A$. (Some authors call it the “adjunct” or “adjoint” or “classical adjoint” of $A$ instead. However, beware of the word “adjoint”: It means too many different things; in particular it has a second meaning for a matrix.)

The appearance of $A_{\sim j, \sim i}$ (not $A_{\sim i, \sim j}$) in Definition 6.79 might be surprising, but it is not a mistake. We will soon see what it is good for.

There is also a related notion, namely that of a “cofactor matrix”. The **cofactor matrix** of an $n \times n$-matrix $A$ is defined to be $\left( (-1)^{i+j} \det \begin{pmatrix} A_{\sim i, \sim j} \end{pmatrix} \right)_{1 \leq i \leq n, 1 \leq j \leq n}$. This is, of course, the transpose $(\text{adj} \ A)^T$ of $\text{adj} \ A$. The entries of this matrix are called the cofactors of $A$.

**Example 6.80.** The adjugate of the $0 \times 0$-matrix is the $0 \times 0$-matrix.

The adjugate of a $1 \times 1$-matrix $\left( \begin{array}{c} a \end{array} \right)$ is $\text{adj} \left( \begin{array}{c} a \end{array} \right) = \left( \begin{array}{c} 1 \end{array} \right)$. (Yes, this shows that all $1 \times 1$-matrices have the same adjugate.)

The adjugate of a $2 \times 2$-matrix $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right)$ is $\text{adj} \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \left( \begin{array}{cc} d & -b \\ -c & a \end{array} \right)$.  

The adjugate of a $3 \times 3$-matrix \( \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \) is \( \begin{pmatrix} d & f & -e \\ -d & a & -c \\ b & -g & f \end{pmatrix} \).

**Proposition 6.81.** Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Then, \( \text{adj} (A^T) = (\text{adj} A)^T \).

**Proof of Proposition 6.81.** Let \( i \in \{1, 2, \ldots, n\} \) and \( j \in \{1, 2, \ldots, n\} \).

From \( i \in \{1, 2, \ldots, n\} \), we obtain \( 1 \leq i \leq n \), so that \( n \geq 1 \) and thus \( n - 1 \in \mathbb{N} \).

The definition of \( A_{i,j} \) yields \( A_{i,j} = \text{sub}_{1,2,\ldots,i,j}^n A \). But the definition of \( (A^T)_{i,j} \) yields

\[
(A^T)_{i,j} = \text{sub}_{1,2,\ldots,i,j}^n (A^T).
\]

On the other hand, Proposition 6.61(e) (applied to \( m = n, u = n - 1, v = n - 1, (i_1, i_2, \ldots, i_u) = (1, 2, \ldots, i, \ldots, n) \) and \( (j_1, j_2, \ldots, j_v) = (1, 2, \ldots, j, \ldots, n) \)) yields

\[
\left(\text{sub}_{1,2,\ldots,i,j}^n A\right)^T = \text{sub}_{1,2,\ldots,i,j}^n (A^T). \]

Compared with (225), this yields

\[
\left(\text{sub}_{1,2,\ldots,i,j}^n A\right)^T = \left(\text{sub}_{1,2,\ldots,i,j}^n A_{i,j}\right)^T.
\]

Hence,

\[
\det \left(\text{sub}_{1,2,\ldots,i,j}^n A \right) = \det \left(\text{sub}_{1,2,\ldots,i,j}^n A_{i,j}\right) = \det \left(A_{i,j}\right) \quad \text{(226)}
\]

(by Exercise 22, applied to \( n - 1 \) and \( A_{i,j} \) instead of \( n \) and \( A \)).

Let us now forget that we fixed \( i \) and \( j \). We thus have shown that (226) holds for every \( i \in \{1, 2, \ldots, n\} \) and \( j \in \{1, 2, \ldots, n\} \).

Now, \( \text{adj} A = \left( (-1)^{i+j} \det (A_{j,i}) \right)_{1 \leq i \leq n, 1 \leq j \leq n} \), and thus the definition of the transpose of a matrix shows that

\[
(\text{adj} A)^T = \left( (-1)^{i+j} \det (A_{i,j}) \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \left( (-1)^{i+j} \det (A_{i,j}) \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]
Compared with

\[
\text{adj} (A^T) = \left( (-1)^{i+j} \det \left( (A^T)_{i\sim j, j\sim i} \right) \right)_{1 \leq i \leq n, 1 \leq j \leq n}^{(\text{by the definition of adj}(A^T))} \\
= \left( (-1)^{i+j} \det (A_{i\sim j, j\sim i}) \right)_{1 \leq i \leq n, 1 \leq j \leq n}^{(\text{by } (226))}
\]

this yields \( \text{adj} (A^T) = (\text{adj } A)^T \). This proves Proposition 6.81. □

The most important property of adjugates, however, is the following fact:

**Theorem 6.82.** Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Then,

\[ A \cdot \text{adj } A = \text{adj } A \cdot A = \det A \cdot I_n. \]

(Recall that \( I_n \) denotes the \( n \times n \) identity matrix. Expressions such as \( \text{adj } A \cdot A \) and \( \det A \cdot I_n \) have to be understood as \( \text{adj } A \cdot A \) and \( \det A \cdot I_n \), respectively.)

**Example 6.83.** Recall that the adjugate of a \( 2 \times 2 \)-matrix is given by the formula

\[ \text{adj} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \]

Thus, Theorem 6.82 (applied to \( n = 2 \)) yields

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left( \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \cdot I_2.
\]

(Of course, \( \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot I_2 = (ad - bc) \cdot I_2 = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \).)

**Proof of Theorem 6.82** For any two objects \( i \) and \( j \), we define \( \delta_{i,j} \) to be the element \( \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases} \) of \( \mathbb{K} \). Then, \( I_n = (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) (by the definition of \( I_n \)), and thus

\[
\det A \cdot \sum_{\mathclap{I_n}} = \det A \cdot (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} = \left( \det A \cdot \delta_{i,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} \cdot (227)
\]

On the other hand, let us write the matrix \( A \) in the form \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \).
Then, the definition of the product of two matrices shows that

\[
A \cdot \text{adj} A = \left( \sum_{k=1}^{n} a_{i,k} (-1)^{k+j} \det (A_{\sim j, \sim k}) \right) \prod_{1 \leq i \leq n, 1 \leq j \leq n}
\]

since \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) and \( \text{adj} A = \left( (-1)^{i+j} \det (A_{\sim j, \sim i}) \right)_{1 \leq i \leq n, 1 \leq j \leq n} \).

\[
= \left( \sum_{q=1}^{n} a_{i,q} (-1)^{q+j} \det (A_{\sim j, \sim q}) \right) \prod_{1 \leq i \leq n, 1 \leq j \leq n}
\]

(here, we renamed the summation index \( k \) as \( q \))

\[
= \left( \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}) \right) \prod_{1 \leq i \leq n, 1 \leq j \leq n}
\]

Now, we claim that

\[
\sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}) = \det A \cdot \delta_{i,j}
\]

for any \((i, j) \in \{1, 2, \ldots, n\}^2\).

**Proof of (229):** Fix \((i, j) \in \{1, 2, \ldots, n\}^2\). We are in one of the following two cases:

Case 1: We have \( i = j \).

Case 2: We have \( i \neq j \).

Let us consider Case 1 first. In this case, we have \( i = j \). Hence, \( \delta_{i,j} = 1 \). Now, Theorem 6.64 (a) (applied to \( p = i \)) yields

\[
\det A = \sum_{q=1}^{n} (-1)^{q+i} a_{i,q} \det (A_{\sim j, \sim q}) = \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}) \prod_{1 \leq i \leq n, 1 \leq j \leq n}
\]

In view of \( \det A \cdot \delta_{i,j} = \det A \), this rewrites as

\[
\det A = \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}) \prod_{1 \leq i \leq n, 1 \leq j \leq n}
\]

Thus, (229) is proven in Case 1.
Let us next consider Case 2. In this case, we have $i \neq j$. Hence, $\delta_{ij} = 0$ and $j \neq i$.

Now, Proposition 6.78(a) (applied to $p = j$ and $r = i$) yields

$$0 = \sum_{q=1}^{n} (-1)^{i+q} a_{i,q} \det (A_{\sim j, \sim q}) = \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}).$$

In view of $\det A \cdot \delta_{ij} = 0$, this rewrites as

$$\det A \cdot \delta_{ij} = \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}).$$

Thus, (229) is proven in Case 2.

We have now proven (229) in each of the two Cases 1 and 2. Thus, (229) is proven.

Now, (228) becomes

$$A \cdot \adj A = \begin{pmatrix} \sum_{q=1}^{n} (-1)^{q+j} a_{i,q} \det (A_{\sim j, \sim q}) \\ \vphantom{\hat{\delta}_{ij}} \hat{\delta}_{ij} \end{pmatrix}_{1\leq i\leq n, 1\leq j\leq n} = \det A \cdot I_{n}$$

(by (227)).

