Logic, Quantifiers and Methods of Reasoning

Baptiste Arnaudo

Logic is the hygiene a mathematician practices to keep his ideas healthy and strong
Hermann Weyl, 1885 - 1955

Contents

1 Introduction

If mathematics seeks to find the truth, logic shows the paths to get there. Through the study of *truth tables* of propositions, one deduces general reasoning methods, useful in all fields of mathematics, allowing to prove elaborate statements. Quantifiers and other symbols, in turn, formalize the whole into a language understandable by all those who pay it a little attention.
In this course, we present the principal elements of logic, such as the negation of a proposition, the so-called or and the so-called and in mathematics, the concepts of implication, of equivalence... before showing the principal methods of reasoning that allow to prove a statement, useful in **every** mathematical exercise. We will also of course define the different symbols employed.

2 What is a proposition?

Definition 1. ***On what a proposition is***
A proposition is a ***statement*** *to which can be assigned two* ***truth values****: true or false.*

For example, let us consider the following proposition denoted P:

P: For every positive real x, x is greater than 2^x

In mathematical language, one would write:

$$P : \forall x \in \mathbb{R}^+, \ x \geq 2^x$$

(Note that - as a French person - "greater than" means "greater than or equal" to me, where as it means "strictly greater" for an English person... Language barriers !)

Definition 2. ***Universal quantifier***
The symbol $\forall$ *is read for all or also whatever and is called the* ***universal quantifier****.*

What about the truth value of P? It is false of course, because for $x = 0$, we do have x positive and $2^0 = 1 > 0 = x$, the value $x = 0$ puts the proposition in default: this is what we call a **counter-example**. Counter-examples serve to refute propositions beginning with For all... , provided of course that these can be refuted, hence are false. For example, the proposition:

$$\forall x \in \mathbb{R}, \cos^2(x) + \sin^2(x) = 1$$

is true, so we cannot find a counter-example to it. Same for the following very useful inequality:

$$\forall x \in \mathbb{R}, \ e^x \geq 1 + x$$

which we invite the reader to prove by the method of his or her choice (a study of function works very well).

3 Truth tables and operations on propositions

3.1 Truth tables and equivalence of propositions

Definition 3. ***Truth table***
A truth table is a table that one associates with a proposition. In the columns on the left appear all the possibilities of the truth values of the propositions on which the studied proposition depends. In the right-hand column, the truth value of the studied proposition as a function of the truth values of the propositions on the left.

3.2 Negation of a proposition

Let us immediately give the example (and the definition) of the **negation** of a proposition, which corresponds exactly to the intuition one may have of it.

Definition 4. ***Negation of a proposition***
The negation of a proposition P, denoted $\neg P$ or $\bar{P}$, is the proposition defined by the truth table:

P	$\neg P$
T	F
F	T

In the left-hand column are all the possible truth values of the original proposition P, and on the right the corresponding truth values of $\neg P$. It expresses that $\neg P$ is the proposition which is false when P is true, and true when P is false, i.e. which always has a truth value contrary to that of P.

The qualifier the in the previous text is not insignificant. Truth tables make it possible to completely characterize a proposition. If two propositions P and Q have the same truth tables, they are true at the same time and false at the same time, in other words, they always carry the same truth values. We say that they are **equivalent**. Thus, if Q is a proposition apparently different from $\neg P$ but which has the same truth table as $\neg P$, then it is equivalent to it: by expressing these propositions with their truth tables, one notices that they are in fact the same propositions, in the sense that their tables are the same, hence the qualifier the .

Definition 5. ***Equivalence of two propositions***
Two propositions P and Q are said to be ***equivalent*** *when they have the same truth values. We then write $P \Leftrightarrow Q$, and thus we have P if and only if we have Q. In a truth table displaying P and Q, their two columns are therefore the same.*

Let us give ourselves a simple example of negation. For real x, the negation of the proposition $(x > 1)$ is $(x \leq 1)$ because when the proposition $(x > 1)$ is true, $(x \leq 1)$ is false, and when $(x > 1)$ is false, $(x \leq 1)$ is true: one indeed retrieves the truth table of definition 4. But it is also $(x - 1 \leq 0)$, or even $(\frac{e^x}{e} \leq 1)$, since all these propositions are equivalent to $(x \leq 1)$.

Let us now give ourselves a more elaborate example of the negation of a proposition.

Consider the proposition:

P: There exists a prime number between every natural integer and its double

This proposition is a theorem, called Bertrand's postulate, formulated by the French mathematician Joseph Bertrand (1822 – 1900), first proved by Pafnuty Chebyshev (1821 – 1894) in 1850. We would like to write P in mathematical language, so we need to translate this there exists .

Definition 6. ***Existential quantifier***
*The symbol $\exists$, called the **existential quantifier**, is read there exists .*

By convention denoting $\mathbb{P}$ the set of prime numbers, we then have:

$$\forall n \in \mathbb{N}, \exists p \in \mathbb{P}, n \leq p \leq 2n$$

How to express $\neg P$? We glimpsed through the example of definition 2 that the concept of **counter-example** is intimately tied to the negation of a proposition beginning with for all . Indeed, Bertrand's postulate is false only if one manages to exhibit a natural integer n such that no prime number lies between n and $2n$, i.e. such that for every prime p, p is not between n and $2n$.

We thus obtain in English:

$\neg P$: There exists a natural integer n such that for every prime number p, p is strictly less than n or p is strictly greater than $2n$.

One will roughly retain that the negation of a "for all" is a "there exists" .

Let us finish with two simple propositions, one of which shows how to use truth tables to prove equivalences.

Proposition 1. ***Double negation***
If P is a proposition,

$$P \Leftrightarrow \neg(\neg P)$$

Proof. It suffices to draw up the truth table:

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

The columns of the truth values of P and of $\neg(\neg P)$ are the same: the propositions are therefore equivalent. □

Proposition 2. *If P and Q are two propositions, P and Q are equivalent if and only if their negations are so.*

Proof. P and Q are equivalent if and only if they have the same truth values, which means that their negations also have the same truth values, since it suffices to change the T into F in the truth table to obtain them. □

3.3 The logical and and the logical or

Definition 7. ***The logical and***
If P, Q are two propositions, we define the proposition $P \wedge Q$ (to be read P and Q) by the truth table:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

As one may expect, $P \wedge Q$ is true only if P and Q are both true, and is false in all other cases.

Definition 8. ***The logical or***
If P, Q are two propositions, we define the proposition $P \vee Q$ (to be read P or Q) by the truth table:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

As one may expect, $P \vee Q$ is true if at least one of the two propositions P or Q is true, and false if both are false.

The or and the and are commutative, which means that for any propositions P, Q, $P \vee Q \Leftrightarrow Q \vee P$ and $P \wedge Q \Leftrightarrow Q \wedge P$.

Proposition 3. ***De Morgan's Laws***
If P and Q are two propositions, then:

$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$$

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$$

Proof. Let us prove the first equivalence, the second is left as an exercise to the reader (it is exactly the same principle). We already know the truth table of the logical and :

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

as well as that of negation:

H	$\neg H$
T	F
F	T

We then combine them to obtain the following table:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

Likewise, we already know the truth table of the logical or :

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

which we combine with the table of negation to obtain:

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

We notice that the columns of the truth values of $\neg P \vee \neg Q$ and $\neg(P \wedge Q)$ are the same: the two propositions are therefore equivalent! □

One will retain that the negation of an or is the and of the negations, and the negation of an and is the or of the negations.

If we take again the example of Bertrand's postulate and seek to negate the proposition $(n \leq p \leq 2n)$, it is worth noting that: $(n \leq p \leq 2n) \Leftrightarrow (n \leq p) \wedge (p \leq 2n)$. We then apply the first De Morgan's law to obtain:

$$\begin{aligned} \neg(n \leq p \leq 2n) &\Leftrightarrow \neg(n \leq p) \vee \neg(p \leq 2n) \\ &\Leftrightarrow (n > p) \vee (p > 2n) \end{aligned}$$

We are then able to write the negation of Bertrand's postulate in mathematical language:

$$\exists n \in \mathbb{N}, \forall p \in \mathbb{P}, (n > p) \vee (p > 2n)$$

Proposition 4. ***Associativity of the or and of the and***
If P, Q and R are three propositions,

$$(P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$$

$$(P \wedge (Q \wedge R)) \Leftrightarrow ((P \wedge Q) \wedge R)$$

We then write $P \vee Q \vee R$ and $P \wedge Q \wedge R$ for these propositions, without worrying about parentheses.

Proof. For the first proposition, as is our habit we draw up the truth tables:

P	Q	R	$P \vee Q$	$Q \vee R$	$(P \vee Q) \vee R$	$P \vee (Q \vee R)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
F	T	T	T	T	T	T
T	F	F	T	F	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

The last two columns are the same, therefore the propositions are equivalent.
Thus, for **all** propositions P, Q, R:

$$(P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$$

To show the second proposition, we take three propositions P, Q and R and apply what we have just shown to $\neg P$, $\neg Q$ and $\neg R$ (we can do so since the result is valid for every triplet of propositions). We obtain:

$$(\neg P \vee (\neg Q \vee \neg R)) \Leftrightarrow ((\neg P \vee \neg Q) \vee \neg R)$$

It remains to take the negation of these propositions and use proposition 2 of the course to obtain:

$$(P \wedge (Q \wedge R)) \Leftrightarrow ((P \wedge Q) \wedge R)$$

and this regardless of the chosen triplet of propositions P, Q, R. □

3.4 Implication of two propositions

Definition 9. ***Implication of two propositions***
If P and Q are two propositions, we define the implication of P and Q, denoted $P \implies Q$, as the proposition defined by the truth table:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

As one may expect, the true can only imply the true . Line 3 may surprise, but it seems less strange when considered together with the last line: in fact the false can imply anything.

To the implications of propositions are tied the central concepts of necessary condition, sufficient condition, and necessary and sufficient condition. Let P and Q be two propositions such that $P \implies Q$ is true.

Q is called a **necessary condition** for the realization of P, because if Q were not true, then P would necessarily be false, since if P were true, Q would also be so, because $P \implies Q$ is true.

P is called a **sufficient condition** for the realization of Q, because it suffices that P be true for Q to be true.

If one has in addition the **reciprocal proposition** $Q \implies P$, then we have $P \Leftrightarrow Q$ (see below proposition 6), and the realization of Q is a **necessary and sufficient condition** for the realization of P.

Proposition 5. *If P and Q are two propositions, we have:*

$$(P \implies Q) \Leftrightarrow \neg P \vee Q$$

$$\neg(P \implies Q) \Leftrightarrow P \wedge (\neg Q)$$

Proof. As you will have guessed, we draw up the truth tables:

P	Q	$\neg P$	$\neg P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

We notice that the columns of the truth values of $\neg P \vee Q$ and of $(P \implies Q)$ are the same: the two propositions are therefore equivalent.

For the second equivalence, one can draw up the truth tables (we encourage the reader to do so), but one can also notice that from proposition 2 and from what we have just shown:

$$\neg(P \implies Q) \Leftrightarrow \neg(\neg P \vee Q)$$

Now by proposition 3:

$$\neg(\neg P \vee Q) \Leftrightarrow \neg(\neg P) \wedge \neg Q \Leftrightarrow P \wedge (\neg Q)$$

□

Let us note that these equivalences are logical : for the second for example, if the fact that P being true automatically implies that Q is true, the opposite would mean that P is true without Q being so.

All these equivalences provide sometimes simpler ways of proving an implication. We will list the different means of reasoning at the end of the course, but before that let us give a few more **really important** results.

Proposition 6. ***Contraposition***
If P and Q are two propositions:

$$(P \implies Q) \Leftrightarrow (\neg Q \implies \neg P)$$

Proof. With proposition 4:

$$(P \implies Q) \Leftrightarrow \neg P \vee Q \Leftrightarrow \neg P \vee \neg(\neg Q) \Leftrightarrow \neg(\neg Q) \vee \neg P \Leftrightarrow (\neg Q \implies \neg P)$$

The last equivalence coming from the first equivalence of proposition 4 by replacing P with $\neg Q$ and Q with $\neg P$. ☐

Proving $\neg Q \implies \neg P$ when one wants to prove $P \implies Q$ is called **reasoning by contraposition (or by the contrapositive)** (see exercises!).

Proposition 7. ***Double implication***
If P and Q are propositions:

$$(P \Leftrightarrow Q) \Leftrightarrow ((P \implies Q) \wedge (Q \implies P))$$

Proof. We draw up the truth table:

P	Q	$P \Leftrightarrow Q$	$P \implies Q$	$Q \implies P$	$((P \implies Q) \wedge (Q \implies P))$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

We notice that the columns of the truth values of $P \Leftrightarrow Q$ and of $(P \implies Q) \wedge (Q \implies P)$ are the same: the two propositions are therefore equivalent. ☐

This equivalence provides a new way of proving an equivalence! Sometimes (and even often) it is difficult to prove $P \Leftrightarrow Q$ by a chain of equivalences, for example when it is a matter of solving somewhat elaborate equations. One often prefers to reason by **double implication**, that is, to prove $P \implies Q$ and $Q \implies P$, and this by the method of one's choice, for example by contraposition or by using the first equivalence of proposition 4: the possibilities are numerous!

For example, over $\mathbb{N}$, $(2 \mid n) \wedge (3 \mid n) \Leftrightarrow (6 \mid n)$. Indeed, if $2 \mid n$ and $3 \mid n$, then since 2 and 3 are coprime, a corollary of Gauss's theorem gives that $2 \times 3 = 6$ divides n: we have proved the direct implication.
If $6 \mid n$, then since 2 and 3 divide it, we indeed have $2 \mid n$ and $3 \mid n$: we have proved the reciprocal implication, which proves the announced proposition.

Proposition 8. ***Distributivity of and (resp. of or) over or (resp. over and)***
If P, Q and R are three propositions, then:

$$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$$

$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$$

Proof. We draw up the truth tables:

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
F	T	T	T	F	F	F	F
T	F	F	F	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

This first table proves the first equivalence (columns 5 and 8 are the same).

Onwards for the second:

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

This one proves the second equivalence for the same reason. □

4 Inventory of methods of reasoning

Fortunately, in practice one does not draw up a truth table when it is a matter of proving a statement. We will now present the different methods, accompanied by an example that we invite the reader to attempt beforehand.

4.1 Reasoning by contradiction

To show that a proposition P is true, one may suppose that it is false and try to arrive at an absurdity, that is to say at the negation of a proposition which we know to be true. For such reasoning to work, it is necessary that the fact of denying P bring us something with which we can work. For example, denying a proposition of the form $\forall x, P(x)$ (where $P(x)$ is a proposition qualifying x, this is called a *predicate* of x) gives us the existence of an x such that $\neg P(x)$, with which we may perhaps work to exhibit an absurdity.

Indeed, reasoning by contradiction consists in showing that $\neg P \implies (Q \wedge \neg Q)$ for some proposition Q. This is equivalent to $(\neg Q \vee Q) \implies P$ (contraposition), and since $\neg Q \vee Q$ is always true (this is called a *tautology*), we conclude that P is true.

One of the most famous reasonings by contradiction appears in the proof of the irrationality of $\sqrt{2}$, which according to legend cost its author Hippasus of Metapontum his life, thrown into the sea by his Pythagorean comrades around 530 BC, so scandalous was the discovery of this irrational number.

Exercise: Show that $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$.

Solution: Suppose that $\sqrt{2} \in \mathbb{Q}$. **Then**, we can write it in irreducible form $\frac{p}{q}$ where thus $\gcd(p, q) = 1$ (reasoning by contradiction is useful here because it brings us this form with which we can work). Then, $p^2 = 2q^2$, so p^2 is even. This implies that p is even, for if it were odd, then p^2 would be also, which is not the case (here is a reasoning worth noticing). We may therefore write p in the form $2k$. But then, we have $2q^2 = p^2 = 4k^2$ and thus $q^2 = 2k^2$: q^2 is even, hence q also. This is absurd, for p and q are supposed to be coprime. We thus deduce that $\sqrt{2}$ is irrational.

4.2 Reasoning by equivalence

To prove a proposition of the form $P \Leftrightarrow Q$, one can start from P (resp. from Q) and try to arrive at Q (resp. at P) by a sequence of **equivalences**. Attention, in all cases it is essential that **all** steps be equivalences, i.e. that one can go back up the reasoning (see first example).

To prove a proposition P, one can also transform it into a proposition that we know to be true with the help of **equivalences**: P will then have the same truth values, i.e. it will be true (see the second example). In practice this is rarely feasible, and when it is not possible, one often employs double implication (see next subsection).

Exercise: Let $n \in \mathbb{N}$. Show that $i^n = 1 \Leftrightarrow 4 \mid n$.

Solution: Knowing that $i = e^{i\frac{\pi}{2}}$, we have:

$$i^n = 1 \Leftrightarrow e^{i\frac{n\pi}{2}} = 1 \Leftrightarrow \exists k \in \mathbb{N},\ n\frac{\pi}{2} = 2k\pi \Leftrightarrow \exists k \in \mathbb{N},\ n = 4k \Leftrightarrow 4 \mid n$$

Exercise: Let x and y be two positive reals. Show that $\frac{x+y}{2} \geq \sqrt{xy}$. This result, called the *arithmetic-geometric inequality*, expresses that the arithmetic mean of two positive numbers is always greater than their geometric mean, defined as the right-hand side of the inequality.

