

4.1 Polynomials as Coefficient Sequences

At school a polynomial is an expression such as $3x^2 - x + 2$, and x is a number that has not been chosen yet. This chapter replaces that picture by a definition that works over every commutative ring of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 2.3.1): over $\mathbb{Q}$, over the fields $\mathbb{F}_p$ of Chapter 2, and over rings such as $\mathbb{Z}/6\mathbb{Z}$, where a product of two non-zero elements can be zero. This section makes the one decision the whole chapter rests on: a polynomial **is** its list of coefficients. It then collects the finite sums, powers and multiples that the next sections compute with.

Throughout, R is a commutative ring, with $a - b := a + (-b)$.

4.1.1 What goes wrong with “an expression in x ”

Take the field $\mathbb{F}_2 = \{0, 1\}$ of Definition 2.2.1, in which $1 + 1 = 0$. Read $x^2 + x$ the school way, as a rule: replace x by an element c and compute $cc + c$. The tables of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$) give

$$0 \cdot 0 + 0 = 0, \quad 1 \cdot 1 + 1 = 1 + 1 = 0.$$

So the rule $c \mapsto cc + c$ and the rule $c \mapsto 0$ give the same output at both elements of $\mathbb{F}_2$. As functions $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ they are equal, by Sets, Relations, and Cardinality, Proposition 1.4.1: same domain, same codomain, same values.

If a polynomial were the function it defines, then $x^2 + x$ would be the zero polynomial over $\mathbb{F}_2$. So would $x^3 + x$ and $x^4 + x^2$, which also give 0 at 0 and $1 + 1 = 0$ at 1. None of them would have a highest power of x , and the rule “the degree of a product is the sum of the degrees”, which we want over every field, would fail for $x \cdot (x + 1) = x^2 + x$: degrees 1 and 1, product “zero”. Over $\mathbb{Q}$ the problem never shows (Section 5.4 proves that over an infinite field a non-zero polynomial never gives the zero function), which is why school algebra can afford the picture. Over a finite ring with $1 \neq 0$ it cannot.

So we decide the other way. Two polynomials are the same when their coefficients are the same, and the letter x is not a number at all.

A polynomial is its list of coefficients; the letter x only marks the positions.

4.1.2 Polynomials over a commutative ring

A list of coefficients that goes on forever is a sequence, that is, a function on $\mathbb{N}$. We keep only the sequences that stop being non-zero.

Definition 4.1.1. Polynomial

Let R be a commutative ring. A **polynomial over R** (in the indeterminate x) is a function $p: \mathbb{N} \rightarrow R$, written $p = (p_0, p_1, p_2, \dots)$, such that **only finitely many** p_k are non-zero: **there exists** $N \in \mathbb{N}$ with $p_k = 0$ **for every** $k > N$. Such an N is called **admissible** for p . The element p_k is the **coefficient of x^k** in p .

For $a \in R$ and $n \in \mathbb{N}$, the **monomial ax^n** is the polynomial with a in position n and 0 in every other position. We set $x := 1x^1$, and for $a \in R$ the **constant a** is the monomial ax^0 . The **zero polynomial** is $0 := (0, 0, 0, \dots)$. The set of all polynomials over R is written $R[x]$.

In words: the first clause says that a polynomial is an infinite list of elements of R , indexed from 0; the second says that from some position on, every entry is 0. The quantifiers are in the order “there is one N that works for every later k ”: a sequence with infinitely many non-zero entries, however sparse, is excluded. A monomial has at most one non-zero entry, so n is admissible for it, and it is a polynomial. The symbol x is the particular sequence $(0, 1, 0, 0, \dots)$: an element of $R[x]$, never an element of R , and never a variable that takes values.

Equality. Two polynomials $p, q \in R[x]$ are functions with the same domain $\mathbb{N}$ and the same codomain R . By Sets, Relations, and Cardinality, Proposition 1.4.1,

$$p = q \iff p_k = q_k \text{ for every } k \in \mathbb{N}.$$

To prove an identity between polynomials we therefore compute the k -th coefficient of both sides, for an arbitrary k . We call this move **compare coefficients**. It is *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2’s “reduce to the level below” once more: a statement about polynomials becomes a statement about elements of R , one position at a time.