It now remains to prove that $\adj A \cdot A = \det A \cdot I_{n}$. One way to do this is by mimicking the above proof using Theorem 6.64(b) and Proposition 6.78(b) instead of Theorem 6.64(a) and Proposition 6.78(a). However, here is a slicker proof:

Let us forget that we fixed $A$. We thus have shown that (230) holds for every $n \times n$-matrix $A$.

Now, let $A$ be any $n \times n$-matrix. Then, we can apply (230) to $A^{T}$ instead of $A$. We thus obtain

$$A^{T} \cdot \adj (A^{T}) = \det (A^{T}) \cdot I_{n} = \det A \cdot I_{n}.$$ (231)

But here are four fundamental properties of transposes which are all easy to check:

- If $u$, $v$ and $w$ are three nonnegative integers, if $P$ is a $u \times v$-matrix, and if $Q$ is a $v \times w$-matrix, then

$$\text{(PQ)}^{T} = Q^{T}P^{T}.$$ (232)
Every \( u \in \mathbb{N} \) satisfies
\[
(I_u)^T = I_u. \tag{233}
\]

If \( u \) and \( v \) are two nonnegative integers, if \( P \) is a \( u \times v \)-matrix, and if \( \lambda \in \mathbb{K} \), then
\[
(\lambda P)^T = \lambda P^T. \tag{234}
\]

If \( u \) and \( v \) are two nonnegative integers, and if \( P \) is a \( u \times v \)-matrix, then
\[
(P^T)^T = P. \tag{235}
\]

Now, (232) (applied to \( u = v = w = n \), \( P = \text{adj} A \) and \( Q = A \)) shows that
\[
(\text{adj} A \cdot A)^T = A^T \cdot \text{adj}(A^T) = \det A \cdot I_n \quad \text{(by (231)).}
\]

Hence,
\[
(\text{adj} A \cdot A)^T \overset{\text{def}}{=} \det A \cdot I_n^T = \det A \cdot I_n \quad \text{(by (233), applied to } u = n) \]
\[
\overset{\text{by (234), applied to } u = v} = \det A \cdot I_n.
\]

Compared with
\[
(\text{adj} A \cdot A)^T = \text{adj} A \cdot A \quad \text{(by (235), applied to } u = v = n \text{ and } P = \text{adj} A \cdot A),
\]
this yields \( \text{adj} A \cdot A = \det A \cdot I_n \). Combined with (230), this yields
\[
A \cdot \text{adj} A = \text{adj} A \cdot A = \det A \cdot I_n.
\]

This proves Theorem 6.82. \( \Box \)

The following is a simple consequence of Theorem 6.82:

**Corollary 6.84.** Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Let \( v \) be a column vector of length \( n \). If \( Av = 0_{n \times 1} \), then \( \det A \cdot v = 0_{n \times 1} \).

(Recall that \( 0_{n \times 1} \) denotes the \( n \times 1 \) zero matrix, i.e., the column vector of length \( n \) whose all entries are 0.)
Proof of Corollary 6.84. Assume that $Av = 0_{n \times 1}$. It is easy to see that every $m \in \mathbb{N}$ and every $n \times m$-matrix $B$ satisfy $I_nB = B$. Applying this to $m = 1$ and $B = v$, we obtain $I_nv = v$.

It is also easy to see that every $m \in \mathbb{N}$ and every $m \times n$-matrix $B$ satisfy $B \cdot 0_{n \times 1} = 0_{n \times 1}$. Applying this to $m = n$ and $B = \text{adj} A$, we obtain $\text{adj} A \cdot 0_{n \times 1} = 0_{n \times 1}$.

Now, Theorem 6.82 yields $\text{adj} A \cdot A = \det A \cdot I_n$. Hence,

$$\text{adj} A \cdot A v = (\det A \cdot I_n) v = \det A \cdot (I_n v) = \det A \cdot v.$$ 

Compared to

$$\text{adj} A \cdot A v = \text{adj} A \cdot (Av) \quad \text{(since matrix multiplication is associative)}$$

we have

$$= \det A \cdot I_n$$

and

$$= 0_{n \times 1},$$

this yields $\det A \cdot v = 0_{n \times 1}$. This proves Corollary 6.84.

Exercise 45. Let $n \in \mathbb{N}$. Let $A$ and $B$ be two $n \times n$-matrices. Prove that

$$\text{adj} (AB) = \text{adj} B \cdot \text{adj} A.$$ 


We now will study inverses of matrices. We begin with a definition:

Definition 6.85. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $A$ be an $n \times m$-matrix.

(a) A left inverse of $A$ means an $m \times n$-matrix $L$ such that $LA = I_m$. We say that the matrix $A$ is left-invertible if and only if a left inverse of $A$ exists.

(b) A right inverse of $A$ means an $m \times n$-matrix $R$ such that $AR = I_n$. We say that the matrix $A$ is right-invertible if and only if a right inverse of $A$ exists.

(c) An inverse of $A$ (or two-sided inverse of $A$) means an $m \times n$-matrix $B$ such that $BA = I_m$ and $AB = I_n$. We say that the matrix $A$ is invertible if and only if an inverse of $A$ exists.

The notions “left-invertible”, “right-invertible” and “invertible” depend on the ring $\mathbb{K}$. We shall therefore speak of “left-invertible over $\mathbb{K}$”, “right-invertible over $\mathbb{K}$” and “invertible over $\mathbb{K}$” whenever the context does not unambiguously determine $\mathbb{K}$.

The notions of “left inverse”, “right inverse” and “inverse” are not interchangeable (unlike for elements in a commutative ring). We shall soon see in what cases they are identical; but first, let us give a few examples.
Example 6.86. For this example, set $\mathbb{K} = \mathbb{Z}$.

Let $P$ be the $1 \times 2$-matrix $\left( \begin{array}{cc} 1 & 2 \end{array} \right)$. The matrix $P$ is right-invertible. For instance, $\left( \begin{array}{cc} -1 \\ 1 \end{array} \right)$ and $\left( \begin{array}{cc} 3 \\ -1 \end{array} \right)$ are two right inverses of $P$ (because $P \left( \begin{array}{cc} -1 \\ 1 \end{array} \right) = (1) = I_1$ and $P \left( \begin{array}{cc} 3 \\ -1 \end{array} \right) = (1) = I_1$). This example shows that the right inverse of a matrix is not always unique.

The $2 \times 1$-matrix $P^T = \left( \begin{array}{cc} 1 \\ 2 \end{array} \right)$ is left-invertible. The left inverses of $P^T$ are the transposes of the right inverses of $P$.

Let $Q$ be the $2 \times 2$-matrix $\left( \begin{array}{cc} 1 & -1 \\ 3 & -2 \end{array} \right)$. The matrix $Q$ is invertible. Its inverse is $\left( \begin{array}{cc} -2 & 1 \\ -3 & 1 \end{array} \right)$ (since $\left( \begin{array}{cc} -2 & 1 \\ -3 & 1 \end{array} \right) Q = I_2$ and $Q \left( \begin{array}{cc} -2 & 1 \\ -3 & 1 \end{array} \right) = I_2$). It is not hard to see that this is its only inverse.

Let $R$ be the $2 \times 2$-matrix $\left( \begin{array}{cc} 1 & 2 \\ 2 & -1 \end{array} \right)$. It can be seen that this matrix is not invertible as a matrix over $\mathbb{Z}$. On the other hand, if we consider it as a matrix over $\mathbb{K} = Q$ instead, then it is invertible, with inverse $\left( \begin{array}{cc} 1/5 & 2/5 \\ 2/5 & -1/5 \end{array} \right)$.

Of course, any inverse of a matrix $A$ is automatically both a left inverse of $A$ and a right inverse of $A$. Thus, an invertible matrix $A$ is automatically both left-invertible and right-invertible.

The following simple fact is an analogue of Proposition 6.52:

Proposition 6.87. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $A$ be an $n \times m$-matrix. Let $L$ be a left inverse of $A$. Let $R$ be a right inverse of $A$.

(a) We have $L = R$.

(b) The matrix $A$ is invertible, and $L = R$ is an inverse of $A$.

Proof of Proposition 6.87. We know that $L$ is a left inverse of $A$. In other words, $L$ is an $m \times n$-matrix such that $LA = I_m$ (by the definition of a “left inverse”).

We know that $R$ is a right inverse of $A$. In other words, $R$ is an $m \times n$-matrix such that $AR = I_n$ (by the definition of a “right inverse”).

Now, recall that $I_m G = G$ for every $k \in \mathbb{N}$ and every $m \times k$-matrix $G$. Applying this to $k = n$ and $G = R$, we obtain $I_n R = R$.