Solution: We reason by equivalence.

$$\frac{x+y}{2} \geq \sqrt{xy} \Leftrightarrow x + y \geq 2\sqrt{xy} \Leftrightarrow x - 2\sqrt{xy} + y \geq 0$$

We then recognize the expanded form of $(\sqrt{x} - \sqrt{y})^2$, which is indeed nonnegative: we deduce that the initial inequality is indeed true.

4.3 Double implication

To show a proposition of the form $P \Leftrightarrow Q$, one can show that $P \implies Q$ and that $Q \implies P$ (in whatever manner one chooses, see below the methods for proving implications). It often happens that one shows $P \implies Q$ and $\neg P \implies \neg Q$.

Exercise: Let a, b, c in $\mathbb{N}$. Show that $(a \mid b) \wedge (a \mid c) \Leftrightarrow (a \mid \gcd(b, c))$.

Solution: Let us denote $d = \gcd(b, c)$.
Suppose that $a \mid d$. Then a divides a divisor of b, hence divides b, and likewise a divides c. We have thus proved the reciprocal direction (in double implications, it is good to begin with the direction that inspires us the most).

Suppose that $a \mid b$ and $a \mid c$. From Bézout's identity,

$$\exists u, v \in \mathbb{Z},\ uc + vb = d$$

Now, $a \mid b$ hence $a \mid vb$, and likewise $a \mid uc$, hence $a \mid uc + vb = d$: we have proved the direct direction, which concludes.

4.4 Contraposition

To prove a proposition of the form $P \implies Q$, one can show that $\neg Q \implies \neg P$.

Exercise: Let $n \in \mathbb{N}$. Show that if n^2 is even, then n is also.

Solution: We reason by contrapositive.
Let us denote P the proposition n^2 is even , and Q the proposition n is even . We want to show $P \implies Q$ by contraposition, in fact by showing that $\neg Q \implies \neg P$. So let us suppose $\neg Q$, namely that n is odd. Then it can be written in the form $2k + 1$. But then,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

is odd. We have thus shown $\neg P$ and completed our reasoning by contraposition.

4.5 Proving a proposition in or

To prove a proposition of the form $P \vee Q$ (this occurs rather seldom in practice), one uses proposition 4 in which one replaces P by $\neg P$ to notice that $P \vee Q \Leftrightarrow (\neg P \implies Q)$. One thus reduces to showing that $\neg P \implies Q$.

Exercise: Let $x \in \left]-\pi; \pi\right[$. Show that $(2|\cos(\frac{x}{2})| \geq 1) \vee (2|\cos(x)| \geq 1)$.

Solution: Suppose $2|\cos(x)| < 1$. From what was said previously, it is then a matter of showing that $2|\cos(\frac{x}{2})| \geq 1$.
Since $2|\cos(x)| \leq 1$ we have $\frac{-1}{2} < \cos(x) < \frac{1}{2}$ and hence $x \in \left]\frac{-2\pi}{3}; \frac{-\pi}{3}\right[\cup \left]\frac{\pi}{3}; \frac{2\pi}{3}\right[$, thus $\frac{x}{2} \in \left]\frac{-\pi}{3}; \frac{-\pi}{6}\right[\cup \left]\frac{\pi}{6}; \frac{\pi}{3}\right[$, therefore $|\cos(\frac{x}{2})| \in \left]\frac{1}{2}; \frac{\sqrt{3}}{2}\right[$ and so $2|\cos(\frac{x}{2})| \geq 1$.

4.6 Reasoning by analysis–synthesis

Reasoning by analysis–synthesis often occurs in exercises of the type: find the x such that $P(x)$ where P is a proposition depending on x. When tackling such an exercise, one does not a priori know these x in question: then comes the phase of **analysis**, where we suppose the existence of such an x, from which we deduce necessary conditions that it must satisfy. Very often, these conditions that x must necessarily satisfy, obtained at the end of the analysis, make it possible to restrict the possible solutions to a small number, which one may then check by hand to see if they indeed satisfy $P(x)$.

The logical scheme is important: we show that **if** x satisfies $P(x)$, **then** it satisfies conditions such that it can only take certain values : but **this is not an equivalence**! Some of the possible values of x obtained at the end of the analysis may not satisfy $P(x)$, so it is necessary to **check** that conversely these values do fit, this is the step of **synthesis**: we then indeed have an equivalence and we have thus determined all the x satisfying $P(x)$.

Let us show, as an example, that if f is a function from $\mathbb{R}$ to $\mathbb{R}$, then it can be written **uniquely** as a sum of an odd function i and an even function p.

A priori, we do not know where to find these functions i and p: we are therefore going to reason by analysis–synthesis.

Analysis: Suppose that f can be written $p+i$ with p even and i odd. Then on the one hand:

$$\forall x \in \mathbb{R},\ f(x) = p(x) + i(x)$$

and on the other hand:

$$\forall x \in \mathbb{R},\ f(-x) = p(-x) + i(-x) = p(x) - i(x)$$

Adding these two relations we obtain:

$$\forall x \in \mathbb{R},\ 2p(x) = f(x) + f(-x)$$

that is,

$$\forall x \in \mathbb{R},\ p(x) = \frac{f(x) + f(-x)}{2}$$

In the same way, by subtracting the two relations we obtain:

$$\forall x \in \mathbb{R},\ i(x) = \frac{f(x) - f(-x)}{2}$$

Thus, if p and i exist, they are necessarily these two functions: p and i are unique provided that the functions highlighted are suitable, let us check this in the synthesis.

Synthesis: Let $p : x \mapsto \frac{f(x)+f(-x)}{2}$ and $i : x \mapsto \frac{f(x)-f(-x)}{2}$. First:

$$\forall x \in \mathbb{R},\ p(-x) = \frac{f(-x) + f(-(-x))}{2} = \frac{f(-x) + f(x)}{2} = p(x)$$

so p is even.

Likewise:

$$\forall x \in \mathbb{R},\ i(-x) = \frac{f(-x) - f(x)}{2} = -\frac{f(x) - f(-x)}{2} = -i(x)$$

so i is odd.

Finally:

$$\forall x \in \mathbb{R},\ p(x) + i(x) = \frac{f(x) + f(-x) + f(x) - f(-x)}{2} = f(x)$$

so indeed we have $f = p + i$: p and i are suitable.

Thus, such functions p and i exist according to the synthesis, and are unique according to the analysis, which concludes.

4.7 Reasoning by induction

The principle of induction is stated as follows:

Proposition 9. ***The principle of induction***
Let P_n be a proposition depending on n. If P_0 is true and if $\forall n \in \mathbb{N},\ P_n \implies P_{n+1}$ then P_n is true for all $n \in \mathbb{N}$.

In practice, to show by induction that a proposition P_n is true for every n, one begins by showing that it is true for $n = 0$ (this is **the initialization**). Then one shows that the property is **hereditary** by proving that if P_n is true for some integer n, then P_{n+1} is also true.
Thus, the principle of induction will make it possible to conclude that P_n is true for all n.

Attention: P_n is a predicate of n, that is, a proposition qualifying n; it must therefore not begin with $\forall n$ since it applies only to n alone.

Let us see an example. We give here the standard write-up of an induction proof.
We establish for $n \in \mathbb{N}$ the property P_n:

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

which we will prove by induction.

For $n = 0$:

$$\sum_{k=0}^{0} k = 0 = \frac{0 \times (0+1)}{2} = 0$$

thus P_0 is true.

Suppose P_n true for some integer n. By the induction hypothesis:

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

and therefore:

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

Thus, if P_n is true then P_{n+1} is also.
The principle of induction makes it possible to conclude that the property is true for all $n \in \mathbb{N}$.

If some see the first traces of reasoning by induction in Euclid's *Elements* (around 300 BC), the first usage resembling the one we make of it is due to Blaise Pascal (1623 – 1662) who wrote it in 1654 in his *Treatise on the Arithmetic Triangle*.

As seen in exercise 49, it may happen that a property is hereditary only from a certain rank n_0. Fortunately, reasoning by induction is applicable by initializing at n_0, as shown by the following proposition.

Proposition 10. ***Induction from a certain rank***
Let P_n be a predicate of n. If $\exists n_0 \in \mathbb{N}$, P_{n_0} is true and $\forall n \geq n_0,\ P_n \implies P_{n+1}$ then $\forall n \geq n_0,\ P_n$ is true.

Proof. It suffices to apply the principle of induction to $Q_n = P_{n+n_0}$. $\square$

For example, we would like to compare n^2 and 2^n. After computing the first values, we notice that $n^2 > 2^n$ for $n \in \{1, 2, 3\}$ but that for $n \geq 4$, 2^n seems to be greater than n^2. We will show that this is indeed the case, by induction, but we will initialize at 4.

We establish for $n \geq 4$ the property P_n: $2^n \geq n^2$.
$2^4 = 16 \geq 4^2 = 16$: P_4 is true.
Suppose P_n for $n \geq 4$ given. Then,

$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1$$

by the induction hypothesis. Now, still by the induction hypothesis,

$$2^n \geq n^2$$

and $n^2 \geq 2n+1$ for $n \geq 4$ (study $x \mapsto x^2 - 2x - 1$), so $2^n \geq 2n+1$, whence:

$$(n+1)^2 \leq 2^n + 2^n = 2^{n+1}$$

Thus, P_{n+1} is true.
By the principle of induction, $\forall n \geq 4,\ 2^n \geq n^2$.

However, inductions may also be finite , as shown by the following proposition:

Proposition 11. ***Finite induction***
Let $n \leq m$ and let P be a predicate defined on $[\![n, m]\!]$. If P_n is true and:

$$\forall k \in [\![n, m-1]\!],\ (P_k \implies P_{k+1})$$

then $\forall k \in [\![n, m]\!],\ P_k$ is true.

Proof. See exercise 40! □

As an example, let us fix $n \in \mathbb{N}^*$ and prove the property P_k defined for $k \in [\![1, n]\!]$ by:

$$\left(1 + \frac{1}{n}\right)^k \leq 1 + \frac{k}{n} + \frac{k^2}{n^2}$$

We have $1 + \frac{1}{n} \leq 1 + \frac{1}{n} + \frac{1}{n^2}$, whence P_1.
Suppose P_k for $k \in [\![1, n-1]\!]$ given. Then:

$$\left(1 + \frac{1}{n}\right)^{k+1} = \left(1 + \frac{1}{n}\right)\left(1 + \frac{k}{n}\right)^k \leq \left(1 + \frac{1}{n}\right)\left(1 + \frac{k}{n} + \frac{k^2}{n^2}\right)$$

$$= 1 + \frac{k+1}{n} + \frac{1}{n^2}\left(k^2 + k + \frac{k}{n}\right)$$

Now, $n \geq 1$ hence $1 + \frac{1}{n} \leq 2$, so $k^2 + \left(1 + \frac{1}{n}\right)k \leq k^2 + 2k \leq k^2 + 2k + 1 = (k+1)^2$, hence:

$$\left(1 + \frac{1}{n}\right)^{k+1} \leq 1 + \frac{k+1}{n} + \frac{(k+1)^2}{n^2}$$

whence P_{k+1}.
Thus, by the principle of (finite) induction,

$$\forall k \in [\![1, n]\!],\ \left(1 + \frac{1}{n}\right)^k \leq 1 + \frac{k}{n} + \frac{k^2}{n^2}$$

Let us now state an other principle of induction well known. In reality, there is only one principle of induction (the first one we introduced) and all the others follow from it.

Proposition 12. ***Double induction***
Let P_n be a predicate of n. If P_0 and P_1 are true and if $\forall n \in \mathbb{N},\ (P_n \wedge P_{n+1}) \implies P_{n+2}$ then P_n is true for all $n \in \mathbb{N}$.

Proof. It suffices to apply the principle of induction to $Q_n = (P_n \wedge P_{n+1})$. □

Of course, one may replace 0 and 1 by some $n_0 \in \mathbb{N}$ and n_0+1 in virtue of proposition 10. Likewise, one may imagine triple induction, quadruple induction, etc.

As an example, let us present the illustrious Fibonacci sequence, named after the Italian mathematician of the 12th century Leonardo Fibonacci, who presented it in his work *Liber abaci* to model a population of rabbits.

We consider the sequence defined by $F_0 = 0$, $F_1 = 1$ and $\forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n$. We set $\alpha = \frac{1+\sqrt{5}}{2}$ (α is commonly denoted φ and is called the golden ratio) and $\beta = \frac{1-\sqrt{5}}{2}$. By noticing that these two numbers are roots of $X^2 - X - 1$, let us show by (double) induction the property P_n: $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$.

(To notice that α and β satisfy the equation $x^2 - x - 1 = 0$, we used the fact that if x and y are two reals, then they are roots of $X^2 - (x+y)X + xy$: we simply replaced x by α and y by β).

$F_0 = 0 = \frac{\alpha^0 - \beta^0}{\sqrt{5}}$, hence P_0.
$\frac{\alpha - \beta}{\sqrt{5}} = 1 = F_1$, hence P_1.
Suppose P_n and P_{n+1} for some $n \in \mathbb{N}$ given.
Then:

$$F_{n+2} = F_{n+1} + F_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} + \frac{\alpha^n - \beta^n}{\sqrt{5}}$$
$$= \frac{\alpha^{n+1} + \alpha^n - (\beta^{n+1} + \beta^n)}{\sqrt{5}}$$

Now, $\alpha^2 = \alpha + 1$, so by multiplying by α^n for $n \in \mathbb{N}$, $\alpha^{n+1} + \alpha^n = \alpha^{n+2}$, and likewise for β, hence:

$$F_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\sqrt{5}}$$

and thus P_{n+2} is true.
By the principle of (double) induction, the property is true at every order.

Let us now present another frequently used principle of induction.

Proposition 13. ***Strong induction***
Let P_n be a predicate of n. Suppose that P_0 is true and that:

$$\forall n \in \mathbb{N},\ (P_0 \wedge \cdots \wedge P_n \implies P_{n+1})$$

Then P_n is true for all $n \in \mathbb{N}$.

Proof. It suffices to apply the principle of induction to $Q_n = P_0 \wedge \cdots \wedge P_n$. □

Of course, one can replace 0 by some arbitrary $n_0 \in \mathbb{N}$.

As an example, let us show the property P_n established for $n \geq 2$: n can be written as a product of prime numbers.
2 being prime, it is indeed a product of prime numbers, hence P_2.
Suppose $P_2, \ldots, P_n$ for some $n \geq 2$ given.

If $n+1$ is prime, it is a product of prime numbers.

Otherwise, it admits a divisor $k \in [\![2, n]\!]$, let $k' = \frac{n+1}{k}$, we then also have $k' \in [\![2, n]\!]$. We may apply P_k and $P_{k'}$: k and k' can be written as products of prime numbers, and since $n+1 = kk'$, the same holds for $n+1$, whence P_{n+1}.

Thus, by the principle of (strong) induction, every integer greater than 2 can be written as a product of prime numbers.
We invite the reader to use his/her knowledge of integer arithmetic to show that such a decomposition is unique up to the order of the factors.

All the examples seen up to now present ascending inductions where one deduces the truth of P_{n+1} from the truth of earlier propositions. Let us now present the principle of descending induction .

Proposition 14. ***Finite descending induction***
Let $n \leq m$ and P a predicate defined on $[\![n, m]\!]$. If P_m is true and if:

$$\forall k \in [\![n+1, m]\!],\ P_k \implies P_{k-1}$$

then P_k is true for every $k \in [\![n, m]\!]$.

Proof. We reason by contradiction by supposing that $\{i \in [\![n, m]\!],\ \neg P_i\}$ is nonempty: since this set is bounded above, it admits a greatest element denoted i_0. Then, $i_0 < m$ because P_m is true. Consequently, $i_0 + 1 \in [\![n+1, m]\!]$, and since $i_0 + 1 > i_0$, by maximality of i_0, P_{i_0+1} is necessarily true. But then, since $P_{i_0+1} \implies P_{i_0}$, P_{i_0} is true: this is absurd.
Thus, $\forall k \in [\![n, m]\!],\ P_k$ is true. □

For an example of application of this type of induction, see exercise 42.

Let us now give way to the exercises, the playground of the mathematician in which he or she fully employs his/her relentless logic. These small or large problems are necessary, and it is not I who say so, it is the brilliant André Weil!

If logic is the hygiene of the mathematician, it is not it which provides him his food; the daily bread on which he lives, these are the great problems
André Weil, 1906 – 1998

5 Exercises:

The difficulty of the exercises is indicated by a number between 1 and 5. If there are prerequisites, they will be stated.

5.1 Truth tables and logic

Exercise 1: (1)
We define the *exclusive or*, denoted XOR, by the fact that for any propositions P and Q, P XOR Q is true only if exactly one of P, Q is true. This operator is notably used in cryptography and in electronics, for example.

Construct its truth table, then show that:

$$(P \text{ XOR } Q) \Leftrightarrow ((P \vee Q) \wedge (\neg P \vee \neg Q)) \Leftrightarrow ((P \wedge \neg Q) \vee (\neg P \wedge Q))$$

The first expression is a *conjunctive normal form* of XOR: a conjunctive normal form is an expression of the form $(P_{1,1} \vee \cdots \vee P_{1,k_1}) \wedge (P_{2,1} \vee \cdots \vee P_{2,k_2}) \wedge \cdots \wedge (P_{l,1} \vee \cdots \vee P_{l,k_l})$.
The second expression is a *disjunctive normal form* of XOR: a disjunctive normal form is an expression of the form $(P_{1,1} \wedge \cdots \wedge P_{1,k_1}) \vee (P_{2,1} \wedge \cdots \wedge P_{2,k_2}) \vee \cdots \vee (P_{l,1} \wedge \cdots \wedge P_{l,k_l})$.