The display. If N is admissible for p , we write

$$p = \sum_{k=0}^N p_k x^k = p_0 + p_1 x + p_2 x^2 + \cdots + p_N x^N.$$

For now this is **notation only**. No addition of polynomials has been defined yet, so the plus signs are not an operation: the display names the sequence by listing its entries, each with a marker x^k for its position. We drop terms whose coefficient is 0, write ax for ax^1 , a for ax^0 , x^k for $1x^k$, and $-ax^k$ for $(-a)x^k$. So $3x^2 - x + 2$ over $\mathbb{Q}$ names the sequence with $p_0 = 2$, $p_1 = -1$, $p_2 = 3$ and $p_k = 0$ for $k \geq 3$. Section 4.2 defines the sum of two polynomials and proves that the display is then an honest sum of monomials.

There is one thing to check about the display. The admissible N is not unique: if N is admissible, so is every $M \geq N$, since $k > M$ implies $k > N$. Passing from N to M only adds the terms $0x^k$ for $N < k \leq M$, which the convention drops. So every admissible N names the same sequence, and the display is well defined.

Why “only finitely many”. Two later uses need it. In Section 4.4 we put an element $c \in R$ in place of x and form $\sum_k p_k c^k$; in a ring only finite sums are defined, and finiteness is what makes the sum finite. In Section 4.3 every non-zero polynomial gets a degree, the highest position holding a non-zero coefficient; without finiteness there may be no highest position.

The degenerate cases. The zero polynomial has every N admissible, including $N = 0$, and it is the monomial $0x^n$ for every n . It is the one polynomial with no non-zero coefficient at all, and Section 4.3 will need a convention for its degree. At the other extreme, let R be the zero ring $\{0\}$ of the examples after *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Definition 2.3.1, where $1 = 0$. There is exactly one function $\mathbb{N} \rightarrow \{0\}$, so $R[x]$ has exactly one element, the zero polynomial, and $x = 1x^1 = 0x^1 = 0$. This is why some results below assume $1 \neq 0$ in R .

Example. Reading off coefficient sequences

Write the coefficient sequence of each polynomial, and check it against [Definition 4.1.1](#). In a ring $\mathbb{Z}/n\mathbb{Z}$, a natural number m written as an element stands for $m \cdot [1] = [m]$ (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 3.4.3 (d)), just as Definition 2.2.1 does for $\mathbb{F}_p$.

- (a) $3x^2 - x + 2 \in \mathbb{Q}[x]$.
- (b) $x^2 + x \in \mathbb{F}_2[x]$.
- (c) $[3]x + [4] \in (\mathbb{Z}/6\mathbb{Z})[x]$.

- (d) The constant 7, over $\mathbb{Z}$, over $\mathbb{Z}/5\mathbb{Z}$ and over $\mathbb{F}_2$.
 (e) $0 \in R[x]$, for any R .

Solution.

- (a) $(2, -1, 3, 0, 0, \dots)$. The entries lie in $\mathbb{Q}$, and $N = 2$ is admissible, so it is a polynomial over $\mathbb{Q}$.
 (b) $(0, 1, 1, 0, 0, \dots)$, with entries in $\mathbb{F}_2$ and $N = 2$ admissible. It is **not** the zero sequence, since its entry in position 1 is $1 \neq 0$. So $x^2 + x \neq 0$ in $\mathbb{F}_2[x]$, although the rule $c \mapsto cc + c$ is the zero function on $\mathbb{F}_2$, as computed above.
 (c) $([4], [3], [0], [0], \dots)$: the constant term comes first. The entries lie in $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2) and $N = 1$ is admissible.
 (d) Over $\mathbb{Z}$: $(7, 0, 0, \dots)$. Over $\mathbb{Z}/5\mathbb{Z}$: $([7], [0], [0], \dots)$, and $[7] = [2]$ because $7 - 2 = 5$ is a multiple of 5; so this is the constant $[2]$. Over $\mathbb{F}_2$: $(1, 0, 0, \dots)$, because $7 = 1$ in $\mathbb{F}_2$ ($7 - 1 = 6 = 3 \cdot 2$). The same symbol 7 names three different polynomials, one in each ring, and in each ring $N = 0$ is admissible.
 (e) $(0, 0, 0, \dots)$, with every N admissible: the degenerate case.