Also, recall that $G I_n = G$ for every $k \in \mathbb{N}$ and every $k \times n$-matrix $G$. Applying this to $k = m$ and $G = L$, we obtain $L I_n = L$. Thus, $L = L I_n = I_n R = I_n R = R$.

This proves Proposition 6.87(a).

(b) We have $LA = I_m$ and $A R = I_n$. Thus, $L$ is an $m \times n$-matrix such that $LA = I_m$ and $AL = I_n$. In other words, $L$ is an inverse of $A$ (by the definition of
an “inverse”). Thus, \( L = R \) is an inverse of \( A \) (since \( L = R \)). This proves Proposition 6.87(b).

**Corollary 6.88.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an \( n \times m \)-matrix.

(a) If \( A \) is left-invertible and right-invertible, then \( A \) is invertible.

(b) If \( A \) is invertible, then there exists exactly one inverse of \( A \).

**Proof of Corollary 6.88.** (a) Assume that \( A \) is left-invertible and right-invertible. Thus, \( A \) has a left inverse \( L \) (since \( A \) is left-invertible). Consider this \( L \). Also, \( A \) has a right inverse \( R \) (since \( A \) is right-invertible). Consider this \( R \). Proposition 6.87(b) yields that the matrix \( A \) is invertible, and \( L = R \) is an inverse of \( A \). Corollary 6.88(a) is proven.

(b) Assume that \( A \) is invertible. Let \( B \) and \( B' \) be any two inverses of \( A \). Since \( B \) is an inverse of \( A \), we know that \( B \) is an \( m \times n \)-matrix such that \( BA = I_m \) and \( AB = I_n \) (by the definition of an “inverse”). Thus, in particular, \( B \) is an \( m \times n \)-matrix such that \( BA = I_m \). In other words, \( B \) is a left inverse of \( A \). Since \( B' \) is an inverse of \( A \), we know that \( B' \) is an \( m \times n \)-matrix such that \( B'A = I_m \) and \( AB' = I_n \) (by the definition of an “inverse”). Thus, in particular, \( B' \) is an \( m \times n \)-matrix such that \( AB' = I_n \). In other words, \( B' \) is a right inverse of \( A \). Now, Proposition 6.87(a) (applied to \( L = B \) and \( R = B' \)) shows that \( B = B' \).

Let us now forget that we fixed \( B \) and \( B' \). We thus have shown that if \( B \) and \( B' \) are two inverses of \( A \), then \( B = B' \). In other words, any two inverses of \( A \) are equal. In other words, there exists at most one inverse of \( A \). Since we also know that there exists at least one inverse of \( A \) (since \( A \) is invertible), we thus conclude that there exists exactly one inverse of \( A \). This proves Corollary 6.88(b).

**Definition 6.89.** Let \( n \in \mathbb{N} \) and \( m \in \mathbb{N} \). Let \( A \) be an invertible \( n \times m \)-matrix. Corollary 6.88(b) shows that there exists exactly one inverse of \( A \). Thus, we can speak of “the inverse of \( A \”. We denote this inverse by \( A^{-1} \).

In contrast to Definition 6.53, we do not define the notation \( B/A \) for two matrices \( B \) and \( A \) for which \( A \) is invertible. In fact, the trouble with such a notation would be its ambiguity: should it mean \( BA^{-1} \) or \( A^{-1}B \)? (In general, \( BA^{-1} \) and \( A^{-1}B \) are not the same.) Some authors do write \( B/A \) for the matrices \( BA^{-1} \) and \( A^{-1}B \) when these matrices are equal; but we shall not have a reason to do so.

Example 6.86 (and your experiences with a linear algebra class, if you have taken one) suggest the conjecture that only square matrices can be invertible. Indeed, this is almost true. There is a stupid counterexample: If \( K \) is a trivial ring, then every matrix over \( K \) is invertible\(^{165}\). It turns out that this is the only case where nonsquare matrices can be invertible. Indeed, we have the following:

\(^{165}\)For example, the \( 1 \times 2 \)-matrix \( \begin{bmatrix} 0_K & 0_K \end{bmatrix} \) over a trivial ring \( K \) is invertible, having inverse
Theorem 6.90. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $A$ be an $n \times m$-matrix.

(a) If $A$ is left-invertible and if $n < m$, then $K$ is a trivial ring.

(b) If $A$ is right-invertible and if $n > m$, then $K$ is a trivial ring.

(c) If $A$ is invertible and if $n \neq m$, then $K$ is a trivial ring.

Proof of Theorem 6.90 (a) Assume that $A$ is left-invertible, and that $n < m$.

The matrix $A$ has a left inverse $L$ (since it is left-invertible). Consider this $L$.

We know that $L$ is a left inverse of $A$. In other words, $L$ is an $m \times n$-matrix such that $LA = I_m$ (by the definition of a “left inverse”). But (167) (applied to $m$, $n$, $L$ and $A$ instead of $n$, $m$, $A$ and $B$) yields $\det (LA) = 0$ (since $n < m$). Thus,

$$0 = \det \left( \frac{L}{=I_m} \right) = \det (I_m) = 1.$$ Of course, the 0 and the 1 in this equality mean the elements $0_K$ and $1_K$ of $K$ (rather than the integers 0 and 1); thus, it rewrites as $0_K = 1_K$. In other words, $K$ is a trivial ring. This proves Theorem 6.90 (a).

(b) Assume that $A$ is right-invertible, and that $n > m$.

The matrix $A$ has a right inverse $R$ (since it is right-invertible). Consider this $R$.

We know that $R$ is a right inverse of $A$. In other words, $R$ is an $m \times n$-matrix such that $AR = I_m$ (by the definition of a “right inverse”). But (167) (applied to $B = R$) yields $\det (AR) = 0$ (since $m < n$). Thus, $0 = \det \left( \frac{AR}{=I_n} \right) = \det (I_n) = 1$. Of course, the 0 and the 1 in this equality mean the elements $0_K$ and $1_K$ of $K$ (rather than the integers 0 and 1); thus, it rewrites as $0_K = 1_K$. In other words, $K$ is a trivial ring. This proves Theorem 6.90 (b).

(c) Assume that $A$ is invertible, and that $n \neq m$. Since $n \neq m$, we must be in one of the following two cases:

Case 1: We have $n < m$.

Case 2: We have $n > m$.

Let us first consider Case 1. In this case, we have $n < m$. Now, $A$ is invertible, and thus left-invertible (since every invertible matrix is left-invertible). Hence, $K$ is a trivial ring (according to Theorem 6.90 (a)). Thus, Theorem 6.90 (c) is proven in Case 1.

Let us now consider Case 2. In this case, we have $n > m$. Now, $A$ is invertible, and thus right-invertible (since every invertible matrix is right-invertible). Hence,
K is a trivial ring (according to Theorem 6.90 (b)). Thus, Theorem 6.90 (c) is proven in Case 2.

We have thus proven Theorem 6.90 (c) in both Cases 1 and 2. Thus, Theorem 6.90 (c) always holds.

Theorem 6.90 (c) says that the question whether a matrix is invertible is only interesting for square matrices, unless the ring K is given so inexplicitly that we do not know whether it is trivial or not. Let us now study the invertibility of a square matrix. Here, the determinant turns out to be highly useful:

**Theorem 6.91.** Let $n \in \mathbb{N}$. Let $A$ be an $n \times n$-matrix.

(a) The matrix $A$ is invertible if and only if the element $\det A$ of $K$ is invertible (in $K$).

(b) If $\det A$ is invertible, then the inverse of $A$ is $A^{-1} = \frac{1}{\det A} \cdot \text{adj } A$.

When $K$ is a field, the invertible elements of $K$ are precisely the nonzero elements of $K$. Thus, when $K$ is a field, the statement of Theorem 6.91 (a) can be rewritten as “The matrix $A$ is invertible if and only if $\det A \neq 0$”; this is a cornerstone of linear algebra. But our statement of Theorem 6.91 (a) works for an arbitrary commutative ring $K$. In particular, it works for $K = \mathbb{Z}$. Here is a consequence:

**Corollary 6.92.** Let $n \in \mathbb{N}$. Let $A \in \mathbb{Z}^{n \times n}$ be an $n \times n$-matrix over $\mathbb{Z}$. Then, the matrix $A$ is invertible if and only if $\det A \in \{1, -1\}$.

**Proof of Corollary 6.92.** If $g$ is an integer, then $g$ is invertible (in $\mathbb{Z}$) if and only if $g \in \{1, -1\}$. In other words, for every integer $g$, we have the following equivalence:

$$\left( g \text{ is invertible (in } \mathbb{Z} \text{)} \right) \iff \left( g \in \{1, -1\} \right).$$  \hspace{1cm} (236)

Now, Theorem 6.91 (a) (applied to $K = \mathbb{Z}$) yields that the matrix $A$ is invertible if and only if the element $\det A$ of $\mathbb{Z}$ is invertible (in $\mathbb{Z}$). Thus, we have the following chain of equivalences:

$$\text{(the matrix } A \text{ is invertible)} \iff \left( \det A \text{ is invertible (in } \mathbb{Z} \text{)} \right) \iff \left( \det A \in \{1, -1\} \right) \iff \left( \det A \in \mathbb{Z} \text{) } \right)$$

(by (236), applied to $g = \det A$).