Each P_{j,k_i} is called a *literal*. These forms allow one to determine easily the *satisfiability* of a proposition, i.e. whether there exists an assignment of truth values to the P_{j,k_i} that makes the proposition true. For example, if P and Q are true and R is false, then the formula $(P \wedge Q) \vee R$ in disjunctive normal form is satisfied (true). The interested reader may consult the *SAT problem*, a central problem in computer science.

Exercise 2: (2)
Show the following equivalences for all propositions P, Q, and R:
a) $(P \wedge Q) \Leftrightarrow (\neg(\neg P \vee \neg Q))$
b) $(P \vee Q) \Leftrightarrow (\neg(\neg P \wedge \neg Q))$
c) $(P \wedge (P \implies Q)) \Leftrightarrow (P \wedge Q)$ (deductive reasoning)
d) $\neg P \Leftrightarrow (\neg(P \vee Q) \vee (\neg P \wedge Q))$
e) $(P \implies Q) \Leftrightarrow (\neg P \vee (P \wedge Q))$
f) $(P \implies (Q \wedge R)) \Leftrightarrow ((P \implies Q) \wedge (P \implies R))$
g) $((P \wedge Q) \implies R) \Leftrightarrow (P \implies (Q \implies R))$

Exercise 3: (1)
(Prerequisite: sequences for questions b), c), f)).
Write the following propositions in mathematical language (f is a function from $\mathbb{R}$ to $\mathbb{R}$):
a) Every even number greater than 4 is the sum of two prime numbers.
(This proposition, formulated around 1740 by the Prussian mathematician Christian Goldbach (1690–1764), is known as *Goldbach's conjecture*. It is still unproven! It has been verified for even numbers up to 4×10^8, strongly suggesting it is true, but the community still awaits a proof.)
b) (u_n) is increasing.
c) (u_n) is bounded.
d) The function f is constant.

e) Every real number is the limit of a sequence of rationals (i.e. $\mathbb{Q}$ is *dense* in $\mathbb{R}$).
If E is a set, the set of sequences with values in E is denoted $E^{\mathbb{N}}$.
f) (u_n) is periodic.
g) The function f is periodic.
h) The function f is strictly decreasing.

Exercise 4: (2)
Negate the previous propositions.

Exercise 5: (2)
Let $f : \mathbb{R} \to \mathbb{R}$ be a function.
State each of the following propositions in plain language. Can one find a function that satisfies it? One that does not?
a) $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ f(x) < f(y)$
b) $\forall x \in \mathbb{R},\ \exists T \in \mathbb{R}^*,\ f(x) = f(x+T)$
c) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ y = f(x)$

5.2 Proof by contradiction

Exercise 6: (1)
Let $a, b \in \mathbb{Q}$. Show that if $a + b\sqrt{2} = 0$ then $a = b = 0$. Deduce that if a, b, c, d are rationals, then:

$$(a + b\sqrt{2} = c + d\sqrt{2}) \implies ((a = c) \wedge (b = d))$$

The first result can be expressed by saying that $(1, \sqrt{2})$ is $\mathbb{Q}$-linearly independent. To make these terms precise, one needs the notions of *vector space* and *field*. Patience! For $\mathbb{R}$ over $\mathbb{Q}$, a family $(x_0, \ldots, x_n)$ of reals is said to be $\mathbb{Q}$-linearly independent if:

$$\forall q_0, \ldots, q_n \in \mathbb{Q},\ (q_1 x_1 + \cdots + q_n x_n = 0) \implies (q_1 = \cdots = q_n = 0)$$

Exercise 7: (1–2 for the second part)
Show that if one puts $n+1$ socks into n drawers, then at least one drawer contains at least 2 socks. As an application, deduce that if $x_0 < \cdots < x_n$ are $n+1$ reals in $[0,1]$, then $\exists i \in [\![0, n-1]\!]$ such that $|x_i - x_{i+1}| \leq \frac{1}{n}$.

This principle, called the *Pigeonhole Principle* (or Dirichlet's drawer principle), has many applications, notably in approximating reals by rationals (see Dirichlet's approximation theorem).

Exercise 8: (2)
Show that if $n \in \mathbb{N}^*$, then $\sqrt{n^2+1} \notin \mathbb{N}$.

Exercise 9: (2)
(Prerequisite for the second part: the Fundamental Theorem of Arithmetic, which states that every integer factors uniquely into prime numbers, up to order.)
Show that $\frac{\ln(3)}{\ln(2)} \notin \mathbb{Q}$. Generalize by replacing 2 and 3 with two distinct prime numbers p and q.

Exercise 10: (2)
Show that exp is not a polynomial.

Exercise 11: (3)
Show that $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Exercise 12: (4)
(Prerequisite: congruences for the second part.)
Show that there are infinitely many prime numbers, and show that there are infinitely many primes congruent to 3 modulo 4 (i.e. of the form $4k + 3$, with $k \in \mathbb{N}$).

This is a special case of Dirichlet's *arithmetic progression theorem* (Peter Gustav Lejeune-Dirichlet, 1805–1859), proved in 1837 using complex analysis tools, thus creating analytic number theory. The theorem states that if a and b are coprime natural numbers, then there are infinitely many primes of the form $ak + b$ with $k \in \mathbb{N}$.

5.3 Reasoning by contraposition

Exercise 13: (1)
Let $n \in \mathbb{N}$. Show that if $n^2 + 1$ is even then n is odd.

Exercise 14: (2)
(Prerequisite: definition of the limit of a sequence.)
Let (u_n) be a sequence of positive reals converging to a limit l. Show that $l \geq 0$.

In topology, a subset $E \subset F$ is called *closed in F* if for any sequence with values in E that converges in F, its limit is also in E. The exercise above shows that $\mathbb{R}^+$ is closed in $\mathbb{R}$. On the other hand, $\mathbb{R}^{+*}$ is not, since $(\frac{1}{n+1})$ is strictly positive but converges to $0 \notin \mathbb{R}^{+*}$.

Exercise 15: (2)
(Prerequisite: modular congruences.)
Let $x, y \in \mathbb{Z}$. Show that:

$$((7 \nmid x) \vee (7 \nmid y)) \implies (7 \nmid x^2 + y^2)$$

Exercise 16: (3)
Let $n \in \mathbb{N}$. Show that:

$$(8 \nmid n^2 - 1) \implies (2|n)$$

Exercise 17: (3)
Show that if $2^n - 1$ is prime, then n is prime.

Numbers of the form $2^n - 1$ are called *Mersenne numbers*, after the French mathematician Marin Mersenne (1588–1648). In 1732, Leonhard Euler showed that the converse is false: $2^{11} - 1 = 2047 = 23 \times 89$ is not prime although 11 is. In 1878, Édouard Lucas devised a primality test (later refined by Derrick Lehmer in 1930) for $2^n - 1$, which has been used to find very large primes — essential in cryptography (RSA encryption relies on the difficulty of prime factorization).

5.4 Reasoning by analysis–synthesis / Determination of necessary conditions

Exercise 18: (1)
Solve for $x \in \mathbb{R}$ the equation: $\sqrt{2x+1} = \sqrt{x-3}$.

Exercise 19: (2)
(Prerequisite: primitive/antiderivative.)
Find all differentiable functions $f : \mathbb{R} \to \mathbb{R}$ satisfying:

$$\forall x, y \in \mathbb{R},\ f(x+y) = f(x) + f(y)$$

Exercise 20: (2)
(Prerequisite: standard primitives/antiderivatives.)
Find all differentiable functions $f : \mathbb{R}^{+*} \to \mathbb{R}$ such that:

$$\forall x, y \in \mathbb{R}^{+*},\ f(xy) = f(x) + f(y)$$

Exercise 21: (2)
Find all $f : \mathbb{R} \to \mathbb{R}$ such that:

$$\forall x, y \in \mathbb{R},\ f(y - f(x)) = 2 - x - y$$

Exercise 22: (2)
Find all $f : \mathbb{R} \to \mathbb{R}$ such that:

$$\forall x, y \in \mathbb{R},\ f(xy) = xf(x) + yf(y)$$

Exercise 23: (3)
Find all $f : \mathbb{R} \to \mathbb{R}$ such that:

$$\forall x \in \mathbb{R},\ f(x) + xf(1-x) = 1 + x$$

Exercise 24: (3)
Find all $f : \mathbb{R} \to \mathbb{R}$ such that:

$$\forall x, y \in \mathbb{R},\ 2f(x) + x + f(f(y) - x) = y$$

Exercise 25: (4)
(Prerequisite: Gauss' lemma — if a, b, c are integers with $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.)
Let $P(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial with integer coefficients, $\deg P = n \geq 1$.
Find a necessary condition on $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ for $\frac{p}{q}$ to be a root of P.
Application: Show that for $n \in \mathbb{N}$, $\sqrt{n}$ is rational if and only if n is a perfect square.

Exercise 26: (5)
(Prerequisite: simple induction; density of $\mathbb{Q}$ in $\mathbb{R}$.)
Find all continuous $f : \mathbb{R} \to \mathbb{R}$ such that:

$$\forall x, y \in \mathbb{R},\ f(x + y) = f(x) + f(y)$$

Hint: Start by proving $\forall n \in \mathbb{N}, f(n) = nf(1)$, then extend to $\mathbb{Z}$, then to $\mathbb{Q}$, and finally to $\mathbb{R}$ using density of $\mathbb{Q}$ in $\mathbb{R}$.

This is known as the *Cauchy functional equation*, named after the French mathematician Augustin-Louis Cauchy (1789–1857). It is one of the simplest functional equations, and many others reduce to it (e.g. see Exercise 20).

5.5 Reasoning by induction

5.5.1 Simple induction

Exercise 27: (1)
Let (u_n) be a sequence with $u_0 \in \mathbb{R}$ and $\forall n \in \mathbb{N},\ u_{n+1} = u_n + r$ where r is a fixed real.

Show that $\forall n \in \mathbb{N},\ u_n = u_0 + nr$.

Such a sequence is called an *arithmetic sequence*, with *common difference* r.

Exercise 28: (1)
Let (u_n) be a sequence with $u_0 \in \mathbb{R}$ and $\forall n \in \mathbb{N},\ u_{n+1} = qu_n$ where q is a fixed real.
Show that $\forall n \in \mathbb{N},\ u_n = q^n u_0$.

Such a sequence is called a *geometric sequence*, with *common ratio* q.

Exercise 29: (2)
(This exercise does not use induction, but explains how to find the general term of an arithmetico–geometric sequence.)
Let $a \in \mathbb{R} \setminus \{1\}$ and $b \in \mathbb{R}$. Let (u_n) be defined by $u_0 \in \mathbb{R}$ and $\forall n \in \mathbb{N},\ u_{n+1} = au_n + b$.
Solve $x = ax + b$ for x; denote the solution by l.
Show that $(u_n - l)$ is geometric, then express u_n in terms of a, b, u_0.

This shows an important idea: if (u_n) is defined by $u_{n+1} = f(u_n)$ with f continuous, it is useful to know the *fixed points* of f (solutions of $f(x) = x$). In the arithmetico–geometric case above, l is a fixed point of $f : x \mapsto ax + b$. Moreover, if (u_n) converges to x, then also (u_{n+1}), and by continuity $\lim f(u_n) = f(x)$, hence $x = f(x)$: the limit must be a fixed point. This is a central theme in the study of *dynamical systems*.

Exercise 30: (2)
Let $f : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function.
Show that $\forall n \in \mathbb{N}, f(n) \geq n$.

Such functions appear when studying sequences: they are called *extractors*. If (u_n) is a sequence and f is such a function, then $(u_{f(n)})$ is a *subsequence*. For example, with $f(n) = 2n$ and $(u_n) = (1, \frac{1}{2}, \frac{1}{3}, \dots)$, the subsequence is $(u_{f(n)}) = (1, \frac{1}{3}, \frac{1}{5}, \dots)$.

A powerful result is the *Bolzano–Weierstrass theorem* (Bolzano 1781–1848, Weierstrass 1815–1897): any bounded sequence of reals has a convergent subsequence. For instance, $(u_n) = ((-1)^n)$ is bounded, and the subsequence (u_{2n}) is convergent (constant equal to 1). For $(\sin n)$, this result is much less obvious.

Exercise 31: (2)
Show that:

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

and also:

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

There is a general formula for

$$\sum_{k=0}^{n-1} k^m$$

where $m \in \mathbb{N}$ and $n \in \mathbb{N}^*$. It involves the fascinating Bernoulli numbers B_n (Jakob Bernoulli, 1654–1705), defined by $B_0 = 1$ and:

$$\forall n \in \mathbb{N}^*,\ B_n = \frac{-1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k.$$

In Exercise 50 we will show:

$$\sum_{k=0}^{n-1} k^m = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k\, n^{m+1-k}.$$

These numbers have deep properties and appear, for instance, in the values of the Riemann zeta function at even integers:

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x},$$

when this series converges. They also arise in the power series expansion of $\tan x$, which for small x gives:

$$\tan(x) = \sum_{n=1}^{\infty} \frac{|B_{2n}|\, 2^{2n}\, (2^{2n}-1)}{(2n)!}\, x^{2n-1}.$$

They appear in algebra as well — in short, these numbers are wonderful and full of mysteries.

Exercise 32: (2)
Define a sequence (u_n) by $u_0 \in \mathbb{R}$ and, for all $n \in \mathbb{N}$, $u_{n+1} = u_n^2$.
Express u_n in terms of u_0 and n.

Exercise 33: (3)
Show that:

$$\forall n \in \mathbb{N}^*,\ \frac{3n}{2n+1} \leq \sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}.$$

We know that $\left(\sum_{k=1}^{n} \frac{1}{k^2}\right)$ is increasing; from the second inequality it is bounded above, hence it converges to some real x. Passing to the limit gives $\frac{3}{2} \leq x \leq 2$.

In fact,

$$x = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \approx 1.644934.$$

This is the celebrated *Basel problem*. Posed by Pietro Mengoli (1626–1686) in 1644 and studied by Jakob Bernoulli, it resisted many attempts until Euler gave a rigorous proof in 1741 (after an initial heuristic argument in 1735 via an infinite product for sin).

Exercise 34: (3)
(Prerequisites: trigonometry, triangle inequality)
Show that:

$$\forall x \in \mathbb{R},\ \forall n \in \mathbb{N}, \quad |\sin(nx)| \leq n\,|\sin x|.$$

Exercise 35: (3)
Find a formula for the n-th derivative of the natural logarithm for all $n \in \mathbb{N}^*$.

Exercise 36: (3)
(Prerequisite: Pascal's identity, $\forall n \in \mathbb{N}$, $\forall k \in [\![1, n-1]\!]$, $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.)
Show that:

$$\forall x, y \in \mathbb{C},\ \forall n \in \mathbb{N}, \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

This is the *binomial theorem*. It holds in great generality—over any commutative ring, not just $\mathbb{C}$ (commutative meaning $ab = ba$ for all a, b).

Exercise 37: (4)
Let $c > 0$, and $f : x \mapsto \frac{x}{\sqrt{1+cx^2}}$.
Determine a general formula for f^n, the n-fold composition of f.

5.5.2 Multiple recurrences (and more!)

Exercise 38: (1)
Let (u_n) be defined by $u_0 = 2$, $u_1 = 5$, and for all $n \in \mathbb{N}$, $u_{n+2} = 5u_{n+1} - 6u_n$.
Show that $u_n = 2^n + 3^n$.

Such sequences, where the $(n+2)$-th term is a linear combination with constant coefficients of the two previous terms, are called *homogeneous linear recurrences of order 2*.

Exercise 39: (1)
Let (u_n) be defined by $u_0 = 1$, $u_1 = 3$, and for all $n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - 2u_n$.
Show that $u_n = 2^{n+1} - 1$.

Exercise 40: (2)
Prove Proposition 11 by following the pattern of the proof of Proposition 14.

Exercise 41: (2)
(This exercise does not *a priori* use induction, though it could; it features the Fibonacci sequence introduced earlier.)
Compute, for all $n \in \mathbb{N}^*$, $F_{n-1}F_{n+1} - F_n^2$.
Then deduce the limit of $\left(\sum_{k=1}^{n} \frac{(-1)^{k+1}}{F_k F_{k+1}}\right)$ after finding a simpler expression for the partial sums.

Exercise 42: (3)
Let $N \geq 2$. Show that for all $m \in [\![2, N]\!]$:

$$\sqrt{m\sqrt{(m+1)\sqrt{\ldots\sqrt{N}}}} < m+1,$$

and deduce that:

$$\sqrt{2\sqrt{3\sqrt{\ldots\sqrt{N}}}} < 3.$$

Exercise 43: (3)
Consider the set E of real sequences satisfying:

$$\forall n \in \mathbb{N}, \quad u_{n+2} = au_{n+1} + bu_n,$$

where $a, b \in \mathbb{R}$ are such that the equation $x^2 = ax + b$ has two distinct real solutions λ and μ.
(This is the *characteristic equation.*)

Show that $\forall \alpha, \beta \in \mathbb{R}$, the sequence $(\alpha\lambda^n + \beta\mu^n)$ belongs to E.

Justify that if $u \in E$, there exist $\alpha, \beta \in \mathbb{R}$ with $(u_0 = \alpha + \beta) \wedge (u_1 = \alpha\lambda + \beta\mu)$, and deduce that $\forall n \in \mathbb{N}$, $u_n = \alpha\lambda^n + \beta\mu^n$.

This explains the appearance of $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$ in the study of Fibonacci: these are the roots of $x^2 = x + 1$, the characteristic equation for $F_{n+2} = F_{n+1} + F_n$.

Exercise 44: (3)
Continue with the notations of Exercise 43, but now assume that a and b are such that $x^2 = ax + b$ has a unique real root $\lambda \neq 0$.
Following the method of Exercise 43, show that:

$$E = \{\, ((\alpha + \beta n)\lambda^n) \;:\; \alpha, \beta \in \mathbb{R} \,\}.$$

Exercise 45: (4)
Show that for every $n \in \mathbb{N}$ there exists a unique sequence (ε_k) with values in $\{0, 1\}$ such that $n = \sum_{k=0}^{\infty} \varepsilon_k 2^k$. Be careful to justify that this sum is finite.

If p is the largest integer such that $\varepsilon_p \neq 0$, then $n = \varepsilon_0 + 2\varepsilon_1 + \cdots + 2^p \varepsilon_p$. The string $\varepsilon_p \ldots \varepsilon_0$ is the *binary expansion* of n. One can generalize by replacing 2 with any integer base $b \geq 2$; this yields the *base-b expansion* (then $\varepsilon_k \in \{0, \ldots, b-1\}$). Our usual numeral system uses base 10.

Exercise 46: (4)
(Prerequisite: facility with summation manipulations.)
Let u and v be two sequences such that:

$$\forall n \in \mathbb{N}, \quad u_n = \sum_{k=0}^{n} \binom{n}{k} v_k.$$

Show, by "strong induction," that:

$$\forall n \in \mathbb{N}, \quad v_n = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n}{k} u_k.$$

This is *Pascal's inversion formula* (Blaise Pascal, 1623–1662). It has many applications in classical counting problems, such as counting surjections between finite sets (a surjection is a map such that each element of the target has at least one preimage).

Exercise 47: (4)
Let (F_n) denote the Fibonacci sequence.
Show that:

$$\forall p \in \mathbb{N}^*,\ \forall q \in \mathbb{N}, \quad F_p F_{q+1} + F_{p-1} F_q = F_{p+q}.$$

This exercise illustrates how crucial it is to set up the induction hypothesis properly.

Exercise 48: (5)
Let $H_n = \sum_{k=1}^{n} \frac{1}{k}$ for $n \in \mathbb{N}^*$.

Show that, when written in lowest terms, H_n is always a fraction with odd numerator and even denominator for $n \geq 2$.

The sequence $\left(\sum_{k=1}^{n} \frac{1}{k}\right)$ is the *harmonic series*. Contrary to what one might think, it diverges—albeit very slowly, roughly like $\ln n$. However, $\left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right)$ converges to a constant commonly denoted γ, the *Euler–Mascheroni constant*. This constant appears in many places, but little is known about it; we do not even know whether it is rational. It is known that if it were rational, the denominator in lowest terms would have more than 242,080 digits... Everything suggests it is irrational, but no proof is known.

Exercise 49: (5)
Define $f : \mathbb{N} \to \mathbb{N}$ by

$$\forall n \in \mathbb{N}, \quad f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even,} \\ n+5 & \text{otherwise.} \end{cases}$$

Let f^k denote the k-fold composition of f for $k \in \mathbb{N}$.
Show that:

$$\forall n \in \mathbb{N}^*,\ \exists k \in \mathbb{N}, \quad f^k(n) \in \{1, 5\}.$$

This resembles the *Collatz (Syracuse) conjecture*, first stated by Lothar Collatz (1910–1990): for

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even,} \\ 3n+1 & \text{otherwise,} \end{cases}$$

the claim is $\forall n \in \mathbb{N}^*,\ \exists k \in \mathbb{N},\ f^k(n) = 1$. Despite its simple statement, no proof is known to this day.

Exercise 50: (5)
(Prerequisite: enjoy calculations and sums!)
Define the sequence (B_n) of Bernoulli numbers by $B_0 = 1$ and:

$$\forall n \in \mathbb{N}^*, \quad B_n = \frac{-1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k.$$

Show that:

$$\forall n, p \in \mathbb{N}^*, \quad \sum_{k=0}^{n-1} k^p = \frac{1}{p+1} \sum_{k=0}^{p} \binom{p+1}{k} B_k\, n^{p+1-k}.$$

Here are the first values of the Bernoulli numbers: $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$, ...

Using the *generating function* (see below) of $\left(\frac{B_n}{n!}\right)$, one can show that $B_n = 0$ for odd $n > 1$, and that B_{2k} has the sign $(-1)^{k-1}$.

Roughly, if (u_n) is a complex sequence, a generating function for u is $f(x) = \sum_{n=0}^{\infty} u_n x^n$ when this makes sense (for $|x|$ small enough).

This function encodes many properties of u: for example, if it is even (resp. odd), then $(u_{2n+1}) = (0)$ (resp. $(u_{2n}) = (0)$), and conversely.

The generating function of $\left(\frac{B_n}{n!}\right)$ is $x \mapsto \frac{x}{e^x - 1}$, and since $x \mapsto \frac{x}{e^x-1} + \frac{x}{2} = 1 + \sum_{n=2}^{\infty} \frac{B_n}{n!} x^n$ is even, it follows that $B_n = 0$ for odd $n \neq 1$.

6 Solutions

Solution to Exercise 1:
Knowing that P XOR Q is true only if exactly one of the two propositions P, Q is true, we obtain the table:

P	Q	P XOR Q
T	T	F
T	F	T
F	T	T
F	F	F

To prove the two remaining equivalences, we can also draw the truth tables of the propositions:

P	Q	$P \vee Q$	$\neg P \vee \neg Q$	$(P \vee Q) \wedge (\neg P \vee \neg Q)$
T	T	T	F	F
T	F	T	T	T
F	T	T	T	T
F	F	F	T	F

P	Q	$P \wedge \neg Q$	$\neg P \wedge Q$	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
T	T	F	F	F
T	F	T	F	T
F	T	F	T	T
F	F	F	F	F

The columns are the same: therefore the propositions are equivalent!

Solution to Exercise 2:
a) According to De Morgan's laws,

$$(\neg(\neg P \vee \neg Q)) \Leftrightarrow ((\neg(\neg P)) \wedge (\neg(\neg Q))).$$

But for any proposition P, $\neg(\neg P) \Leftrightarrow P$ (Proposition 1), hence the result.
b) Similarly according to De Morgan's laws,

$$(\neg(\neg P \wedge \neg Q)) \Leftrightarrow (\neg(\neg P) \vee \neg(\neg Q)) \Leftrightarrow (P \vee Q).$$

We could also have applied the result of a) to $\neg P$ and $\neg Q$, then used the fact that for any propositions P and Q, $(P \Leftrightarrow Q) \Leftrightarrow (\neg P \Leftrightarrow \neg Q)$.
c) According to Proposition 4, $(P \implies Q) \Leftrightarrow (\neg P \vee Q)$, hence:

$$(P \wedge (P \implies Q)) \Leftrightarrow (P \wedge (\neg P \vee Q)) \Leftrightarrow ((P \wedge \neg P) \vee (P \wedge Q)),$$

according to distributivity of "and" over "or." But $P \wedge \neg P$ is never true so

$$((P \wedge \neg P) \vee (P \wedge Q)) \Leftrightarrow (P \wedge Q),$$

which concludes.
d) Knowing that $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$, we have:

$$(\neg(P \vee Q) \vee (\neg P \wedge Q)) \Leftrightarrow ((\neg P \wedge \neg Q) \vee (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge (Q \vee \neg Q)),$$

the last equivalence being a consequence of distributivity rules.
But $Q \vee \neg Q$ is always true (it is a tautology), hence:

$$(\neg P \wedge (Q \vee \neg Q)) \Leftrightarrow \neg P.$$

e) By distributivity,

$$(\neg P \vee (P \wedge Q)) \Leftrightarrow ((\neg P \vee P) \wedge (\neg P \vee Q)).$$

But $\neg P \vee P$ is a tautology, therefore:

$$(\neg P \vee (P \wedge Q)) \Leftrightarrow (\neg P \vee Q) \Leftrightarrow (P \implies Q),$$

according to Proposition 4.
f) According to Proposition 4,

$$(P \implies (Q \wedge R)) \Leftrightarrow (\neg P \vee (Q \wedge R)).$$

By distributivity,

$$(\neg P \vee (Q \wedge R)) \Leftrightarrow ((\neg P \vee Q) \wedge (\neg P \vee R)).$$

According to Proposition 4,

$$(\neg P \vee Q) \Leftrightarrow (P \implies Q),$$

and likewise for the right-hand proposition.
Thus,

$$(P \implies (Q \wedge R)) \Leftrightarrow ((P \implies Q) \wedge (P \implies R)).$$

g) According to Proposition 4,

$$((P \wedge Q) \implies R) \Leftrightarrow ((\neg(P \wedge Q)) \vee R).$$

But according to De Morgan's laws,

$$(\neg(P \wedge Q)) \Leftrightarrow (\neg P \vee \neg Q).$$

Hence,

$$((\neg(P \wedge Q)) \vee R) \Leftrightarrow ((\neg P \vee \neg Q) \vee R).$$

But

$$((\neg P \vee \neg Q) \vee R) \Leftrightarrow (\neg P \vee (\neg Q \vee R)) \Leftrightarrow (P \implies (\neg Q \vee R)) \Leftrightarrow (P \implies (Q \implies R)),$$

where we used associativity of "or" and Proposition 4 twice.

Solution to Exercise 3:
a) $\forall n \in \mathbb{N},\ n \geq 4,\ 2|n,\ \exists p, q \in \mathbb{P},\ n = p + q$

We could also write:
$\forall n \in \mathbb{N},\ n \geq 4,\ (2|n) \implies (\exists p, q \in \mathbb{P},\ n = p + q)$

b) $\forall n, n' \in \mathbb{N},\ (n \leq n') \implies (u_n \leq u_{n'})$

c) $\exists M \in \mathbb{R},\ \forall n \in \mathbb{N},\ |u_n| \leq M$

d) $\exists c \in \mathbb{R},\ \forall x \in \mathbb{R}, f(x) = c$
Translated into plain language: there exists a constant c such that every real x has c as its image by f.

e) $\forall x \in \mathbb{R},\ \exists (q_n) \in \mathbb{Q}^{\mathbb{N}},\ q_n \to x$

f) $\exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ u_n = u_{n+N}$

g) $\exists T \in \mathbb{R},\ \forall x \in \mathbb{R},\ f(x+T) = f(x)$
For example, if $f = \sin$, any $T \in \{2k\pi, k \in \mathbb{Z}\}$ works.

h) $\forall x, y \in \mathbb{R},\ (x < y) \implies (f(x) < f(y))$

Solution to Exercise 4:
a) $\exists n \in \mathbb{N},\ n \geq 4,\ 2|n,\ \forall p, q \in \mathbb{P},\ n \neq p + q$
Yes indeed! The proposition to be negated was of the form "for all n satisfying ..." followed by a predicate on n: its negation is therefore that there exists an n satisfying ... but which does not satisfy the predicate in question.

b) $\exists n, n' \in \mathbb{N},\ (n \leq n') \wedge (u_n > u_{n'})$
The reasoning is the same as for a), which is essentially due to the fact that we could also have written question a) of Exercise 3 with an implication.

c) $\forall M \in \mathbb{R},\ \exists n \in \mathbb{N},\ |u_n| > M$
Which in plain language means that (u_n) takes arbitrarily large values!

d) $\forall c \in \mathbb{R},\ \exists x \in \mathbb{R},\ f(x) \neq c$

e) $\exists x \in \mathbb{R},\ \forall (q_n) \in \mathbb{Q}^{\mathbb{N}},\ q_n \nrightarrow x$

f) $\forall N \in \mathbb{N},\ \exists n \in \mathbb{N},\ u_n \neq u_{n+N}$

g) $\forall T \in \mathbb{R},\ \exists x \in \mathbb{R},\ f(x) \neq f(x+T)$

h) $\exists x, y \in \mathbb{R},\ (x < y) \wedge (f(x) \geq f(y))$

Solution to Exercise 5:
a) Let us translate once quickly: for every real x, there exists a real y whose image by f strictly exceeds

that of x. This means exactly that f has no maximum! For example, $f : x \mapsto x^2$ or $f : x \mapsto 1 - \frac{1}{1+x^2}$ satisfy this proposition, but $f : x \mapsto \frac{1}{1+x^2}$ does not: it has a maximum of 1 at 0.

b) This statement means that every value taken by f is taken at least twice: for any real x, one can find a nonzero real T such that x and $x + T$ have the same image. For example, any periodic function satisfies this property, say cos or even $x \mapsto \{x\}$ where $\{x\}$ is the *fractional part* of x, the difference between x and its integer part (this function is 1-periodic, prove it!).

c) This statement says that there exists a real x whose image by f is all of $\mathbb{R}$: this is impossible! No function satisfies it.

Solution to Exercise 6:

The idea is to use the irrationality of $\sqrt{2}$. Let us reason by contradiction by assuming that $b \neq 0$. Then:

$$(a + b\sqrt{2} = 0) \Leftrightarrow (\sqrt{2} = -\tfrac{a}{b} \in \mathbb{Q}).$$

This is absurd because $\sqrt{2}$ is irrational. Thus $b = 0$, and since $a + b\sqrt{2} = 0$ we obtain $a = 0$.
Now, $\forall a, b, c, d \in \mathbb{Q}$,

$$(a + b\sqrt{2} = c + d\sqrt{2}) \Leftrightarrow ((a - c) + (b - d)\sqrt{2} = 0).$$

And by virtue of what precedes, $a - c = b - d = 0$, hence $a = c$ and $b = d$.

Solution to Exercise 7:

Suppose that all drawers contain at most one sock. Since there are n of them, the number of socks is at most n, i.e. $n + 1 \leq n$: this is absurd.
Thus, at least one drawer contains at least two socks.

For the application, it suffices to consider the drawers $\left[\frac{k}{n}, \frac{k+1}{n}\right]$, $0 \leq k < n$.
According to what precedes, there exists a drawer containing two socks, i.e.:

$$\exists k \in [\![0; n-1]\!],\ \exists i < j \in [\![0; n-1]\!],\ \frac{k}{n} \leq x_i \leq x_j \leq \frac{k+1}{n},$$

and therefore $|x_i - x_{i+1}| = x_{i+1} - x_i \leq x_j - x_i \leq \frac{k+1}{n} - \frac{k}{n} = \frac{1}{n}$.

Solution to Exercise 8:

Let $n \in \mathbb{N}^*$.
Suppose that $\sqrt{1 + n^2}$ is an integer, denoted d. Then,

$$1 = d^2 - n^2 = (d - n)(d + n).$$

Therefore $d + n \mid 1$. Since it is a natural integer, it cannot be -1, so $d + n = 1$, and then $d - n = 1$. From the half-sum of these equalities we deduce $d = 1$ and thus $n = 0$, whereas n had precisely been chosen to be nonzero.
Thus, $\forall n \in \mathbb{N}^*,\ \sqrt{1 + n^2} \notin \mathbb{N}$.

Solution to Exercise 9:
Suppose that $\frac{\ln(3)}{\ln(2)}$ is rational, write it in irreducible form $\frac{p}{q}$. Then,

$$\frac{\ln(3)}{\ln(2)} = \frac{p}{q} \Leftrightarrow q\ln(3) = \ln(3^q) = p\ln(2) = \ln(2^p)$$

$$\Leftrightarrow 3^q = 2^p.$$

But the left-hand side is odd, whereas the right-hand side is even (unless $p = 0$, which is clearly not the case): this is absurd. Thus, $\frac{\ln(3)}{\ln(2)} \notin \mathbb{Q}$.
Replace 2 and 3 by two distinct prime numbers r and s. Then:

$$\tfrac{\ln(r)}{\ln(s)} = \tfrac{p}{q} \Leftrightarrow r^q = s^p,$$

which is absurd by uniqueness of the factorization of an integer into prime factors.
Thus, if r and s are distinct prime numbers, $\frac{\ln(r)}{\ln(s)} \notin \mathbb{Q}$.

Solution to Exercise 10:
Suppose that exp is a polynomial:

$$\exists n \in \mathbb{N},\ \exists a_0, \dots, a_n \in \mathbb{R},\ \forall x \in \mathbb{R},\ \mathrm{e}^x = a_0 + \cdots + a_n x^n.$$

We know that a polynomial of degree n differentiated $n+1$ times is zero. But since $\exp' = \exp$, by differentiating $n+1$ times the relation above we obtain:

$$\forall x \in \mathbb{R},\ \mathrm{e}^x = 0,$$

which is of course absurd.
Thus, exp is not a polynomial.

Solution to Exercise 11:
Suppose that $\sqrt{2} + \sqrt{3}$ is a rational, denote it r.
Then:

$$r^2 = 5 + 2\sqrt{6},$$

and therefore:

$$\sqrt{6} = \tfrac{r^2-5}{2} \in \mathbb{Q}.$$

Now write $\sqrt{6} = \frac{p}{q}$ in irreducible form (with p and q coprime).
We have $p^2 = 6q^2$, so 2 divides p^2 and thus 2 divides p.
Then $\exists k \in \mathbb{Z},\ p = 2k$ so $4k^2 = 6q^2$ i.e. $2k^2 = 3q^2$, so 2 divides $3q^2$ but 2 and 3 are coprime, so by Gauss's lemma $2|q^2$ i.e. $2|q$: contradiction with the fact that p and q are coprime.
Thus, $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Solution to Exercise 12:
Suppose that there exist only finitely many primes r, denoted $p_1, \dots, p_r$.
The idea is to construct a number that cannot have any prime divisor in the list $\{p_1, \dots, p_r\}$ without

leading to an absurdity (which will then give us our final contradiction).