This proves Corollary 6.92.  \hspace{1cm} \Box

---

166This actually happens rather often in algebra! For example, rings are often defined by “generators and relations” (such as “the ring with commuting generators $a, b, c$ subject to the relations $a^2 + b^2 = c^2$ and $ab = c^2$”). Sometimes the relations force the ring to become trivial (for instance, the ring with generator $a$ and relations $a = 1$ and $a^2 = 2$ is clearly the trivial ring, because in this ring we have $2 = a^2 = 1^2 = 1$). Often this is not clear a-priori, and theorems such as Theorem 6.90 can be used to show this. The triviality of a ring can be a nontrivial statement! (Richman makes this point in [Richma].)
Notice that Theorem 6.91(b) yields an explicit way to compute the inverse of a square matrix $A$ (provided that we can compute determinants and the inverse of $\det A$). This is not the fastest way (at least not when $K$ is a field), but it is useful for various theoretical purposes.

Proof of Theorem 6.91 (a) $\implies$: Assume that the matrix $A$ is invertible. In other words, an inverse $B$ of $A$ exists. Consider such a $B$.

The matrix $B$ is an inverse of $A$. In other words, $B$ is an $n \times n$-matrix such that $BA = I_n$ and $AB = I_n$ (by the definition of an “inverse”). Theorem 6.22 yields
\[
\det (AB) = \det A \cdot \det B, \text{ so that } \det A \cdot \det B = \det \begin{pmatrix} AB \\ = I_n \end{pmatrix} = \det (I_n) = 1.
\]
Of course, we also have $\det B \cdot \det A = \det A \cdot \det B = 1$. Thus, $B$ is an inverse of $\det A$ in $K$. Therefore, the element $\det A$ is invertible (in $K$). This proves the $\implies$ direction of Theorem 6.91 (a).

$\Leftarrow$: Assume that the element $\det A$ is invertible (in $K$). Thus, its inverse $\frac{1}{\det A}$ exists. Theorem 6.82 yields
\[
A \cdot \adj A = \adj A \cdot A = \det A \cdot I_n.
\]
Now, define an $n \times n$-matrix $B$ by $B = \frac{1}{\det A} \cdot \adj A$. Then,
\[
A = \frac{B}{\det A} \adj A = \frac{1}{\det A} \cdot \left( \frac{1}{\det A} \cdot \adj A \right) = \frac{1}{\det A} \cdot \adj A = \frac{1}{\det A} \cdot \det A \cdot I_n = I_n
\]
and
\[
B = \frac{A}{\det A} \adj A = \frac{1}{\det A} \cdot \adj A \cdot A = \frac{1}{\det A} \cdot \det A \cdot I_n = I_n.
\]
Thus, $B$ is an $n \times n$-matrix such that $BA = I_n$ and $AB = I_n$. In other words, $B$ is an inverse of $A$ (by the definition of an “inverse”). Thus, an inverse of $A$ exists; in other words, the matrix $A$ is invertible. This proves the $\Leftarrow$ direction of Theorem 6.91 (a).

---

$^\text{167}$In case you don’t know what the notation “$\implies$” here means: Theorem 6.91 (a) is an “if and only if” assertion. In other words, it asserts that $\mathcal{U} \iff \mathcal{V}$ for two statements $\mathcal{U}$ and $\mathcal{V}$. (In our case, $\mathcal{U}$ is the statement “the matrix $A$ is invertible”, and $\mathcal{V}$ is the statement “the element $\det A$ of $K$ is invertible (in $K$)”). In order to prove a statement of the form $\mathcal{U} \iff \mathcal{V}$, it is sufficient to prove the implications $\mathcal{U} \implies \mathcal{V}$ and $\mathcal{U} \Leftarrow \mathcal{V}$. Usually, these two implications are proven separately (although not always; for instance, in the proof of Corollary 6.92, we have used a chain of equivalences to prove $\mathcal{U} \iff \mathcal{V}$ directly). When writing such a proof, one often uses the abbreviations “$\implies$” and “$\Leftarrow$” for “Here comes the proof of the implication $\mathcal{U} \implies \mathcal{V}$” and “Here comes the proof of the implication $\mathcal{U} \Leftarrow \mathcal{V}$”, respectively.
We have now proven both directions of Theorem 6.91 (a). Theorem 6.91 (a) is thus proven.

(b) Assume that det \( A \) is invertible. Thus, its inverse \( \frac{1}{\det A} \) exists. We define an \( n \times n \)-matrix \( B \) by \( B = \frac{1}{\det A} \cdot \text{adj} \ A \). Then, \( B \) is an inverse of \( A \). In other words, \( B \) is the inverse of \( A \). In other words, \( B = A^{-1} \). Hence, \( A^{-1} = B = \frac{1}{\det A} \cdot \text{adj} A \).

This proves Theorem 6.91 (b).

**Corollary 6.93.** Let \( n \in \mathbb{N} \). Let \( A \) and \( B \) be two \( n \times n \)-matrices such that \( AB = I_n \).

(a) We have \( BA = I_n \).

(b) The matrix \( A \) is invertible, and the matrix \( B \) is the inverse of \( A \).

**Proof of Corollary 6.93** Theorem 6.22 yields \( \det (AB) = \det A \cdot \det B \), so that \( \det A \cdot \det B = 1 \). Thus, \( \det B \) is an inverse of \( \det A \) in \( \mathbb{K} \). Therefore, the element \( \det A \) is invertible (in \( \mathbb{K} \)). Therefore, the matrix \( A \) is invertible (according to the \( \iff \) direction of Theorem 6.91 (b)). Thus, the inverse of \( A \) exists. Let \( C \) be this inverse. Thus, \( C \) is a left inverse of \( A \) (since every inverse of \( A \) is a left inverse of \( A \)).

The matrix \( B \) is an \( n \times n \)-matrix satisfying \( AB = I_n \). In other words, \( B \) is a right inverse of \( A \). On the other hand, \( C \) is a left inverse of \( A \). Hence, Proposition 6.87 (applied to \( L = C \) and \( R = B \)) yields \( C = B \). Hence, the matrix \( B \) is the inverse of \( A \) (since the matrix \( C \) is the inverse of \( A \)). Thus, Corollary 6.93 (b) is proven.

Since \( B \) is the inverse of \( A \), we have \( BA = I_n \) and \( AB = I_n \) (by the definition of an “inverse”). This proves Corollary 6.93 (a).

**Remark 6.94.** Corollary 6.93 is not obvious! Matrix multiplication, in general, is not commutative (we have \( AB \neq BA \) more often than not), and there is no reason to expect that \( AB = I_n \) implies \( BA = I_n \). The fact that this is nevertheless true for square matrices took us quite some work to prove (we needed, among other things, the notion of an adjugate). This fact would not hold for rectangular matrices. Nor does it hold for “infinite square matrices”: Without wanting to go into the details of how products of infinite matrices are defined, I invite you to check that the two infinite matrices

\[
\begin{pmatrix}
0 & 1 & 0 & \cdots \\
0 & 0 & 1 & \cdots \\
0 & 0 & 0 & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
0 & 0 & 0 & \cdots \\
1 & 0 & 0 & \cdots \\
0 & 1 & 0 & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{pmatrix}
\]

satisfy \( AB = I_\infty \) but \( BA \neq I_\infty \). This makes Corollary 6.93 (a) 168

\[168\text{We have shown this in our proof of the } \iff \text{ direction of Theorem 6.91 (a).}\]
all the more interesting.

6.15. Noncommutative rings

I think that here is a good place to introduce two other basic notions from algebra: that of a noncommutative ring, and that of a group.

**Definition 6.95.** The notion of a noncommutative ring is defined in the same way as we have defined a commutative ring (in Definition 6.2), except that we no longer require the “Commutativity of multiplication” axiom.

As I have already said, the word “noncommutative” (in “noncommutative ring”) does not mean that commutativity of multiplication has to be false in this ring; it only means that commutativity of multiplication is not required. Thus, every commutative ring is a noncommutative ring. Therefore, each of the examples of a commutative ring given in Section 6.1 is also an example of a noncommutative ring. Of course, it is more interesting to see some examples of noncommutative rings which actually fail to obey commutativity of multiplication. Here are some of these examples:

- If \( n \in \mathbb{N} \) and if \( \mathbb{K} \) is a commutative ring, then the set \( \mathbb{K}^{n \times n} \) of matrices becomes a noncommutative ring (when endowed with the addition and multiplication of matrices, with the zero \( 0_{n \times n} \) and with the unity \( I_n \)). This is actually a commutative ring when \( \mathbb{K} \) is trivial or when \( n \leq 1 \), but in all “interesting” cases it is not commutative.