Consider $N = p_1 \dots p_r + 1$. Since N is strictly larger than p_r, it is not prime (otherwise it would be in the list): it has a prime divisor denoted p_k which belongs to the list $\{p_1, \dots, p_r\}$ by hypothesis. But p_k divides $p_1 \dots p_r$, so p_k divides $N - p_1 \dots p_r = 1$: absurd.
Thus, there exists an infinity of prime numbers.

Note that this demonstration shows that if p_n denotes the n-th prime, then $p_{n+1} \leq p_1 \dots p_n + 1$: the $(n+1)$-th prime cannot be "too large." Yet, one can find sequences of successive numbers arbitrarily long such that none is prime: it suffices to consider $n!+2, n!+3, \dots, n!+n$, which is a sequence of length $n-1$ of successive composite numbers (because $\forall k \in [\![2, n]\!],\ n!+k = k(1 \times 2 \times \dots \times (k-1) \times (k+1) \times \dots \times n))$. Puzzling!

Now let us show that there exist infinitely many primes congruent to 3 modulo 4: again, suppose there exist only finitely many r, denoted $p_1, \dots, p_r$. Let us take inspiration from the previous proof to construct an integer N that will necessarily have a prime divisor congruent to 3 modulo 4 which is not in the list, without this being absurd.
Notice that a product of numbers congruent to 1 modulo 4 is congruent to 1 modulo 4, so if our number N is congruent to 3 modulo 4, it will necessarily have a prime divisor congruent to 3 modulo 4!

These considerations, as well as the idea from the previous question, lead us to set $N = 4p_1 \dots p_r - 1$, which is congruent to 3 modulo 4, so it admits a prime divisor congruent to 3 modulo 4, which by hypothesis belongs to the list, let us denote it p_k. Since p_k divides $p_1 \dots p_r$, it divides $4p_1 \dots p_r - N = 1$: absurd!
Thus, there exists an infinity of prime numbers congruent to 3 modulo 4.

Solution to Exercise 13:
We reason by contrapositive: if n is even, then n^2 is also even because n can be written $2k$ and thus $n^2 = 2 \times 2k^2$ is even. Then $n^2 + 1$ is odd: we have indeed proved the desired proposition by contraposition!

Solution to Exercise 14:
We reason by contrapositive by assuming that $l < 0$, let us show therefore that (u_n) is not positive-term, i.e. that at least one of the terms is strictly negative. In mathematics, and in particular in this kind of exercises where visualization is essential, it is imperative to make **drawings**.
By definition of the limit,

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ |u_n - l| < \varepsilon.$$

Take $\varepsilon = \frac{-l}{2} > 0$.

Then, by definition,

$$\exists N \in \mathbb{N},\ \forall n \geq N,\ |u_n - l| < \tfrac{-l}{2}.$$

By choosing ε in this way, we are sure that for $n \geq N$, the u_n will all be in the yellow zone, and thus

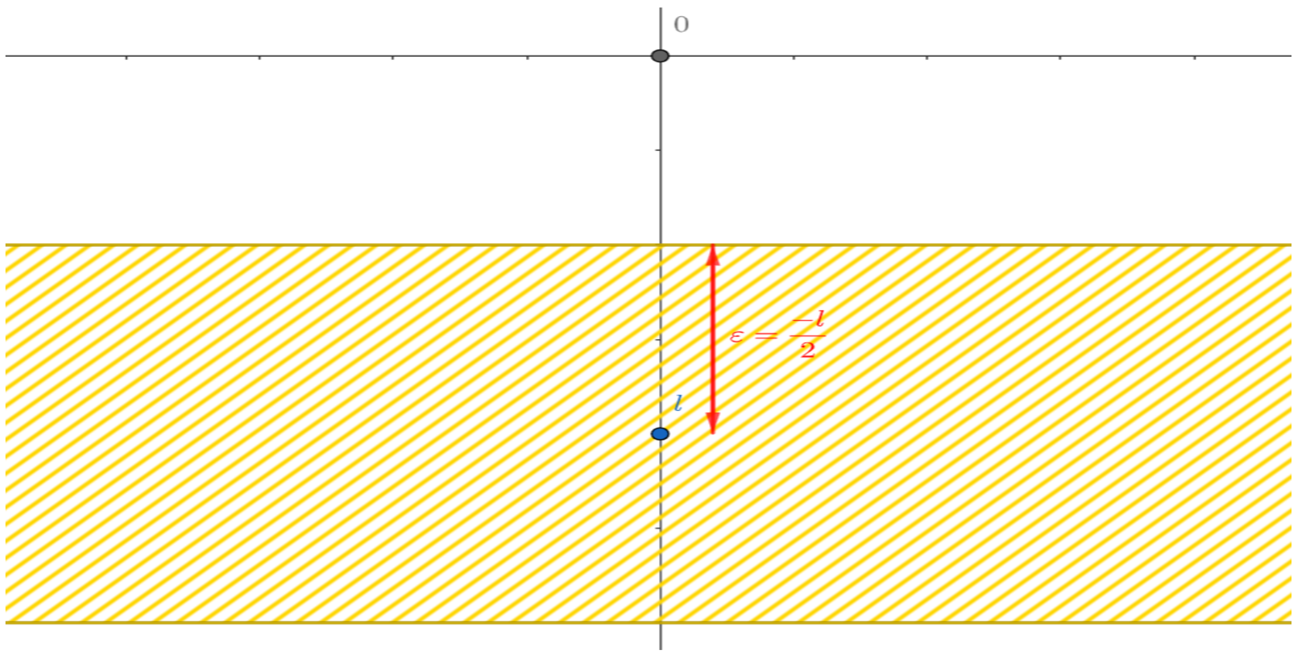

Figure 1: Drawing

will be strictly negative.
In particular,

$$u_N - l \leq |u_N - l| < \tfrac{-l}{2},$$

and therefore $u_N < \frac{l}{2} < 0$, which concludes!

Solution to Exercise 15:
We reason by contrapositive by showing that:

$$(7|x^2 + y^2) \implies ((7|x) \wedge (7|y)).$$

To do this, we can construct a double-entry table giving the residue modulo 7 of $x^2 + y^2$ as a function of those of x and y.

x mod 7 \ y mod 7	0	1	2	3	4	5	6
0	0	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	3	3
4	2	3	6	4	4	6	3
5	4	5	1	3	6	1	5
6	1	2	5	3	3	5	2

where we see that

$$(7|x^2 + y^2) \Leftrightarrow ((7|x) \wedge (7|y)).$$

In particular, we have proved the desired proposition.

Solution to Exercise 16:
We reason by contrapositive by assuming that n is odd and we show that $8|n^2-1$.

We know that $n^2-1=(n-1)(n+1)$ and since n is odd, $n-1$ and $n+1$ are even.
If $n=1$, we clearly have $8|n^2-1$.
Otherwise, $n \geq 3$ and therefore $n-1$ and $n+1$ are two even numbers greater than 2 and differing by 2: at least one of them is divisible by 4. Indeed, if $n=2k+1$ and we suppose that $n-1=2k$ is not divisible by 4, then k is odd, of the form $2k'+1$ and thus $n+1=2(2k'+1)+2=4(k'+1)$: $n+1$ is divisible by 4.
In the same way, if $n+1$ is not divisible by 4, then $n-1$ is.

Since $n^2-1=(n-1)(n+1)$ and one of the two factors is divisible by 2 while the other is divisible by 4, n^2-1 is divisible by $2\times 4=8$: we have proved the desired proposition by contraposition.

Solution to Exercise 17:
We reason by contrapositive by assuming that n is composite: it then admits a divisor different from 1, denoted a. We can therefore write n in the form ab with $a,b \geq 2$.
We know the formula valid for all complex x,y and every integer n:

$$x^n-y^n=(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k},$$

from which we deduce that:

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

But $a\neq 1$ so $2^a-1\neq 1$, and $b\neq 1$ so a fortiori $a\neq n$ and thus $2^a-1\neq 2^n-1$.
Thus, we have shown by the equality above that 2^a-1 was a divisor of 2^n-1 but was neither 1 nor 2^n-1, which means that 2^n-1 is composite: we have proved the desired proposition by contraposition.

Solution to Exercise 18:
We are tempted to solve such an equation by equivalence as usual, but the presence of the square root prevents us from "reversing" the reasoning: we are therefore naturally led to reason by analysis-synthesis.

Analysis: Suppose the existence of $x\in\mathbb{R}$ satisfying the given equation.
Then, a necessary condition for the square roots to exist at all is that $2x+1\geq 0$ and $x-3\geq 0$, i.e. $x\geq 3$.
If x is a solution, **then** $2x+1=x-3$ (this is not an equivalence but an **implication**, because we squared: we cannot reverse the reasoning by simply taking the square root, since for $y\in\mathbb{R}$, $\sqrt{y^2}=|y|$ and not y! Beware of this frequent mistake).
We then deduce that $x=-4$. But a necessary condition for x to be a solution was that $x\geq 3$: we deduce from this analysis that the proposed equation has no solution!

Solution to Exercise 19:
We reason by analysis-synthesis.

Analysis: Let f be a function from $\mathbb{R}$ to itself satisfying the proposed equation.
By substituting 0 for x and y we obtain $f(0) = 2f(0)$ i.e. $f(0) = 0$ (a necessary condition for f to be a solution is that $f(0) = 0$).
Fix $x \in \mathbb{R}$ **arbitrary**. Differentiate the function $y \mapsto f(x+y) = f(x) + f(y)$ (we can because f is differentiable). We have then:

$$\forall y \in \mathbb{R},\ f'(x+y) = f'(y).$$

But this holds for any fixed real x, so if we consider an arbitrary real y and substitute $-y$ for x in the above equality, we obtain that $\forall y \in \mathbb{R},\ f'(y) = f'(0)$: f' is constant.
Now, given that $f(0) = 0$, we deduce that f is linear.
Thus, a necessary condition for f to be a solution is that it be linear. Let us show in the synthesis that this condition is sufficient.

Synthesis: Let $f : x \mapsto ax$ where a is any real.
Then f is differentiable and:

$$\forall x, y \in \mathbb{R},\ f(x+y) = a(x+y) = ax + ay = f(x) + f(y).$$

Thus, linear functions are solutions and by the analysis they are the only ones.

Solution to Exercise 20:
We reason by analysis-synthesis.

Analysis: Let $f : \mathbb{R}^{+*} \to \mathbb{R}$ be differentiable satisfying the given equation.
Let us take inspiration from Exercise 19 and fix any strictly positive real y. Differentiate then $x \mapsto f(xy) = f(x) + f(y)$, we obtain:

$$\forall x \in \mathbb{R}^{+*},\ yf'(xy) = f'(x).$$

Now, since this holds for any strictly positive real x, by evaluating at 1 we get $yf'(y) = f'(1)$ i.e. $f'(y) = \frac{f'(1)}{y}$, and this holds for any strictly positive real y chosen. By integrating, we deduce that:

$$\exists c \in \mathbb{R},\ \forall y \in \mathbb{R}^{+*},\ f(y) = f'(1)\ln(y) + c.$$

Now, by substituting 1 for x and y in the initial equation, we obtain $2f(1) = f(1)$ i.e. $f(1) = 0$ and thus $c = 0$.
Thus, a necessary condition for f to be a solution is to be proportional to the natural logarithm. Let us check in the synthesis that this is a sufficient condition.

Synthesis: Let $f : x \mapsto a\ln(x)$ for any $a \in \mathbb{R}$.
Then f is differentiable and:

$$\forall x, y \in \mathbb{R}^{+*},\ f(xy) = a\ln(xy) = a\ln(x) + a\ln(y) = f(x) + f(y).$$

Thus, functions proportional to the logarithm are solutions and by the analysis they are the only ones.

Solution to Exercise 21:
We reason by analysis-synthesis.

Analysis: Let f be a function from $\mathbb{R}$ to itself satisfying the given equation. Fix any real x and substitute the real $f(x)$ for y, it follows:

$$f(0) = 2 - x - f(x)$$

i.e. $f(x) = 2 - x - f(0)$ and this for any real x. By substituting 0 for x it follows $f(0) = 2 - f(0)$ i.e. $f(0) = 1$ and therefore $\forall x \in \mathbb{R},\ f(x) = 1 - x$.

Synthesis: Let $f : x \mapsto 1 - x$. Then,

$$\forall x, y \in \mathbb{R},\ f(y - f(x)) = 1 - y + f(x) = 2 - y - x.$$

Thus, the solution to this equation is $x \mapsto 1 - x$.

Solution to Exercise 22:
We reason by analysis-synthesis.

Analysis: Let f be a function from $\mathbb{R}$ to itself satisfying the given equation.
By evaluating x and y at 1 we obtain $f(1) = 2f(1)$ i.e. $f(1) = 0$.
Next, by evaluating at $y = 1$ we obtain:

$$(\forall x \in \mathbb{R},\ f(x) = xf(x)) \Leftrightarrow (\forall x \in \mathbb{R},\ f(x)(1 - x) = 0)$$

$$\Leftrightarrow (\forall x \in \mathbb{R},\ x \neq 1,\ f(x) = 0).$$

Finally, given that $f(1) = 0$, we obtain that f is identically zero.

Synthesis: Conversely, we immediately verify that the zero function is a solution.
Thus, only the zero function is a solution.

Solution to Exercise 23:
We reason by analysis-synthesis.

Analysis: Let f be a function from $\mathbb{R}$ to itself that is a solution of the given equation.
We know that:

$$\forall x \in \mathbb{R},\ f(x) + xf(1 - x) = 1 + x.$$

Since this holds for all real x, we obtain by replacing x by $1 - x$ for any real x:

$$f(1 - x) + (1 - x)f(x) = 2 - x.$$

By multiplying the second relation by x and subtracting it from the first, we obtain:

$$\forall x \in \mathbb{R},\ f(x)(1 - x + x^2) = 1 - x + x^2.$$

Now the discriminant of $X^2 - X + 1$ is $-3 < 0$, hence $\forall x \in \mathbb{R},\ x^2 - x + 1 \neq 0$.
Therefore:

$$(\forall x \in \mathbb{R},\ f(x)(x^2 - x + 1) = x^2 - x + 1) \Leftrightarrow (\forall x \in \mathbb{R},\ f(x) = 1).$$

Thus, if f is a solution, it is constant, equal to 1.

Synthesis: Conversely, we immediately verify that the constant function equal to 1 works.
Thus, the only solution is the constant function equal to 1.

Solution to Exercise 24:
We reason by analysis-synthesis.

Analysis: Let $f : \mathbb{R} \to \mathbb{R}$ be a solution of the given equation.
Take any $y \in \mathbb{R}$. By substituting $f(y)$ for x in the equation we obtain:

$$2f(f(y)) + f(y) + f(0) = y,$$

and therefore:

$$\forall y \in \mathbb{R},\ f(f(y)) = \tfrac{y-f(y)-f(0)}{2}.$$

From there, by substituting 0 for x, we have:

$$\forall y \in \mathbb{R},\ 2f(0) + f(f(y)) = y,$$

and by using the expression of $f \circ f$ determined above,

$$(\forall y \in \mathbb{R},\ 2f(0) + \tfrac{y-f(y)-f(0)}{2} = y) \Leftrightarrow (\forall y \in \mathbb{R},\ f(y) = -y + 3f(0)).$$

And by evaluating at $y = 0$, we obtain that $f(0) = 0$, thus $f : x \mapsto -x$.

Synthesis: If $f : x \mapsto -x$ then:

$$\forall x, y \in \mathbb{R},\ 2f(x) + x + f(f(y) - x) = -2x + x - (-y - x) = y.$$

Thus, the only solution to the given equation is $f : x \mapsto -x$.

Solution to Exercise 25:
Suppose that $r = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $\mathrm{GCD}(p, q) = 1$ is a root of $P(X) = a_0 + a_1X + \cdots + a_nX^n$ where $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, $n \geq 1$.
Then,

$$a_0 + a_1\tfrac{p}{q} + \cdots + a_n\left(\tfrac{p}{q}\right)^n = 0 \implies q^na_0 + q^{n-1}a_1p + \cdots + qa_{n-1}p^{n-1} + a_np^n = 0,$$

where we have multiplied by q^n.

Then,

$$-a_np^n = q(q^{n-1}a_0 + q^{n-2}a_1p + \cdots + a_{n-1}p^{n-1}),$$

so $q | -a_np^n$. But $\mathrm{GCD}(p, q) = 1$ so $\mathrm{GCD}(p^n, q) = 1$, so by Gauss's lemma $q|a_n$.
Moreover, we also have:

$$p(a_1q^{n-1} + \cdots + qa_{n-1}p^{n-2} + a_np^{n-1}) = -a_0q^n.$$

And by the same reasoning, we deduce that $p|a_0$.

Thus, a necessary condition for $\frac{p}{q}$, $\text{GCD}(p,q) = 1$ to be a root of a non-constant integer-coefficient polynomial P is that the numerator p divides its constant coefficient, and that the denominator q divides its leading coefficient.

This criterion allows us to know quickly whether a polynomial does or does not have obvious roots: consider the polynomial $X^3 - 2X^2 + 7$. If it had a rational root $\frac{p}{q}$ (in irreducible form), then q would divide 1, i.e. would equal -1 or 1, and p would divide 7, i.e. would equal -7, 7, 1 or -1: the only possible rational roots are thus 7, -7, 1 or -1, and we verify that none of them is a root of the polynomial, so we do not need to look any further.