- If you have heard of the [quaternions](#), you should realize that they form a noncommutative ring.

- Given a commutative ring \( \mathbb{K} \) and \( n \) distinct symbols \( X_1, X_2, \ldots, X_n \), we can define a ring of polynomials in the noncommutative variables \( X_1, X_2, \ldots, X_n \) over \( \mathbb{K} \). We do not want to go into the details of its definition at this point, but let us just mention some examples of its elements: For instance, the ring of polynomials in the noncommutative variables \( X \) and \( Y \) over \( \mathbb{Q} \) contains elements such as \( 1 + \frac{2}{3}X, X^2 + \frac{3}{2}Y - 7XY + YX, 2XY, 2YX \) and \( 5X^2Y - 6XYX + 7Y^2X \) (and of course, the elements \( XY \) and \( YX \) are not equal).

- If \( n \in \mathbb{N} \) and if \( \mathbb{K} \) is a commutative ring, then the set of all lower-triangular \( n \times n \)-matrices over \( \mathbb{K} \) becomes a noncommutative ring (with addition, multiplication, zero and unity defined in the same way as in \( \mathbb{K}^{n \times n} \)). This is because the sum and the product of any two lower-triangular \( n \times n \)-matrices over \( \mathbb{K} \) are again lower-triangular, and because the matrices \( 0_{n \times n} \) and \( I_n \) are lower-triangular.

\(^{169}\) Check this! (For the sum, it is clear, but for the product, it is an instructive exercise.)
• In contrast, the set of all invertible $2 \times 2$-matrices over $K$ is not a noncommutative ring (for example, because the sum of the two invertible matrices $I_2$ and $-I_2$ is not invertible).

• If $K$ is a commutative ring, then the set of all invertible $3 \times 3$-matrices over $K$ is not a noncommutative ring (for example, because the sum of the two invertible matrices $I_2$ and $-I_2$ is not invertible).

• On the other hand, if $K$ is a commutative ring, then the set of all $3 \times 3$-matrices (over $K$) of the form
  \[
  \begin{pmatrix}
  a & b & c \\
  0 & d & 0 \\
  0 & 0 & f
  \end{pmatrix}
  \]
  (with $a, b, c, d, f \in K$) is not a noncommutative ring (unless $K$ is trivial), because products of matrices in this set are not always in this set.

For the rest of this section, we let $L$ be a noncommutative ring. What can we do with elements of $L$? We can do some of the things that we can do with a commutative ring, but not all of them. For example, we can still define the sum $a_1 + a_2 + \cdots + a_n$ and the product $a_1 a_2 \cdots a_n$ of $n$ elements of a noncommutative ring. But we cannot arbitrarily reorder the factors of a product and expect to always get the same result! (With a sum, we can do this.) We can still define $na$ for any $n \in \mathbb{Z}$ and $a \in L$ (in the same way as we defined $na$ for $n \in \mathbb{Z}$ and $a \in K$ when $K$ was a commutative ring). We can still define $a^n$ for any $n \in \mathbb{N}$ and $a \in L$ (again, in the same fashion as for commutative rings). The identities (123), (124), (125), (126), (127), (128), (129) and (130) still hold when the commutative ring $K$ is replaced by the noncommutative ring $L$; but the identities (131) and (132) may not (although they do hold if we additionally assume that $ab = ba$). Finite sums such as $\sum_{s \in S} a_s$ (where $S$ is a finite set, and $a_s \in L$ for every $s \in S$) are well-defined, but finite products such as $\prod_{s \in S} a_s$ are not (unless we specify the order in which their factors are to be multiplied).

\[170\] To check this, one needs to prove that the matrices $0_{3 \times 3}$ and $I_3$ have this form, and that the sum and the product of any two matrices of this form is again a matrix of this form. All of this is clear, except for the claim about the product. The latter claim follows from the computation

\[
\begin{pmatrix}
  a & b & c \\
  0 & d & 0 \\
  0 & 0 & f
\end{pmatrix}
\begin{pmatrix}
  a' & b' & c' \\
  0 & d' & 0 \\
  0 & 0 & f'
\end{pmatrix} =
\begin{pmatrix}
  aa' & bd' + ab' & cf' + ac' \\
  0 & dd' & 0 \\
  0 & 0 & ff'
\end{pmatrix}.
\]

\[171\] Indeed, if $a, b, c, d, f \in \mathbb{R}$, then

\[
\begin{pmatrix}
  a & b & 0 \\
  0 & c & d \\
  0 & 0 & f
\end{pmatrix}
\begin{pmatrix}
  a' & b' & 0 \\
  0 & c' & d' \\
  0 & 0 & f'
\end{pmatrix} =
\begin{pmatrix}
  aa' & ab' + bc' & bd' \\
  0 & cc' & cd' + df' \\
  0 & 0 & ff'
\end{pmatrix}
\]

can have $bd' \neq 0$. 
We can define matrices over $\mathbb{L}$ in the same way as we have defined matrices over $\mathbb{K}$. We can even define the determinant of a square matrix over $\mathbb{L}$ using the formula (134); however, this determinant lacks many of the important properties that determinants over $\mathbb{K}$ have (for instance, it satisfies neither Exercise 22 nor Theorem 6.22), and is therefore usually not studied.

We define the notion of an inverse of an element $a \in \mathbb{L}$; in order to do so, we simply replace $\mathbb{K}$ by $\mathbb{L}$ in Definition 6.51. (Now it suddenly matters that we required both $ab = 1$ and $ba = 1$ in Definition 6.51.) Proposition 6.52 still holds (and its proof still works) when $\mathbb{K}$ is replaced by $\mathbb{L}$.

We define the notion of an invertible element of $\mathbb{L}$; in order to do so, we simply replace $\mathbb{K}$ by $\mathbb{L}$ in Definition 6.53 (a). We cannot directly replace $\mathbb{K}$ by $\mathbb{L}$ in Definition 6.53 (b), because for two invertible elements $a$ and $b$ of $\mathbb{L}$ we do not necessarily have $(ab)^{-1} = a^{-1}b^{-1}$; but something very similar holds (namely, $(ab)^{-1} = b^{-1}a^{-1}$). Trying to generalize Definition 6.53 (c) to noncommutative rings is rather hopeless: In general, we cannot bring a “noncommutative fraction” of the form $ba^{-1} + dc^{-1}$ to a “common denominator”.

Example 6.96. Let $\mathbb{K}$ be a commutative ring. Let $n \in \mathbb{N}$. As we know, $\mathbb{K}^{n \times n}$ is a noncommutative ring. The invertible elements of this ring are exactly the invertible $n \times n$-matrices. (To see this, just compare the definition of an invertible element of $\mathbb{K}^{n \times n}$ with the definition of an invertible $n \times n$-matrix. These definitions are clearly equivalent.)

6.16. Groups, and the group of units

Let me finally define the notion of a group.

Definition 6.97. A group means a set $G$ endowed with

- a binary operation called “multiplication” (or “composition”, or just “binary operation”), and denoted by $\cdot$, and written infix, and

- an element called $1_G$ (or $e_G$)

such that the following axioms are satisfied:

- **Associativity**: We have $a(bc) = (ab)c$ for all $a \in G$, $b \in G$ and $c \in G$. Here and in the following, $ab$ is shorthand for $a \cdot b$ (as is usual for products of numbers).

- **Neutrality of 1**: We have $a1_G = 1_Ga = a$ for all $a \in G$.

- **Existence of inverses**: For every $a \in G$, there exists an element $a' \in G$ such that $aa' = a'a = 1_G$. This $a'$ is commonly denoted by $a^{-1}$ and called the inverse of $a$. (It is easy to check that it is unique.)

Some algebraists have come up with subtler notions of determinants for matrices over noncommutative rings. But I don’t want to go in that direction here.
Definition 6.98. The element $1_G$ of a group $G$ is denoted the neutral element (or the identity) of $G$.

The binary operation $\cdot$ in Definition 6.97 is usually not identical with the binary operation $\cdot$ on the set of integers, and is denoted by $\cdot_G$ when confusion can arise.

The definition of a group has similarities with that of a noncommutative ring. Viewed from a distance, it may look as if a noncommutative ring would “consist” of two groups with the same underlying set. This is not quite correct, though, because the multiplication in a nontrivial ring does not satisfy the “existence of inverses” axiom. But it is true that there are two groups in every noncommutative ring:

Proposition 6.99. Let $\mathbb{L}$ be a noncommutative ring.

(a) The set $\mathbb{L}$, endowed with the addition $+_{\mathbb{L}}$ (as multiplication) and the element $0_{\mathbb{L}}$ (as neutral element), is a group. This group is called the additive group of $\mathbb{L}$, and denoted by $\mathbb{L}^+$. 

(b) Let $\mathbb{L}^\times$ denote the set of all invertible elements of $\mathbb{L}$. Then, the product of two elements of $\mathbb{L}^\times$ again belongs to $\mathbb{L}^\times$. Thus, we can define a binary operation $\cdot_{\mathbb{L}^\times}$ on the set $\mathbb{L}^\times$ (written infix) by

$$a \cdot_{\mathbb{L}^\times} b = ab$$

for all $a \in \mathbb{L}^\times$ and $b \in \mathbb{L}^\times$.

The set $\mathbb{L}^\times$, endowed with the multiplication $\cdot_{\mathbb{L}^\times}$ (as multiplication) and the element $1_{\mathbb{L}}$ (as neutral element), is a group. This group is called the group of units of $\mathbb{L}$.

Proof of Proposition 6.99

(a) The addition $+_{\mathbb{L}}$ is clearly a binary operation on $\mathbb{L}$, and the element $0_{\mathbb{L}}$ is clearly an element of $\mathbb{L}$. The three axioms in Definition 6.97 are clearly satisfied for the binary operation $+_{\mathbb{L}}$ and the element $0_{\mathbb{L}}$. Therefore, the set $\mathbb{L}$, endowed with the addition $+_{\mathbb{L}}$ (as multiplication) and the element $0_{\mathbb{L}}$ (as neutral element), is a group. This proves Proposition 6.99 (a).

(b) If $a \in \mathbb{L}^\times$ and $b \in \mathbb{L}^\times$, then $ab \in \mathbb{L}^\times$. In other words, the product of two

---

173 In fact, they boil down to the “associativity of addition”, “neutrality of 0” and “existence of additive inverses” axioms in the definition of a noncommutative ring.

174 Proof. Let $a \in \mathbb{L}^\times$ and $b \in \mathbb{L}^\times$. We have $a \in \mathbb{L}^\times$; in other words, $a$ is an invertible element of $\mathbb{L}$ (because $\mathbb{L}^\times$ is the set of all invertible elements of $\mathbb{L}$). Thus, the inverse $a^{-1}$ of $a$ is well-defined. Similarly, the inverse $b^{-1}$ of $b$ is well-defined. Now, since we have

$$\left( b^{-1} a^{-1} \right) (ab) = b^{-1} a^{-1} a b = b^{-1} b = 1_{\mathbb{L}}$$

and

$$\left( ab \right) b^{-1} a^{-1} = a b b^{-1} a^{-1} = a a^{-1} = 1_{\mathbb{L}}$$

we see that the element $b^{-1} a^{-1}$ of $\mathbb{L}$ is an inverse of $ab$. Thus, the element $ab$ has an inverse. In other words, $ab$ is invertible. In other words, $ab \in \mathbb{L}^\times$ (since $\mathbb{L}^\times$ is the set of all invertible elements of $\mathbb{L}$), qed.
elements of $\mathbb{L}^\times$ again belongs to $\mathbb{L}^\times$. Thus, we can define a binary operation $\cdot_{\mathbb{L}^\times}$ on the set $\mathbb{L}^\times$ (written infix) by

$$a \cdot_{\mathbb{L}^\times} b = ab$$

for all $a \in \mathbb{L}^\times$ and $b \in \mathbb{L}^\times$.

Also, $1_\mathbb{L}$ is an invertible element of $\mathbb{L}$ (indeed, its inverse is $1_\mathbb{L}$), and thus an element of $\mathbb{L}^\times$.

Now, we need to prove that the set $\mathbb{L}^\times$, endowed with the multiplication $\cdot_{\mathbb{L}^\times}$ (as multiplication) and the element $1_\mathbb{L}$ (as neutral element), is a group. In order to do so, we need to check that the “associativity”, “neutrality of 1” and “existence of inverses” axioms are satisfied.

The “associativity” axiom follows from the “associativity of multiplication” axiom in the definition of a noncommutative ring. The “neutrality of 1” axiom follows from the “unitality” axiom in the definition of a noncommutative ring. It thus remains to prove that the “existence of inverses” axiom holds.

Thus, let $a \in \mathbb{L}^\times$. We need to show that there exists an $a' \in \mathbb{L}^\times$ such that $a \cdot_{\mathbb{L}^\times} a' = a' \cdot_{\mathbb{L}^\times} a = 1_\mathbb{L}$ (since $1_\mathbb{L}$ is the neutral element of $\mathbb{L}^\times$).

We know that $a$ is an invertible element of $\mathbb{L}$ (since $a \in \mathbb{L}^\times$); it thus has an inverse $a^{-1}$. Now, $a$ itself is an inverse of $a^{-1}$ (since $aa^{-1} = 1_\mathbb{L}$ and $a^{-1}a = 1_\mathbb{L}$), and thus the element $a^{-1}$ of $\mathbb{L}$ has an inverse. In other words, $a^{-1}$ is invertible, so that $a^{-1} \in \mathbb{L}^\times$. The definition of the operation $\cdot_{\mathbb{L}^\times}$ shows that $a \cdot_{\mathbb{L}^\times} a^{-1} = aa^{-1} = 1_\mathbb{L}$ and that $a^{-1} \cdot_{\mathbb{L}^\times} a = a^{-1}a = 1_\mathbb{L}$. Hence, there exists an $a' \in \mathbb{L}^\times$ such that $a \cdot_{\mathbb{L}^\times} a' = a' \cdot_{\mathbb{L}^\times} a = 1_\mathbb{L}$ (namely, $a' = a^{-1}$). Thus we have proven that the “existence of inverses” axiom holds. The proof of Proposition 6.99 (b) is thus complete.

We now have a plentitude of examples of groups: For every noncommutative ring $\mathbb{L}$, we have the two groups $\mathbb{L}^+$ and $\mathbb{L}^\times$ defined in Proposition 6.99. Another example, for every set $X$, is the symmetric group of $X$ (endowed with the composition of permutations as multiplication, and the identity permutation id : $X \to X$ as the neutral element). (Many other examples can be found in textbooks on algebra, such as Artin.)

**Remark 6.100.** Throwing all notational ballast aside, we can restate Proposition 6.99 (b) as follows: The set of all invertible elements of a noncommutative ring $\mathbb{L}$ is a group (where the binary operation is multiplication). We can apply this to the case where $\mathbb{L} = \mathbb{K}^{n \times n}$ for a commutative ring $\mathbb{K}$ and an integer $n \in \mathbb{N}$. Thus, we obtain that the set of all invertible elements of $\mathbb{K}^{n \times n}$ is a group. Since we know that the invertible elements of $\mathbb{K}^{n \times n}$ are exactly the invertible $n \times n$-matrices (by Example 6.96), we thus have shown that the set of all invertible $n \times n$-matrices is a group. This group is commonly denoted by $\text{GL}_n(\mathbb{K})$.

### 6.17. Cramer’s rule

Let us return to the classical properties of determinants. We have already proven many, but here is one more: It is an application of determinants to solving systems of linear equations.
Theorem 6.101. Let \( n \in \mathbb{N} \). Let \( A \) be an \( n \times n \)-matrix. Let \( b = (b_1, b_2, \ldots, b_n)^T \) be a column vector of length \( n \) (that is, an \( n \times 1 \)-matrix).

For every \( j \in \{1, 2, \ldots, n\} \), let \( A_j^\# \) be the \( n \times n \)-matrix obtained from \( A \) by replacing the \( j \)-th column of \( A \) with the vector \( b \).

(a) We have \( A \cdot \left( \det (A_1^\#), \det (A_2^\#), \ldots, \det (A_n^\#) \right)^T = \det A \cdot b \).

(b) Assume that the matrix \( A \) is invertible. Then, \( A^{-1} b = \left( \frac{\det (A_1^\#)}{\det A}, \frac{\det (A_2^\#)}{\det A}, \ldots, \frac{\det (A_n^\#)}{\det A} \right)^T \).

Theorem 6.101 (or either part of it) is known as Cramer’s rule.

Remark 6.102. A system of \( n \) linear equations in \( n \) variables \( x_1, x_2, \ldots, x_n \) can be written in the form \( Ax = b \), where \( A \) is a fixed \( n \times n \)-matrix and \( b \) is a column vector of length \( n \) (and where \( x \) is the column vector \((x_1, x_2, \ldots, x_n)^T\) containing all the variables). When the matrix \( A \) is invertible, it thus has a unique solution: namely, \( x = A^{-1} b \) (just multiply the equation \( Ax = b \) from the left with \( A^{-1} \) to see this), and this solution can be computed using Theorem 6.101. This looks nice, but isn’t actually all that useful for solving systems of linear equations: For one thing, this does not immediately help us solve systems of fewer or more than \( n \) equations in \( n \) variables; and even in the case of exactly \( n \) equations, the matrix \( A \) coming from a system of linear equations will not always be invertible (and in the more interesting cases, it will not be). For another thing, at least when \( \mathbb{K} \) is a field, there are faster ways to solve a system of linear equations than anything that involves computing \( n + 1 \) determinants of \( n \times n \)-matrices. Theorem 6.101 nevertheless turns out to be useful in proofs.