Now let us answer the second part of the exercise. Let $n \in \mathbb{N}$. It suffices to remark that $\sqrt{n}$ is a root of $X^2 - n$: according to the previous criterion, if $\sqrt{n}$ were rational, of the irreducible form $\frac{p}{q}$, then q would divide 1, thus would equal 1 or -1, so $\sqrt{n}$ would be integer and n would be a perfect square. Conversely, if n is a perfect square, $\sqrt{n}$ is an integer, hence rational.

Thus, all numbers $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \ldots$ are irrational.

Solution to Exercise 26:
We reason by analysis-synthesis.

Analysis: Let $f : \mathbb{R} \to \mathbb{R}$ be **continuous** verifying the given equation.
We establish for $n \in \mathbb{N}$ the property $P_n : f(n) = nf(1)$.
By evaluating the equation verified by f at $x = 0$ and $y = 0$ we obtain $f(0) = 2f(0)$ i.e. $f(0) = 0$: P_0 is true.
Suppose P_n for a given $n \in \mathbb{N}$. Then by the relation verified by f:

$$f(n+1) = f(n) + f(1).$$

But by induction hypothesis, $f(n) = nf(1)$ hence:

$$f(n+1) = nf(1) + f(1) = (n+1)f(1).$$

Thus, P_{n+1} is true.
By the principle of induction, $\forall n \in \mathbb{N}, f(n) = nf(1)$.

Let us extend this result to $\mathbb{Z}$: it is already true for positive integers, so let $-n \in \mathbb{Z} - \mathbb{N}$ be a strictly negative integer.
We first remark that f is odd. Indeed, if $x \in \mathbb{R}$ is any real and we substitute $y = -x$ into the equation verified by f, then we obtain:

$$(\forall x \in \mathbb{R},\ f(0) = 0 = f(x) + f(-x)) \implies (\forall x \in \mathbb{R},\ f(-x) = -f(x)).$$

Hence, $f(n) = nf(1)$ on the one hand but also $f(n) = f(-(-n)) = -f(-n)$ so $f(-n) = -nf(1)$: we have indeed extended the result to strictly negative integers.

Now let us extend the result to $\mathbb{Q}$. Let $r = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$.
As we showed above, on the one hand we have $f(qr) = qf(r)$.
But $f(qr) = f(p) = pf(1)$ again according to what we have already shown. Thus, $qf(r) = pf(1)$ i.e. $f(r) = \frac{p}{q}f(1) = rf(1)$: we have indeed extended the result to $\mathbb{Q}$.

Now let us extend the result to the whole of $\mathbb{R}$: let $x \in \mathbb{R}$.
By density of $\mathbb{Q}$ in $\mathbb{R}$:

$$\exists (q_n) \in \mathbb{Q}^{\mathbb{N}}, \ \lim_{n\to\infty} q_n = x.$$

According to what we have shown, $\forall n \in \mathbb{N}, \ f(q_n) = q_n f(1)$ because (q_n) takes rational values.
But, by continuity of f and since $q_n \to x$:

$$\lim_{n\to\infty} f(q_n) = f(x).$$

Thus by passing to the limit we obtain $f(x) = xf(1)$, whatever the real x considered.
Hence, f is linear.

Synthesis: Conversely, we have already checked in the synthesis of Exercise 19 that linear functions did indeed verify the required relation, and these are continuous.
Thus, the solutions of this functional equation are linear functions.

The reader having notions of general algebra will surely have noticed that we have just determined the set of *continuous group morphisms* from $(\mathbb{R}, +)$ into itself.

Solution to Exercise 27:
We reason by induction by establishing for $n \in \mathbb{N}$ the property $P_n : u_n = u_0 + nr$.
We have indeed $u_0 = u_0 + 0 \times r$ hence P_0.
Suppose P_n for a given $n \in \mathbb{N}$.
Then, $u_{n+1} = u_n + r$ by definition of u, but $u_n = u_0 + nr$ by induction hypothesis, thus $u_{n+1} = u_0 + nr + r = u_0 + (n+1)r$: P_{n+1} is true.
By the principle of induction, $\forall n \in \mathbb{N}, \ u_n = u_0 + nr$.

One could have intuited this result by "descending" as follows: we know that $u_n = u_{n-1} + r$, but $u_{n-1} = u_{n-2} + r$ so $u_n = u_{n-2} + 2r$, and so on until u_0. Beware, this does not constitute a proof, one must properly formulate their reasoning by induction. Moreover, to avoid confusion and mistakes with indices, it is good to identify a quantity that does not vary: when writing $u_n = u_j + lr$, one notices that each time one decrements j, one increments l: the quantity $l + j$ is therefore constant and equals n. Thus, at the end, when $j = 0$, l equals n, and not $n+1$ or $n-1$, for example.

Solution to Exercise 28:
We reason by induction by establishing for $n \in \mathbb{N}$ the property $P_n : u_n = q^n u_0$.
We have indeed $u_0 = q^0 u_0$ hence P_0.
Suppose P_n for a given $n \in \mathbb{N}$. Then, by definition of u, $u_{n+1} = qu_n$. But by induction hypothesis, $u_n = q^n u_0$, hence $u_{n+1} = q \times q^n u_0 = q^{n+1} u_0$: P_{n+1} is true.
Thus, by the principle of induction, $\forall n \in \mathbb{N}, \ u_n = q^n u_0$.

Solution to Exercise 29:
First, the solution l of the equation $x = ax + b$ is naturally $l = \frac{b}{1-a}$ (we can divide by $1 - a$ because a is different from 1). But we will not replace l by its value right away and simply use the relation $l = al + b$. To show that $(u_n - l)$ is geometric, let us compute $u_{n+1} - l$ for any $n \in \mathbb{N}$:

$$u_{n+1} - l = au_n + b - l = au_n + b - (al + b) = a(u_n - l).$$

The second equality comes from the relation $l = al + b$.
Thus, $(u_n - l)$ is geometric of ratio a. From the previous exercise, we know how to express explicitly its general term:

$$\forall n \in \mathbb{N},\ u_n - l = a^n(u_0 - l).$$

We then deduce the expression of u_n as a function of n, u_0, a, b by replacing l by its value:

$$\forall n \in \mathbb{N},\ u_n = a^n\left(u_0 - \frac{b}{1-a}\right) + \frac{b}{1-a}.$$

We now know how to express explicitly the general term of arithmetico-geometric sequences!

Solution to Exercise 30:
We reason by induction by establishing for $n \in \mathbb{N}$ the property $P_n : f(n) \geq n$.
f takes values in $\mathbb{N}$, hence takes positive values, therefore $f(0) \geq 0$: P_0 is true.
Suppose P_n for a given $n \in \mathbb{N}$.
Since f is strictly increasing, $f(n+1) > f(n)$. But, by induction hypothesis, $f(n) \geq n$, hence $f(n+1) > n$.
But f takes integer values, so $f(n+1)$ is an integer strictly greater than n: it is therefore at least equal to $n+1$, hence $f(n+1) \geq n+1$.
Thus, P_{n+1} is true.
Hence, by the principle of induction: $\forall n \in \mathbb{N},\ f(n) \geq n$.

Solution to Exercise 31:
We establish for $n \in \mathbb{N}$ the property P_n:

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

It is immediate that P_0 is true, both sides of the equality being zero when n is.
Suppose P_n for a given $n \in \mathbb{N}$. Then:

$$\sum_{k=0}^{n+1} k^2 = \sum_{k=0}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2,$$

by induction hypothesis. Now,

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n(2n+1) + 6(n+1))}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6}.$$

And noting that:

$$(n+2)(2n+3) = 2n^2 + 7n + 6,$$

we obtain:

$$\sum_{k=0}^{n+1} k^2 = \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6},$$

and thus P_{n+1} is true.
Hence, by the principle of induction:

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

We now establish for $n \in \mathbb{N}$ the property P_n:

$$\sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Likewise, P_0 is clearly true (both sides are zero when $n = 0$).
Suppose P_n for a given $n \in \mathbb{N}$.
Then,

$$\sum_{k=0}^{n+1} k^3 = \sum_{k=0}^{n} k^3 + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3,$$

by induction hypothesis. Now,

$$\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2(n^2+4n+4)}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2.$$

Therefore P_{n+1} is true.
Thus,

$$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Solution to Exercise 32:
We can quickly compute the first terms: $u_1 = u_0^2$, $u_2 = u_1^2 = (u_0^2)^2 = u_0^4$, $u_3 = u_2^2 = u_0^8$.
This leads us to establish for $n \in \mathbb{N}$ the property P_n: $u_n = u_0^{2^n}$.
We have $u_0 = u_0^{2^0}$ hence P_0 is true.
Suppose P_n for a given $n \in \mathbb{N}$. Then,

$$u_{n+1} = u_n^2 = (u_0^{2^n})^2 = u_0^{2^{n+1}},$$

hence P_{n+1}.
Thus, by the principle of induction,

$$\forall n \in \mathbb{N},\ u_n = u_0^{2^n}.$$

Solution to Exercise 33:
We reason by induction by establishing for $n \in \mathbb{N}^*$ the property P_n:

$$\frac{3n}{2n+1} \leq \sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}.$$

For $n = 1$, we clearly have $\frac{3\times 1}{2\times 1+1} = 1 \leq 1 \leq 2 - \frac{1}{1}$ hence P_1.
Suppose P_n for a given $n \in \mathbb{N}^*$. By the induction hypothesis,

$$\frac{3n}{2n+1} \leq \sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n},$$

hence:

$$\frac{3n}{2n+1} + \frac{1}{(n+1)^2} \leq \sum_{k=1}^{n+1} \frac{1}{k^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

Thus, we must show that:

$$\frac{3n}{2n+1} + \frac{1}{(n+1)^2} \geq \frac{3(n+1)}{2n+3},$$

and:

$$2 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n+1}.$$

This last inequality is equivalent to:

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

which is clearly true for any $n \in \mathbb{N}^*$.
After bringing to a common denominator, the first inequality is equivalent to:

$$3n(n+1)^2(2n+3) + (2n+1)(2n+3) - 3(n+1)^3(2n+1) \geq 0.$$

Now the left-hand side equals:

$$\begin{aligned}
&3(n+1)^2(n(2n+3) - (n+1)(2n+1)) + (2n+1)(2n+3) \\
&= 3(n+1)^2(2n^2 + 3n - 2n^2 - 3n - 1) + (2n+1)(2n+3) \\
&= (2n+1)(2n+3) - 3(n+1)^2 = n^2 + 2n,
\end{aligned}$$

which is clearly positive for $n \in \mathbb{N}^*$. Thus,

$$\frac{3(n+1)}{2n+3} \leq \sum_{k=1}^{n+1} \frac{1}{k^2} \leq 2 - \frac{1}{n+1},$$

hence P_{n+1}.
In conclusion, by the principle of induction,

$$\forall n \in \mathbb{N}^*,\ \frac{3n}{2n+1} \leq \sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}.$$

Solution to Exercise 34:

We reason by induction by establishing for $n \in \mathbb{N}$ the property P_n: $\forall x \in \mathbb{R},\ |\sin(nx)| \leq n|\sin(x)|$.
We clearly have $\forall x \in \mathbb{R},\ |\sin(0 \times x)| = 0 \leq 0 \times |\sin(x)| = 0$ hence P_0.
Suppose P_n for a given $n \in \mathbb{N}$.
We know that $\forall x, y \in \mathbb{R},\ \sin(x+y) = \sin(x)\cos(y) + \sin(y)\cos(x)$, hence:

$$\forall x \in \mathbb{R},\ |\sin((n+1)x)| = |\sin(nx)\cos(x) + \sin(x)\cos(nx)|.$$

But by the triangular inequality, this is less than or equal to:

$$|\sin(nx)||\cos(x)| + |\sin(x)||\cos(nx)|.$$

But by the induction hypothesis, $\forall x \in \mathbb{R},\ |\sin(nx)| \leq n|\sin(x)|$.
By bounding $|\cos(x)|$ and $|\cos(nx)|$ above by 1 in the above expression, we obtain:

$$\forall x \in \mathbb{R},\ |\sin((n+1)x)| \leq n|\sin(x)| + |\sin(x)| = (n+1)|\sin(x)|,$$

hence P_{n+1}.
Thus, by the principle of induction:

$$\forall x \in \mathbb{R},\ \forall n \in \mathbb{N},\ |\sin(nx)| \leq n|\sin(x)|.$$

Solution to Exercise 35:

Let us detail the draft reasoning that will lead us to set the correct induction hypothesis.
We begin by calculating the successive derivatives of ln:

$$\forall x \in \mathbb{R}^{+*},\ (\ln)'(x) = \frac{1}{x}$$
$$\forall x \in \mathbb{R}^{+*},\ (\ln)''(x) = \frac{-1}{x^2}$$
$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(3)}(x) = \frac{2}{x^3}$$
$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(4)}(x) = \frac{-6}{x^4}$$

It would seem that:

$$\forall n \in \mathbb{N}^*,\ \exists u_n \in \mathbb{N},\ \forall x \in \mathbb{R}^{+*},\ (\ln)^{(n)}(x) = \frac{(-1)^{n+1}u_n}{x^n}.$$

Manifestly, $u_1 = 1$. If n is any nonzero natural integer, we have on the one hand:

$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(n+1)}(x) = \frac{(-1)^{n+2}u_{n+1}}{x^{n+1}},$$

but also:

$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(n+1)}(x) = ((\ln)^{(n)})'(x) = \frac{(-1)^{n+2} n u_n}{x^{n+1}},$$

(we differentiated the conjectured expression of $\ln^{(n)}$).
Thus, (u_n) would verify $u_1 = 1$ and $\forall n \in \mathbb{N}^*,\ u_{n+1} = n u_n$. We deduce that $\forall n \in \mathbb{N}^*,\ u_n = (n-1)!$.

Hence, we establish for $n \geq 1$ the property P_n:

$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(n)}(x) = \frac{(-1)^{n+1}(n-1)!}{x^n}.$$

From the computations at the beginning, P_1 is true.
Suppose P_n for a given $n \in \mathbb{N}^*$. Then,

$$\forall x \in \mathbb{R}^{+*},\ (\ln)^{(n+1)}(x) = \frac{-(-1)^{n+1}(n-1)!n}{x^{n+1}} = \frac{(-1)^{n+2} n!}{x^{n+1}},$$

hence P_{n+1}.
Thus, by the principle of induction:

$$\forall n \in \mathbb{N}^*,\ \forall x \in \mathbb{R}^{+*},\ (\ln)^{(n)}(x) = \frac{(-1)^{n+1}(n-1)!}{x^n}.$$

Solution to Exercise 36:
We reason by induction by establishing for $n \in \mathbb{N}$ the property P_n:

$$\forall x, y \in \mathbb{R},\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

For $n = 0$, we have:

$$\forall x, y \in \mathbb{R},\ (x+y)^0 = 1 = \binom{0}{0} x^0 y^0,$$

hence P_0.
Suppose P_n for a given $n \in \mathbb{N}$. Then:

$$\forall x, y \in \mathbb{R},\ (x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$

where we used the induction hypothesis in the last equality.
But:

$$\begin{aligned}(x+y)\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} &= x\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} + y\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\\ &= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}.\end{aligned}$$

By making a change of variable $j = k+1$ in the left sum and isolating the last term, we have:

$$\sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} = \sum_{j=1}^{n+1} \binom{n}{j-1} x^j y^{n+1-j} = x^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} x^k y^{n+1-k}.$$

Moreover, isolating the first term of the right sum:

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} = y^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k}.$$

Hence:

$$\begin{aligned}(x+y)^{n+1} &= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1}\right) x^k y^{n+1-k} \\ &= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k},\end{aligned}$$

where we used Pascal's identity recalled in the prerequisites at the penultimate equality.
Thus, P_{n+1} is true.
In conclusion, by the principle of induction,

$$\forall x, y \in \mathbb{R},\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

For culture, let us cite its analogue for the differentiation of $\mathscr{C}^n$ functions, called *Leibniz's formula*, which can be proven in the same way:

$$\text{For all functions of class } \mathscr{C}^n,\ (fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

Solution to Exercise 37:
Note that f is well-defined because $\forall x \in \mathbb{R},\ 1 + cx^2 > 0$ since $c > 0$.
To get an idea of the formula to conjecture, let us compute $f \circ f$:

$$\forall x \in \mathbb{R},\ f \circ f(x) = \frac{f(x)}{\sqrt{1 + cf(x)^2}} = \frac{x}{\sqrt{1+cx^2}} \times \frac{1}{\sqrt{1 + c\frac{x^2}{1+cx^2}}}.$$

$$= \frac{x}{\sqrt{1+cx^2}} \times \sqrt{\frac{1+cx^2}{1+2cx^2}} = \frac{x}{\sqrt{1+2cx^2}}.$$

We are then naturally led to establish for $n \in \mathbb{N}$ the property P_n:

$$\forall x \in \mathbb{R},\ f^n(x) = \frac{x}{\sqrt{1+ncx^2}}.$$

By convention, f^0 is the identity, thus:

$$\forall x \in \mathbb{R},\ f^0(x) = x = \frac{x}{\sqrt{1 + 0 \times cx^2}},$$

hence P_0.
Suppose P_n for a given $n \in \mathbb{N}$. Then,

$$\forall x \in \mathbb{R},\ f^{n+1}(x) = f(f^n(x)) = \frac{f^n(x)}{\sqrt{1 + cf^n(x)^2}} = \frac{x}{\sqrt{1 + ncx^2}} \times \frac{1}{\sqrt{1 + c\frac{x^2}{1+ncx^2}}}.$$

$$= \frac{x}{\sqrt{1 + ncx^2}} \times \frac{\sqrt{1 + ncx^2}}{\sqrt{1 + (n+1)cx^2}} = \frac{x}{\sqrt{1 + (n+1)cx^2}},$$

hence P_{n+1}.
Thus, by the principle of induction:

$$\forall n \in \mathbb{N},\ \forall x \in \mathbb{R},\ f^n(x) = \frac{x}{\sqrt{1 + ncx^2}}.$$

Solution to Exercise 38:
We reason by induction (double) by establishing for $n \in \mathbb{N}$ the property P_n: $u_n = 2^n + 3^n$.
$2^0 + 3^0 = 2 = u_0$ hence P_0 is true.
$2^1 + 3^1 = 5 = u_1$ hence P_1 is true.
Suppose P_n and P_{n+1} for a given $n \in \mathbb{N}$. Then,

$$u_{n+2} = 5u_{n+1} - 6u_n = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n).$$

$$= 2^n(10 - 6) + 3^n(15 - 6) = 2^{n+2} + 3^{n+2},$$

hence P_{n+2}.
Thus, $\forall n \in \mathbb{N},\ u_n = 2^n + 3^n$.