Proof of Theorem 6.101. (a) Fix \( j \in \{1, 2, \ldots, n\} \). Let \( C = A_j^\# \). Thus, \( C = A_j^\# \) is the \( n \times n \)-matrix obtained from \( A \) by replacing the \( j \)-th column of \( A \) with the vector \( b \).

In particular, the \( j \)-th column of \( C \) is the vector \( b \). In other words, we have

\[
c_{p,j} = b_p \quad \text{for every } p \in \{1, 2, \ldots, n\}.
\] (237)

Furthermore, the matrix \( C \) is equal to the matrix \( A \) in all columns but its \( j \)-th column (because it is obtained from \( A \) by replacing the \( j \)-th column of \( A \) with the vector \( b \)). Thus, if we cross out the \( j \)-th columns in both matrices \( C \) and \( A \), then these two matrices become equal. Consequently,

\[
C_{\sim p, \sim j} = A_{\sim p, \sim j} \quad \text{for every } p \in \{1, 2, \ldots, n\}
\] (238)

\[175\]The reader should keep in mind that \((b_1, b_2, \ldots, b_n)^T\) is just a space-saving way to write \[
\begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{pmatrix}.
\]
(because the matrices $C_{p, j}$ and $A_{p, j}$ are obtained by crossing out the $p$-th row and the $j$-th column in the matrices $C$ and $A$, respectively). Now,

$$\det \left( \begin{array}{ccc} A^\#_j & = & C \\ \end{array} \right) = \det C = \sum_{p=1}^{n} (-1)^{p+j} c_{p,j} \begin{array}{ccc} \text{det} C_{p, j} \\ \vspace{-1ex} \text{by } (237) \\ \end{array} = \begin{array}{ccc} \text{det} A_{p, j} \\ \vspace{-1ex} \text{by } (238) \\ \end{array}$$

by Theorem 6.64 (b), applied to $C$, $c_{i,j}$ and $j$ instead of $A$, $a_{i,j}$ and $q$.

$$= \sum_{p=1}^{n} (-1)^{p+j} b_p \det (A_{p, j}). \quad (239)$$

Let us now forget that we fixed $j$. We thus have proven (239) for every $j \in \{1, 2, \ldots, n\}$. Now, fix $i \in \{1, 2, \ldots, n\}$. Then, for every $p \in \{1, 2, \ldots, n\}$ satisfying $p \neq i$, we have

$$\sum_{q=1}^{n} b_p (-1)^{p+q} a_{i,q} \det (A_{p, q}) = 0 \quad (240)$$

Also, we have

$$\sum_{q=1}^{n} b_i (-1)^{i+q} a_{i,q} \det (A_{i, q}) = \det A \cdot b_i \quad (242)$$

176 Proof of (240): Let $p \in \{1, 2, \ldots, n\}$ be such that $p \neq i$. Hence, Proposition 6.78 (a) (applied to $r = i$) shows that

$$0 = \sum_{q=1}^{n} (-1)^{p+q} a_{i,q} \det (A_{p, q}). \quad (241)$$

Now,

$$\sum_{q=1}^{n} b_p (-1)^{p+q} a_{i,q} \det (A_{p, q}) = b_p \sum_{q=1}^{n} (-1)^{p+q} a_{i,q} \det (A_{p, q}) = 0.$$

(by 241)

Thus, (240) is proven.
\[ \sum_{k=1}^{n} a_{i,k} \det \left( A^k_i \right) \]
\[ = \sum_{p=1}^{n} (-1)^{p+k} b_p \det (A_{\sim_p \sim k}) \]
(by (239), applied to \( j = k \))
\[ = \sum_{k=1}^{n} a_{i,k} \sum_{p=1}^{n} (-1)^{p+k} b_p \det (A_{\sim_p \sim k}) \]
\[ = \sum_{p=1}^{n} \sum_{q=1}^{n} (-1)^{p+q} b_p a_{i,q} \det (A_{\sim_p \sim q}) \]
\[ = \sum_{p \in \{1, \ldots, n\}} \sum_{q=1}^{n} b_p (-1)^{p+q} a_{i,q} \det (A_{\sim_p \sim q}) \]
\[ = \sum_{p \in \{1, \ldots, n\}; \, p \neq i} \sum_{q=1}^{n} b_p (-1)^{p+q} a_{i,q} \det (A_{\sim_p \sim q}) + b_i (-1)^{i+q} a_{i,q} \det (A_{\sim_i \sim q}) \]
\[ = \det A \cdot b_i \]
\[ (\text{by (240)}) \]
\[ (\text{by (242)}) \]
\[ (\text{here, we have split off the addend for } p = i \text{ from the sum}) \]
\[ = \sum_{p \in \{1, \ldots, n\}; \, p \neq i} 0 + \det A \cdot b_i = \det A \cdot b_i. \]  
(244)

Now, let us forget that we fixed \( i \). We thus have proven (244) for every \( i \in \{1, \ldots, n\} \).

177 Proof of (242): Applying Theorem 6.64 (a) to \( p = i \), we obtain
\[ \det A = \sum_{q=1}^{n} (-1)^{i+q} a_{i,q} \det (A_{\sim_i \sim q}). \]  
(243)

Now,
\[ \sum_{q=1}^{n} b_i (-1)^{i+q} a_{i,q} \det (A_{\sim_i \sim q}) = b_i \sum_{q=1}^{n} (-1)^{i+q} a_{i,q} \det (A_{\sim_i \sim q}) = b_i \det A = \det A \cdot b_i. \]
\[ (\text{by (243)}) \]
This proves (242).
\{1, 2, \ldots, n\}. Now, let \(d\) be the vector \((\det(A_1^#), \det(A_2^#), \ldots, \det(A_n^#))^T\). Thus,

\[
d = (\det(A_1^#), \det(A_2^#), \ldots, \det(A_n^#))^T = \left(\begin{array}{c}
\det(A_1^#) \\
\det(A_2^#) \\
\vdots \\
\det(A_n^#)
\end{array}\right)
\]

Thus, \(d = (\det(A_1^#))^T_{1 \leq i \leq n, 1 \leq j \leq 1}\).

The definition of the product of two matrices shows that

\[
A \cdot d = \left(\sum_{k=1}^{n} a_{i,k} \det(A_k^#)\right)_{1 \leq i \leq n, 1 \leq j \leq 1}
\]

(by \(244\))

\[
= (\det(A \cdot b))_{1 \leq i \leq n, 1 \leq j \leq 1} = (\det A^#)^T_{1 \leq i \leq n, 1 \leq j \leq 1}
\]

Comparing this with

\[
\det A \cdot (b_1, b_2, \ldots, b_n)^T = (\det A \cdot b_1, \det A \cdot b_2, \ldots, \det A \cdot b_n)^T,
\]

we obtain \(A \cdot d = \det A \cdot b\). Since \(d = (\det(A_1^#), \det(A_2^#), \ldots, \det(A_n^#))^T\), we can rewrite this as \(A \cdot (\det(A_1^#), \det(A_2^#), \ldots, \det(A_n^#))^T = \det A \cdot b\). This proves Theorem 6.101 (a).

(b) Theorem 6.91 (a) shows that the matrix \(A\) is invertible if and only if the element \(\det A\) of \(\mathbb{K}\) is invertible (in \(\mathbb{K}\)). Hence, the element \(\det A\) of \(\mathbb{K}\) is invertible (since the matrix \(A\) is invertible). Thus, \(\frac{1}{\det A}\) is well-defined. Clearly,
\[
\frac{1}{\det A} \cdot \det A \cdot b = b, \text{ so that } \frac{1}{\det A} \cdot \det A \cdot b = b = \left( \det(A^1), \det(A^2), \ldots, \det(A^n) \right)^T
\]

(by Theorem 6.101(a))

\[
= \frac{1}{\det A} \cdot A \cdot \left( \det(A^1), \det(A^2), \ldots, \det(A^n) \right)^T
\]

\[
= A \cdot \left( \frac{1}{\det A} \cdot \left( \det(A^1), \det(A^2), \ldots, \det(A^n) \right)^T \right)
\]

\[
= \left( \frac{1}{\det A} \cdot \frac{1}{\det A} \cdot \ldots \cdot \frac{1}{\det A} \right)^T \det(A^1) \det(A^2) \ldots \det(A^n)
\]

\[
= A \cdot \left( \frac{\det(A^1)}{\det A}, \frac{\det(A^2)}{\det A}, \ldots, \frac{\det(A^n)}{\det A} \right)^T
\]

Therefore,

\[
A^{-1} \cdot b = A \cdot \left( \frac{\det(A^1)}{\det A}, \frac{\det(A^2)}{\det A}, \ldots, \frac{\det(A^n)}{\det A} \right)^T
\]

\[
= A^{-1} A \cdot \left( \frac{\det(A^1)}{\det A}, \frac{\det(A^2)}{\det A}, \ldots, \frac{\det(A^n)}{\det A} \right)^T
\]

\[
= I_n \cdot \left( \frac{\det(A^1)}{\det A}, \frac{\det(A^2)}{\det A}, \ldots, \frac{\det(A^n)}{\det A} \right)^T
\]

This proves Theorem 6.101(b).

[To be continued!]
Additional exercise 18. Compute the determinant of the horrible $7 \times 7$-matrix

$$
\begin{pmatrix}
a & 0 & 0 & 0 & 0 & b \\
0 & a' & 0 & 0 & b' & 0 \\
0 & 0 & a'' & 0 & b'' & 0 \\
0 & 0 & 0 & e & 0 & 0 \\
0 & 0 & c'' & 0 & d'' & 0 \\
0 & c' & 0 & 0 & d' & 0 \\
c & 0 & 0 & 0 & 0 & d
\end{pmatrix}.
$$

Additional exercise 19. Recall that the binomial coefficients satisfy the recurrence relation (46), which (visually) says that every entry of Pascal’s triangle is the sum of the two entries left-above it and right-above it.

Let us now define a variation of Pascal’s triangle as follows: Define a nonnegative integer $\binom{m}{n}_D$ for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$ recursively as follows:

- Set $\binom{0}{n}_D = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n > 0 \end{cases}$ for every $n \in \mathbb{N}$.

- For every $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$, set $\binom{m}{n}_D = 0$ if either $m$ or $n$ is negative.

- For every positive integer $m$ and every $n \in \mathbb{N}$, set

$$
\binom{m}{n}_D = \binom{m-1}{n-1}_D + \binom{m-1}{n}_D + \binom{m-2}{n-1}_D.
$$

(Thus, if we lay these $\binom{m}{n}_D$ out in the same way as the binomial coefficients $\binom{m}{n}$ in Pascal’s triangle, then every entry is the sum of the three entries left-above it, right-above it, and straight above it.)

The integers $\binom{m}{n}_D$ are known as the Delannoy numbers.

(a) Show that

$$
\binom{n+m}{n}_D = \sum_{i=0}^{n} \binom{n}{i} \binom{m+i}{n} = \sum_{i=0}^{n} \binom{n}{i} \binom{m}{i} 2^i
$$

for every $n \in \mathbb{N}$ and $m \in \mathbb{N}$. (The second equality sign here is a consequence of Proposition 3.9 (e).)
(b) Let $n \in \mathbb{N}$. Let $A$ be the $n \times n$-matrix $\left(\begin{array}{c}
 + j - 2 \\
i - 1 \end{array}\right)_{1 \leq i \leq n, 1 \leq j \leq n}$ (an analogue of the matrix $A$ from Exercise 28). Show that
\[ \det A = 2^{n(n-1)/2}. \]

**Additional exercise 20.** Let $n \in \mathbb{N}$. Let $A$ be an $n \times n$-matrix over the commutative ring $\mathbb{K}$. Consider the commutative ring $\mathbb{K}[X]$ of polynomials in the indeterminate $X$ (that is, polynomials in the indeterminate $X$ with coefficients lying in $\mathbb{K}$). We can then regard $A$ as a matrix over the ring $\mathbb{K}[X]$ as well (because every element of $\mathbb{K}$ can be viewed as a constant polynomial in $\mathbb{K}[X]$).

Consider the $n \times n$-matrix $A + XI_n$ over the commutative ring $\mathbb{K}[X]$. (For example, if $n = 2$ and $A = \begin{pmatrix} a & b \\
c & d \end{pmatrix}$, then $A + XI_n = \begin{pmatrix} a & b \\
c & d \end{pmatrix} + X \begin{pmatrix} 1 & 0 \\
0 & 1 \end{pmatrix} = \begin{pmatrix} a + X & b \\
c & d + X \end{pmatrix}$.) In general, the matrix $A + XI_n$ is obtained from $A$ by adding an $X$ to each diagonal entry.

The determinant $\det (A + XI_n)$ is a polynomial in $\mathbb{K}[X]$. (For instance, for $n = 2$ and $A = \begin{pmatrix} a & b \\
c & d \end{pmatrix}$, we have
\[ \det (A + XI_n) = \det \begin{pmatrix} a + X & b \\
c & d + X \end{pmatrix} = (a + X)(d + X) - bc = X^2 + (a + d)X + (ad - bc). \]

What can you say about the coefficients of this polynomial? Most importantly, what are the coefficients before $X^n$, before $X^{n-1}$, and before $X^0$? Can you express the other coefficients as sums of determinants?

**Additional exercise 21.** Let $n \in \mathbb{N}$. Let $u$ be a column vector of length $n$, and let $v$ be a row vector of length $n$. (Thus, $uv$ is an $n \times n$-matrix, whereas $vu$ is a $1 \times 1$-matrix.) Let $A$ be an $n \times n$-matrix. Prove that
\[ \det (A + uv) = \det A + v (\text{adj} A) u \]
(where we regard the $1 \times 1$-matrix $v (\text{adj} A) u$ as an element of $\mathbb{K}$).

**Additional exercise 22.** Let $P = \sum_{k=0}^{d} p_k X^k$ and $Q = \sum_{k=0}^{e} q_k X^k$ be two polynomials over $\mathbb{K}$ (where $p_0, p_1, \ldots, p_d \in \mathbb{K}$ and $q_0, q_1, \ldots, q_e \in \mathbb{K}$ are their coefficients). Define a $(d + e) \times (d + e)$-matrix $A$ as follows:
• For every $k \in \{1, 2, \ldots, e\}$, the $k$-th row of $A$ is
\[
\begin{pmatrix}
0, 0, \ldots, 0, p_d, p_{d-1}, \ldots, p_1, p_0, 0, 0, \ldots, 0 \\
_{k-1 \text{ zeroes}}^{e-k \text{ zeroes}}
\end{pmatrix}.
\]

• For every $k \in \{1, 2, \ldots, d\}$, the $(e+k)$-th row of $A$ is
\[
\begin{pmatrix}
0, 0, \ldots, 0, q_e, q_{e-1}, \ldots, q_1, q_0, 0, 0, \ldots, 0 \\
_{k-1 \text{ zeroes}}^{d-k \text{ zeroes}}
\end{pmatrix}.
\]

(For example, if $d = 4$ and $e = 3$, then
\[
A = \begin{pmatrix}
p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\
0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\
0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\
q_3 & q_2 & q_1 & q_0 & 0 & 0 & 0 \\
0 & q_3 & q_2 & q_1 & q_0 & 0 & 0 \\
0 & 0 & q_3 & q_2 & q_1 & q_0 & 0 \\
0 & 0 & 0 & q_3 & q_2 & q_1 & q_0
\end{pmatrix}.
\]

Assume that the polynomials $P$ and $Q$ have a common root $z$ (that is, there exists a $z \in \mathbb{K}$ such that $P(z) = 0$ and $Q(z) = 0$). Show that $\det A = 0$.

[Hint: Find a column vector $v$ of length $d+e$ satisfying $Av = 0_{(d+e) \times 1}$; then apply Corollary 6.84]

Remark 6.103. The matrix $A$ in Additional exercise 22 is called the **Sylvester matrix** of the polynomials $P$ and $Q$ (for degrees $d$ and $e$); its determinant $\det A$ is known as their **resultant** (at least when $d$ and $e$ are actually the degrees of $P$ and $Q$). According to the exercise, the condition $\det A = 0$ is necessary for $P$ and $Q$ to have a common root. In the general case, the converse does not hold: For one, you can always force $\det A$ to be 0 by taking $d > \deg P$ and $e > \deg Q$ (so $p_d = 0$ and $q_e = 0$, and thus the 1-st column of $A$ consists of zeroes). More importantly, the resultant of the two polynomials $X^3 - 1$ and $X^2 + X + 1$ is 0, but they only have common roots in $\mathbb{C}$, not in $\mathbb{R}$. Thus, there is more to common roots than just the vanishing of a determinant.

However, if $\mathbb{K}$ is an algebraically closed field (I won’t go into the details of what this means, but an example of such a field is $\mathbb{C}$), and if $d = \deg P$ and $e = \deg Q$, then the polynomials $P$ and $Q$ have a common root if and only if their resultant is 0.
References


http://web.mit.edu/~darij/www/