Solution to Exercise 39:
We reason by induction (double) by establishing for $n \in \mathbb{N}$ the property P_n: $u_n = 2^{n+1} - 1$.
$2^{0+1} - 1 = 1 = u_0$ hence P_0 is true.
$2^{1+1} - 1 = 3 = u_1$ hence P_1 is true.
Suppose P_n and P_{n+1} for a given $n \in \mathbb{N}$. Then,

$$u_{n+2} = 3u_{n+1} - 2u_n = 3(2^{n+2} - 1) - 2(2^{n+1} - 1) = 2^{n+1}(6 - 2) - 1 = 2^{n+3} - 1,$$

hence P_{n+2}.
Thus, $\forall n \in \mathbb{N},\ u_n = 2^{n+1} - 1$.

Solution to Exercise 40:
We reason by contradiction by assuming that $\{i \in [\![n, m]\!],\ \neg P_i\}$ is non-empty; let us denote by i_0 its

smallest element (it exists because it is a set of integers). Then, $i_0 > n$ because P_n is true, hence $i_0 - 1 \in [\![n, m-1]\!]$. By minimality of i_0, P_{i_0-1} is necessarily true, but then P_{i_0} is also true because $P_{i_0-1} \implies P_{i_0}$: this is absurd.
Thus, $\forall k \in [\![n, m]\!],\ P_k$ is true.

Solution to Exercise 41:
Let us denote $\Delta_n = F_{n-1}F_{n+1} - F_n^2$ for $n \in \mathbb{N}^*$.
Let us compute Δ_n for some values of n:

$$\Delta_1 = F_0F_2 - F_1^2 = 0 \times 2 - 1 = -1$$

$$\Delta_2 = F_1F_3 - F_2^2 = 1 \times 2 - 1 = 1$$

$$\Delta_3 = F_2F_4 - F_3^2 = 1 \times 3 - 4 = -1$$

It would seem that $(\Delta_n) = ((-1)^n)$, which would imply that $(\Delta_{n+1}) = (-\Delta_n)$. Let us try to show it. We have:

$$\forall n \in \mathbb{N}^*,\ \Delta_{n+1} = F_nF_{n+2} - F_{n+1}^2.$$

We want to make Δ_n appear, thus make $F_{n-1}F_n$ and F_n^2 appear. We will therefore replace F_{n+2} by $F_{n+1} + F_n$ to make F_n^2 appear, then F_n by $F_{n+1} - F_{n-1}$ to make $F_{n-1}F_n$ appear. Then:

$$\forall n \in \mathbb{N}^*,\ \Delta_{n+1} = F_n(F_{n+1} + F_n) - F_{n+1}^2 = F_nF_{n+1} + F_n^2 - F_{n+1}^2$$

$$= (F_{n+1} - F_{n-1})F_{n+1} + F_n^2 - F_{n+1}^2 = F_n^2 - F_{n-1}F_{n+1}$$

$$= -\Delta_n.$$

Thus, (Δ_n) is a geometric sequence of ratio -1 and of first term -1, hence $\forall n \in \mathbb{N}^*,\ \Delta_n = (-1)^n$.
Therefore:

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} \frac{(-1)^{k+1}}{F_kF_{k+1}} = \sum_{k=1}^{n} \frac{\Delta_{k+1}}{F_kF_{k+1}} = \sum_{k=1}^{n} \frac{F_kF_{k+2} - F_{k+1}^2}{F_kF_{k+1}}.$$

$$= \sum_{k=1}^{n} \left(\frac{F_{k+2}}{F_{k+1}} - \frac{F_{k+1}}{F_k} \right) = \frac{F_{n+2}}{F_{n+1}} - 1.$$

Now, as seen in the course, denoting $\varphi = \frac{1+\sqrt{5}}{2}$ and $\tilde{\varphi} = \frac{1-\sqrt{5}}{2}$, we have $\forall n \in \mathbb{N},\ F_n = \frac{\varphi^n - \tilde{\varphi}^n}{\sqrt{5}}$ and thus:

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} \frac{(-1)^{k+1}}{F_kF_{k+1}} = \frac{\varphi^{n+2} - \tilde{\varphi}^{n+2}}{\varphi^{n+1} - \tilde{\varphi}^{n+1}} - 1 = \frac{\varphi - \frac{\tilde{\varphi}^{n+2}}{\varphi^{n+1}}}{1 - \frac{\tilde{\varphi}^{n+1}}{\varphi^{n+1}}} - 1.$$

Now,

$$\lim_{n\to\infty} \tilde{\varphi}^n = 0 \text{ since } |\tilde{\varphi}| < 1 \text{ and } \lim_{n\to\infty} \varphi^n = +\infty,$$

hence:

$$\lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{(-1)^{k+1}}{F_kF_{k+1}} \right) = \varphi - 1 = \frac{\sqrt{5}-1}{2}.$$

Solution to Exercise 42:
We establish for $m \in [\![2, N]\!]$ the property P_m:

$$\sqrt{m\sqrt{(m+1)\sqrt{\dots\sqrt{N}}}} < m+1,$$

which we will prove by downward induction.
If $m = N$, it amounts to showing that $\sqrt{N} < N+1$, which is equivalent to $N < N^2 + 2N + 1$ or again to $N^2 + N + 1 > 0$, which is obviously true. Thus, P_N is true.
Suppose P_m for a given $m \in [\![3, N]\!]$ and let us show that P_{m-1} is true. We have:

$$\sqrt{m\sqrt{(m+1)\sqrt{\dots\sqrt{N}}}} < m+1,$$

thus:

$$\sqrt{(m-1)\sqrt{m\sqrt{(m+1)\sqrt{\dots\sqrt{N}}}}} < \sqrt{(m-1)(m+1)}.$$

It is therefore sufficient to show that $\sqrt{(m-1)(m+1)} \leq m$, which is equivalent to $m^2 - 1 \leq m^2$, an inequality which is clearly true.
Therefore:

$$\sqrt{(m-1)\sqrt{m\sqrt{(m+1)\sqrt{\dots\sqrt{N}}}}} < \sqrt{(m-1)(m+1)} \leq m,$$

hence P_{m-1}.
Thus, by the principle of (downward) induction, the property is true for all $m \in [\![2, N]\!]$. In particular, for $m = 2$, we obtain:

$$\sqrt{2\sqrt{3\sqrt{\dots\sqrt{N}}}} < 3.$$

It would have been more complicated to show this result by induction on N. Here, the good idea to obtain this result was indeed to prove the first proposition, stronger but simpler to demonstrate!

Solution to Exercise 43:
Let $\alpha, \beta \in \mathbb{R}$. Let us show that $(\alpha\lambda^n + \beta\mu^n) \in E$.

$$\forall n \in \mathbb{N},\ a(\alpha\lambda^{n+1} + \beta\mu^{n+1}) + b(\alpha\lambda^n + \beta\mu^n) = \alpha(a\lambda^{n+1} + b\lambda^n) + \beta(a\mu^{n+1} + b\mu^n).$$

Now, λ and μ are solutions of $x^2 = ax + b$, hence solutions of $x^{n+2} = ax^{n+1} + bx^n$ after multiplication by x^n for $n \in \mathbb{N}$. Thus:

$$\forall n \in \mathbb{N},\ a(\alpha\lambda^{n+1} + \beta\mu^{n+1}) + b(\alpha\lambda^n + \beta\mu^n) = \alpha\lambda^{n+2} + \beta\mu^{n+2},$$

which proves that $(\alpha\lambda^n + \beta\mu^n) \in E$, and this whatever $\alpha, \beta \in \mathbb{R}$.

Let us now show that E is included in the set of sequences of the form $(\alpha\lambda^n + \beta\mu^n)$. Let $u \in E$. We seek $\alpha, \beta \in \mathbb{R}$ such that $u_0 = \alpha + \beta$ and $u_1 = \alpha\lambda + \beta\mu$. Why so? Because this will allow us to

initialize our double induction (u_0 and u_1 will already be of the form $\alpha\lambda^n + \beta\mu^n$).
We are thus led to solve a system of two equations with two unknowns.
We have:

$$\begin{cases} u_0 = \alpha + \beta \\ u_1 = \alpha\lambda + \beta\mu \end{cases}$$

That is to say:

$$\begin{cases} \alpha = \frac{u_1 - \mu u_0}{\lambda - \mu} \\ \beta = \frac{\lambda u_0 - u_1}{\lambda - \mu} \end{cases}$$

We can divide by $\lambda - \mu$ because $\lambda \neq \mu$ by hypothesis.
Thus, such α, β exist. Let us then prove by (double) induction the property P_n defined for $n \in \mathbb{N}$ by:

$$u_n = \alpha\lambda^n + \beta\mu^n.$$

$u_0 = \alpha + \beta = \alpha\lambda^0 + \beta\mu^0$ hence P_0.
$u_1 = \alpha\lambda + \beta\mu = \alpha\lambda^1 + \beta\mu^1$ hence P_1.
Suppose P_n and P_{n+1} for a given $n \in \mathbb{N}$. Since $u \in E$:

$$\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n.$$

Using the induction hypothesis,

$$\forall n \in \mathbb{N},\ u_{n+2} = a(\alpha\lambda^{n+1} + \beta\mu^{n+1}) + b(\alpha\lambda^n + \beta\mu^n) = \alpha(a\lambda^{n+1} + b\lambda^n) + \beta(a\mu^{n+1} + b\mu^n).$$

$$= \alpha\lambda^{n+2} + \beta\mu^{n+2},$$

hence P_{n+2}.
Thus, by the principle of induction:

$$\forall n \in \mathbb{N},\ u_n = \alpha\lambda^n + \beta\mu^n.$$

And in conclusion, we have indeed shown by double inclusion that $E = \{(\alpha\lambda^n + \beta\mu^n), \alpha, \beta \in \mathbb{R}\}$.

Solution to Exercise 44:

Let us first show that sequences of the form $((\alpha + \beta n)\lambda^n)$, where $\alpha, \beta \in \mathbb{R}$, are in E.
We have:

$$\forall n \in \mathbb{N},\ b(\alpha + \beta n)\lambda^n + a(\alpha + \beta(n+1))\lambda^{n+1} = \alpha(a\lambda^{n+1} + b\lambda^n) + \beta(bn\lambda^n + a(n+1)\lambda^{n+1}).$$

$$= \alpha\lambda^{n+2} + \beta(n(b\lambda^n + a\lambda^{n+1}) + a\lambda^{n+1}) = \alpha\lambda^{n+2} + \beta n\lambda^{n+2} + \beta a\lambda^{n+1}.$$

All these equalities being a consequence of the fact that $\lambda^2 = a\lambda + b$ hence $\lambda^{n+2} = a\lambda^{n+1} + b\lambda^n$.
Now, λ is a double root of $X^2 - aX - b$, hence $\lambda = \frac{a}{2}$, thus $a\lambda^{n+1} = \frac{a^{n+2}}{2^{n+1}} = 2\lambda^{n+2}$, whence:

$$\forall n \in \mathbb{N},\ b(\alpha + \beta n)\lambda^n + a(\alpha + \beta(n+1))\lambda^{n+1} = \alpha\lambda^{n+2} + \beta n\lambda^{n+2} + 2\beta\lambda^{n+2} = (\alpha + (n+2)\beta)\lambda^{n+2},$$

which proves that $((\alpha + \beta n)\lambda^n) \in E$.

Let us show that conversely, all sequences verifying $\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n$ are of the form $((\alpha + \beta n)\lambda^n)$ where $\alpha, \beta \in \mathbb{R}$. Let u be a sequence verifying such a recurrence relation.

We take inspiration from the previous exercise by seeking $\alpha, \beta \in \mathbb{R}$ such that $u_0 = \alpha$ and $u_1 = (\alpha+\beta)\lambda$ (seeking them in this way will allow us to initialize the double induction), which immediately leads us to set $\alpha = u_0$ and $\beta = \frac{u_1}{\lambda} - \alpha$ (we can because $\lambda \neq 0$).

We now establish for $n \in \mathbb{N}$ the property P_n: $u_n = (\alpha + \beta n)\lambda^n$.
By construction of α and β, P_0 and P_1 are true.
Suppose P_n and P_{n+1} for a given $n \in \mathbb{N}$. Then:

$$u_{n+2} = au_{n+1} + bu_n = a(\alpha + \beta(n+1))\lambda^{n+1} + b(\alpha+\beta n)\lambda^n = (\alpha + (n+2)\beta)\lambda^{n+2},$$

from the previous computations. Thus, P_{n+2} is true.
Therefore, by the principle of induction:

$$\forall n \in \mathbb{N},\ u_n = (\alpha+\beta n)\lambda^n.$$

We have thus shown that if $X^2 - aX - b$ has a nonzero double root, the set of sequences verifying $\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n$ is exactly $\{((\alpha+\beta n)\lambda^n), \alpha, \beta \in \mathbb{R}\}$.

Solution to Exercise 45:
Let us show that if $n \in \mathbb{N}$ is written $\sum_{k=0}^{\infty} \varepsilon_k 2^k$ with the ε_k in $\{0; 1\}$ then this sum is finite.
Let m be a natural integer such that $2^m > n$ (it exists because $2^m \to \infty$). Then, $\forall i \geq m,\ \varepsilon_i = 0$ because if there existed $k \geq m$ such that $\varepsilon_k = 1$ then we would have:

$$n = \sum_{k=0}^{\infty} \varepsilon_k 2^k \geq 2^i \geq 2^m > n,$$

which is absurd.
Thus, this sum is finite.

Let us begin with the uniqueness of such a sequence. Suppose that n is written:

$$n = \sum_{k=0}^{\infty} \varepsilon_k 2^k = \sum_{k=0}^{\infty} \tilde{\varepsilon}_k 2^k,$$

and let us show that $(\varepsilon_k) = (\tilde{\varepsilon}_k)$.
Suppose the contrary and let p be the smallest index such that $\varepsilon_p \neq \tilde{\varepsilon}_p$ (this one exists because then the set of indices k such that $\varepsilon_k \neq \tilde{\varepsilon}_k$ is a non-empty subset of $\mathbb{N}$).
We then have, after simplification of the common terms:

$$\sum_{k=p}^{\infty} \varepsilon_k 2^k = \sum_{k=p}^{\infty} \tilde{\varepsilon}_k 2^k,$$

that is, dividing by 2^{p+1}:

$$\frac{\varepsilon_p}{2} + \sum_{k=p+1}^{\infty} \varepsilon_k 2^{k-p-1} = \frac{\tilde{\varepsilon}_p}{2} + \sum_{k=p+1}^{\infty} \tilde{\varepsilon}_k 2^{k-p-1}.$$

Now the right-hand term on each side of the equality is an integer, while the left-hand term is smaller than $\frac{1}{2}$. We deduce that by taking the integer part we obtain:

$$\sum_{k=p+1}^{\infty} \varepsilon_k 2^{k-p-1} = \sum_{k=p+1}^{\infty} \tilde{\varepsilon}_k 2^{k-p-1},$$

and thus:

$$\sum_{k=p+1}^{\infty} \varepsilon_k 2^{k} = \sum_{k=p+1}^{\infty} \tilde{\varepsilon}_k 2^{k},$$

whence returning to the starting equality:

$$\varepsilon_p = \tilde{\varepsilon}_p,$$

which is absurd.
Thus, $(\varepsilon_k) = (\tilde{\varepsilon}_k)$ and such a writing is unique.

Let us now deal with existence.
We establish for $n \in \mathbb{N}$ the property P_n:

$$\exists(\varepsilon_k) \in \{0;1\}^{\mathbb{N}},\ n = \sum_{k=0}^{\infty} \varepsilon_k 2^k,$$

which we will prove by (strong) induction.
For $n = 0$, it suffices to consider $(\varepsilon_k) = (0)$ (the identically zero sequence). Thus, P_0 is true.
For the needs of our induction (see below) we need to initialize up to 1: for $n = 1$, the sequence (ε_k) defined by $\varepsilon_0 = 1$ and $\forall k \geq 1,\ \varepsilon_k = 0$ works, hence P_1.
Suppose $P_0, \ldots, P_n$ are true for a given $n \in \mathbb{N}^*$.
We distinguish according to the parity of n.
If n is even: by the induction hypothesis,

$$\exists(\varepsilon_k) \in \{0;1\}^{\mathbb{N}},\ n = \sum_{k=0}^{\infty} \varepsilon_k 2^k,$$

but since n is even, $\varepsilon_0 = 0$. Considering the sequence $(\tilde{\varepsilon}_k)$ defined by $\tilde{\varepsilon}_0 = 1$ and $\forall k \geq 1,\ \tilde{\varepsilon}_k = \varepsilon_k$ we obtain:

$$n + 1 = \sum_{k=0}^{\infty} \tilde{\varepsilon}_k 2^k,$$

hence P_{n+1}.
If n is odd, $n+1$ is even. We would like to apply the induction hypothesis to $\frac{n+1}{2}$ but we must make sure that $\frac{n+1}{2} \leq n$ and thus that $n \geq 1$: this is why we initialized up to 1!
We apply the induction hypothesis to $\frac{n+1}{2}$:

$$(\varepsilon_k) \in \{0;1\}^{\mathbb{N}},\ \frac{n+1}{2} = \sum_{k=0}^{\infty} \varepsilon_k 2^k,$$

and thus:

$$n + 1 = \sum_{k=0}^{\infty} \varepsilon_k 2^{k+1} = \sum_{k=1}^{\infty} \varepsilon_{k-1} 2^k,$$

and thus by setting $\tilde{\varepsilon}_0 = 0$ and $\forall k \geq 1,\ \tilde{\varepsilon}_k = \varepsilon_{k-1}$, the sequence $(\tilde{\varepsilon}_k)$ works, hence P_{n+1}.
Thus, by the principle of induction:

$$\forall n \in \mathbb{N},\ \exists(\varepsilon_k) \in \{0;1\}^{\mathbb{N}},\ n = \sum_{k=0}^{\infty} \varepsilon_k 2^k.$$

Solution to Exercise 46:
We establish for $n \in \mathbb{N}$ the property P_n:

$$v_n = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n}{k} u_k.$$

By hypothesis, we know that $u_0 = \binom{0}{0} = v_0$ hence indeed $v_0 = (-1)^0 \times (-1)^0 \binom{0}{0} u_0 = u_0$: P_0 is true.
Suppose $P_0, \ldots, P_n$ for a given $n \in \mathbb{N}$. Then:

$$(-1)^{n+1} \sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} u_k = (-1)^{n+1} \sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} \sum_{j=0}^{k} \binom{k}{j} v_j = (-1)^{n+1} \sum_{k=0}^{n+1} \sum_{j=0}^{k} (-1)^k \binom{n+1}{k} \binom{k}{j} v_j,$$

by definition of u.
Let us follow our legendary instinct and interchange the two sums:

$$(-1)^{n+1} \sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} u_k = (-1)^{n+1} \sum_{j=0}^{n+1} \sum_{k=j}^{n+1} (-1)^k \binom{n+1}{k} \binom{k}{j} v_j.$$

We find ourselves stuck because the second sum is over k but one of the terms is $\binom{k}{j}$, and we do not quite know how to sum binomial coefficients when it is the upper index that varies. Let us make it disappear to make $\binom{n+1-j}{k-j}$ appear which will greatly facilitate the computation of the sum on the right after a change of index $l = k - j$. We remark that:

$$\binom{n+1}{k}\binom{k}{j} = \frac{(n+1)!}{k!(n+1-k)!} \times \frac{k!}{j!(k-j)!} = \frac{(n+1)!}{j!(n+1-j)!} \times \frac{(n+1-j)!}{(k-j)!(n+1-j-(k-j))!}.$$

$$= \binom{n+1}{j}\binom{n+1-j}{k-j},$$

and therefore:

$$(-1)^{n+1} \sum_{j=0}^{n+1} \sum_{k=j}^{n+1} (-1)^k \binom{n+1}{k} \binom{k}{j} v_j = (-1)^{n+1} \sum_{j=0}^{n} \binom{n+1}{j} v_j \sum_{k=j}^{n+1} (-1)^k \binom{n+1-j}{k-j}.$$

After performing the change of index $l = k - j$,

$$(-1)^{n+1} \sum_{j=0}^{n+1} \binom{n+1}{j} v_j \sum_{k=j}^{n+1} (-1)^k \binom{n+1-j}{k-j} = (-1)^{n+1} \sum_{j=0}^{n+1} \binom{n+1}{j} v_j \sum_{l=0}^{n+1-j} (-1)^{l+j} \binom{n+1-j}{l}.$$

$$= (-1)^{n+1} \sum_{j=0}^{n+1} (-1)^j \binom{n+1}{j} v_j \sum_{l=0}^{n+1-j} (-1)^l \binom{n+1-j}{l}.$$

Now, by the binomial theorem,

$$\sum_{l=0}^{n+1-j} (-1)^l \binom{n+1-j}{l} = (1-1)^{n+1-j},$$

which equals 0 if $j \neq n+1$ and 1 otherwise.
Thus, only remains:

$$(-1)^{n+1} \times (-1)^{n+1} \binom{n+1}{n+1} v_{n+1} = v_{n+1},$$

and therefore:

$$(-1)^{n+1} \sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} u_k = v_{n+1},$$

hence P_{n+1}.
Thus, by the principle of induction:

$$\forall n \in \mathbb{N},\ v_n = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n}{k} u_k.$$

Solution to Exercise 47:

When approaching the exercise, we notice that the proposition concerns two variables p and q. We then wonder which induction to do in order to combine the two. We could denote the property $P_{p,q}$ and try to show that $P_{p,q}$ implies $P_{p+1,q}$ and $P_{p,q+1}$ (show that this is legitimate!), or we could reason by induction on the value $p+q$ (we invite the reader to try these methods), or else get rid of the dependence in q by including it directly in the property to be proved, by stating the property Q_p:

$$\forall q \in \mathbb{N},\ F_p F_{q+1} + F_{p-1} F_q = F_{p+q}.$$

We indeed have $\forall q \in \mathbb{N},\ F_1 F_{q+1} + F_0 F_q = 1 \times F_{q+1} + 0 \times F_q = F_{q+1}$ hence Q_1.
Suppose Q_p for a given $p \in \mathbb{N}^*$. By the induction hypothesis,

$$\forall q \in \mathbb{N},\ F_p F_{q+1} + F_{p-1} F_q = F_{p+q},$$

and we would like to show that:

$$\forall q \in \mathbb{N},\ F_{p+1} F_{q+1} + F_p F_q = F_{p+1+q}.$$

Since the first property is true whatever $q \in \mathbb{N}$, we can take any $q \in \mathbb{N}$ and apply it to $q+1$. We obtain:

$$F_{p+(q+1)} = F_{p+1+q} = F_p F_{q+2} + F_{p-1} F_{q+1}.$$

It remains to make disappear what we do not want and make appear what we want by using that $F_{q+2} = F_{q+1} + F_q$ and $F_{p-1} = F_{p+1} - F_p$:

$$F_{p+1+q} = F_p(F_{q+1} + F_q) + (F_{p+1} - F_p) F_{q+1} = F_p F_q + F_{p+1} F_{q+1},$$

hence Q_{p+1}.
Thus, by the principle of induction:

$$\forall p \in \mathbb{N}^*,\ \forall q \in \mathbb{N},\ F_p F_{q+1} + F_{p-1} F_q = F_{p+q}.$$

Solution to Exercise 48:
When approaching the exercise roughly, we feel that the parity of n is going to be a problem. Indeed, if we write $H_n = \frac{p_n}{q_n}$ with p_n odd and q_n even, then $H_{n+1} = H_n + \frac{1}{n+1} = \frac{(n+1)p_n + q_n}{(n+1)q_n}$.
Since q_n is even, $(n+1)q_n$ is so. However, the numerator has the parity of $n+1$, because p_n is odd: we thus feel that we are going to have to reason on the parity of n within the induction.

We establish for $n \geq 2$ the property P_n:

$$\exists p_n, q_n \in \mathbb{N},\ p_n \text{ odd},\ q_n \text{ even},\ H_n = \frac{p_n}{q_n},\ \text{GCD}(p_n, q_n) = 1.$$

For $n = 2$, $H_2 = \frac{3}{2}$: P_2 is true.
Suppose $P_2, \ldots, P_n$ for a given $n \geq 2$. Following our preliminary remark, we distinguish the parity of n.
If n is even: we saw that $H_{n+1} = \frac{(n+1)p_n + q_n}{(n+1)q_n}$ with numerator odd and denominator even. To conclude that in this case P_{n+1} is true, it remains that this fraction be in irreducible form. The only problem would be that the denominator or numerator change parity after division by the GCD of these two numbers (i.e. reduction to lowest terms). Now since they are of opposite parity, their GCD is odd, and thus the parity of these two numbers does not change after division by their GCD (if m is written kl with k odd then m has the parity of l).
Thus, in this case P_{n+1} is true.
Suppose n odd and write it in the form $2k+1$. This time, it is a bit more complicated. The idea is to separate even and odd indices in the sum defining H_{n+1} so as to make appear on the one hand a fraction whose denominator is odd as a product of odds, and to use the induction hypothesis on the other hand (this work being done on rough paper, we will beforehand have noticed the necessity to set a strong induction). We have:

$$H_{n+1} = H_{2k+2} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2k+2} = \left(1 + \frac{1}{3} + \cdots + \frac{1}{2k+1}\right) + \left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2k+2}\right).$$

By factoring $\frac{1}{2}$ in the right sum, we notice that $H_{k+1} = H_{\frac{n+1}{2}}$ appears:

$$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2k+2} = \frac{1}{2}\left(1 + \frac{1}{2} + \cdots + \frac{1}{k+1}\right) = \frac{H_{k+1}}{2} = \frac{H_{\frac{n+1}{2}}}{2}.$$

By the induction hypothesis, we can write H_{k+1} as a fraction $\frac{p_{k+1}}{q_{k+1}}$ which works.
On the other hand, if we put over the same denominator the left sum, we obtain a fraction of the form $\frac{A}{B}$ with B odd as a product of odds.
Thus,

$$H_{n+1} = \frac{A \times 2q_{k+1} + Bp_{k+1}}{2Bq_{k+1}}.$$

The numerator has the parity of Bp_{k+1} which is odd as a product of odd, the denominator is even. By virtue of the preceding remark, the parity of numerator and denominator does not change after reduction to lowest terms, hence P_{n+1} in this case.
Thus, by the principle of induction, the property is true for all $n \geq 2$.

Solution to Exercise 49:

We notice that the proposition is indeed proved by strong induction provided that we go back by iterating f: let us start from a value $n \in \mathbb{N}$ and suppose that for all values strictly less than n we fall back on 1 or 5 after a sufficient number of compositions by f. Then, if after m compositions of n by f we arrive at a number strictly less than n, we know that after a sufficient number of compositions of this number by f, say k, we fall back on 1 or 5: then, after $m+k$ compositions of n by f we fall back on 1 or 5.
We notice that if n is even, we immediately go back after one iteration by f, since $f(n) = \frac{n}{2} < n$ for $n \geq 1$.
If n is odd, then $f(n) = n+5$: we do not go back. However, $n+5$ is odd, and therefore $f(f(n)) = \frac{n+5}{2}$. Have we gone back? To know this, it suffices to solve the inequality $\frac{n+5}{2} < n$, which is verified for all $n \geq 6$. Thus, our reasoning by strong induction will only be applicable starting from $n = 6$, so we are going to have to initialize up to 6.

We establish for $n \in \mathbb{N}^*$ the property P_n:

$$\exists k \in \mathbb{N},\ f^k(n) \in \{1; 5\}.$$

For $n = 1$: $f(1) = 6$, $f(f(1)) = 3$, $f(f(f(1))) = 8 = 2^3$ and thus we deduce that $f^6(1) = 1$: P_1 is true.
For $n = 2$: $f(2) = 1$: P_2 is true.
For $n = 3$: $f(3) = 8 = 2^3$ hence $f^4(3) = 1$: P_3 is true.
For $n = 4$: $f^2(4) = 1$: P_4 is true.
For $n = 5$: $f^2(5) = 5$: P_5 is true.
For $n = 6$: $f(6) = 3$ hence with the previous calculations, $f^5(6) = 1$: P_6 is true.
Suppose $P_1, \ldots, P_n$ for a given $n \in \mathbb{N}^*$.
If n is odd, $f(n+1) = \frac{n+1}{2} \leq n$ (since $n \geq 1$), thus by the induction hypothesis,

$$\exists k \in \mathbb{N}^*,\ f^k\left(\frac{n+1}{2}\right) = f^k(f(n+1)) = f^{k+1}(n+1) \in \{1; 5\},$$

thus P_{n+1} is true.
If n is even, then if $n \leq 5$ we know that P_{n+1} is true. Otherwise, $n+1 \geq 6$ hence $f(f(n+1)) < n+1$ hence $f(f(n+1)) \leq n$ hence by the induction hypothesis,

$$\exists k \in \mathbb{N}^*,\ f^k(f(f(n+1))) = f^{k+2}(n+1) \in \{1; 5\},$$

whence P_{n+1}.
Thus, by the principle of induction, the property is true for all $n \in \mathbb{N}^*$.

Solution to Exercise 50:

Let us take inspiration from Exercise 45 by establishing for $n \in \mathbb{N}^*$ the property P_n:

$$\forall p \in \mathbb{N}^*,\ \sum_{k=0}^{n-1} k^p = \frac{1}{p+1} \sum_{k=0}^{p} \binom{p+1}{k} B_k n^{p+1-k}.$$

but let us immediately rewrite this last sum:

$$\forall p \in \mathbb{N}^*,\ \sum_{k=0}^{n-1} k^p = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}n^k.$$

For $n=1$:

$$\forall p \in \mathbb{N}^*,\ \sum_{k=0}^{1-1} k^p = 0,$$

since $p \geq 1$, and:

$$\forall p \in \mathbb{N}^*,\ \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k} = \frac{1}{p+1}\binom{p+1}{1}B_p + \frac{1}{p+1}\sum_{k=2}^{p+1}\binom{p+1}{k}B_{p+1-k}$$

$$= B_p + \frac{1}{p+1}\sum_{j=0}^{p-1}\binom{p+1}{j}B_j,$$

after change of index $j = p+1-k$.
By definition of the Bernoulli numbers, we indeed obtain 0: P_1 is true.
Suppose P_n for a given $n \geq 1$. By hypothesis,

$$\forall p \in \mathbb{N}^*,\ \sum_{k=0}^{n-1} k^p = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}n^k.$$

We are going to use the fact that this property is valid **for all** $p \in \mathbb{N}^*$ to show that:

$$\sum_{k=0}^{n} k^p = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}(n+1)^k,$$

where p is any given positive integer.
There is going to be quite a lot of computation, the important thing is to be organized. Let us compute:

$$\frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}(n+1)^k = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}\sum_{j=0}^{k}\binom{k}{j}n^j.$$

We want to interchange the sums, to do so we isolate the first term of the right sum so that the starting values of the indices are the same:

$$\frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}\sum_{j=0}^{k}\binom{k}{j}n^j = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}\left(1+\sum_{j=1}^{k}\binom{k}{j}n^j\right).$$

then we separate:

$$= \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k} + \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}\sum_{j=1}^{k}\binom{k}{j}n^j.$$

By P_0, the left sum is zero. From the computations done in Exercise 44,

$$\binom{p+1}{k}\binom{k}{j} = \binom{p+1}{j}\binom{p+1-j}{k-j},$$

whence:

$$\frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}\sum_{j=1}^{k}\binom{k}{j}n^j = \frac{1}{p+1}\sum_{j=1}^{p+1}\sum_{k=j}^{p+1}\binom{p+1}{k}B_{p+1-k}\binom{k}{j}n^j.$$

$$= \frac{1}{p+1}\sum_{j=1}^{p+1}\sum_{k=j}^{p+1}\binom{p+1}{j}\binom{p+1-j}{k-j}B_{p+1-k}n^j = \frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^j\sum_{k=j}^{p+1}\binom{p+1-j}{k-j}B_{p+1-k}.$$

then after change of index and isolating the first term of the right sum:

$$= \frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^j\sum_{k=0}^{p-j+1}\binom{p+1-j}{k}B_{p-j+1-k}.$$

$$= \frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^j\left(B_{p-j+1}+\sum_{k=1}^{p-j+1}\binom{p+1-j}{k}B_{p-j+1-k}\right).$$

$$= \frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^jB_{p+1-j} + \frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^j\sum_{k=1}^{p-j+1}\binom{p+1-j}{k}B_{p-j+1-k}.$$

By the induction hypothesis:

$$\frac{1}{p+1}\sum_{j=1}^{p+1}\binom{p+1}{j}n^jB_{p+1-j} = \sum_{k=0}^{n-1}k^p.$$

Let us now consider the right-hand term. In the right sum, if $p-j\neq 0$ we can substitute $p-j$ for p (because the property is valid for all non-zero p and we recognize the special case $n=1$) and obtain that:

$$\forall j\in [\![1;p+1]\!],\ j\neq p,\ \sum_{k=1}^{p+1-j}\binom{p+1-j}{k}B_{p+1-j-k} = \frac{1}{p-j+1}\sum_{k=0}^{1-1}k^p = 0,$$

since $p\geq 1$. Thus, only the term corresponding to $j=p$ is not zero, it equals:

$$\frac{1}{p+1}\binom{p+1}{p}n^pB_0 = n^p.$$

whence:

$$\frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}(n+1)^k = \sum_{k=0}^{n-1}k^p + n^p = \sum_{k=0}^{n}k^p,$$

hence P_{n+1} (finally!).

Thus, by the principle of induction:

$$\forall n\in\mathbb{N}^*,\ \forall p\in\mathbb{N}^*,\ \sum_{k=0}^{n-1}k^p = \frac{1}{p+1}\sum_{k=1}^{p+1}\binom{p+1}{k}B_{p+1-k}n^k.$$