Now a non-example, by a minimal change. Start from $1 + x + x^2 \in \mathbb{Q}[x]$, the sequence $(1, 1, 1, 0, 0, \dots)$, and change every later 0 to 1. The result $(1, 1, 1, 1, \dots)$, informally “ $1 + x + x^2 + \dots$ ”, is still a function $\mathbb{N} \rightarrow \mathbb{Q}$. The one clause that fails is **only finitely many**: for every N , the entry in position $N + 1$ is $1 \neq 0$, so no N is admissible. It is a *formal power series*, met again in the exercises of Section 4.2, but not a polynomial. An expression such as $x^{-1} + 1$ fails for a more basic reason: it would need an entry in position -1 , and a polynomial is a function on $\mathbb{N}$.

$\mathbb{R}$ and $\mathbb{C}$ are commutative rings too (for $\mathbb{R}$, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5; for $\mathbb{C}$, Chapter 1), so $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are defined, and they are the main examples of the linear-algebra companion. No proof in this chapter needs them; our examples come from $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{F}_p$, the rings this series has built.

Where R matters. Nothing in Definition 4.1.1 mentions inverses, an order, or size. It makes sense word for word over $\mathbb{Z}/6\mathbb{Z}$, where $[2][3] = [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five)), and over the zero ring. The price is that school rules about polynomials cannot be assumed: each one that survives is proved, here or (division with remainder, counting roots) in Chapter 5, and each result says what it needs from R (nothing at all, no zero divisors, a unit leading coefficient, finiteness with $1 \neq 0$, or, for the derivative, the characteristic of a field).

Warning. p_2 is a coefficient; $p(2)$ will be a value. Section 4.4 writes $p(c)$ for the result of putting $c \in R$ in place of x . For $p = x^2 + 1 \in \mathbb{Z}[x]$, the coefficient p_2 is 1, while the value at 2 will be $2 \cdot 2 + 1 = 5$. Both are integers, so a reader who writes $p(k)$ for “the k -th coefficient” gets $1 = 5$. This book never writes $p(k)$ for a coefficient: the coefficient of x^k is p_k , always with a subscript.

Quick check. Is $6x^2$ equal to the zero polynomial in $(\mathbb{Z}/6\mathbb{Z})[x]$? In $\mathbb{Z}[x]$?

Solution. In $(\mathbb{Z}/6\mathbb{Z})[x]$, yes: $6x^2$ is the monomial $[6]x^2$, and $[6] = [0]$, so every entry is $[0]$ and the two sequences agree in every position. In $\mathbb{Z}[x]$, no: the entry in position 2 is $6 \neq 0$, while the zero polynomial has 0 there. Same display, two rings, two answers.

4.1.3 Sums, powers and multiples

The next section defines the product of two polynomials by a formula whose k -th coefficient is a finite sum $\sum_{i=0}^k p_i q_{k-i}$ of products in R . Later sections raise elements of R , and polynomials, to powers, and use multiples $k \cdot a$. This subsection collects what we use about all three. Most of it is already proved: finite sums and multiples in a commutative ring are Chapter 2's (Lemma 2.6.1, Lemma 2.5.1), and the recursions follow the patterns that *Sets, Relations, and Cardinality*, Section 2.3 set up for real numbers (Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2). The patterns are reused; no fact about $\mathbb{R}$ is.

One point deserves care before we start. The sums of polynomials in Section 4.2 must be formed **before** we know that $R[x]$ is a commutative ring, because they are used to prove it. So part (a) below asks for an addition and a left-neutral element 0, and nothing more.

Lemma 4.1.1. Finite Sums, Powers and Multiples

Let R be a commutative ring.

- (a) (*Sums.*) Let T be a set with a function $+: T \times T \rightarrow T$ and an element $0 \in T$ with $0 + u = u$ for every $u \in T$. For a sequence $(u_i)_{i \in \mathbb{N}}$ in T there is exactly one way to define $\sum_{i=0}^k u_i \in T$, for $k \in \mathbb{N}$, such that

$$\sum_{i=0}^0 u_i = u_0, \quad \sum_{i=0}^{k+1} u_i = \sum_{i=0}^k u_i + u_{k+1},$$

starting from the empty sum 0. The sum $\sum_{i=0}^k u_i$ depends only on $u_0, \dots, u_k$; so a finite list $u_0, \dots, u_k$ has a sum, computed from any extension of the list to a sequence. Likewise, a finite list $s_1, \dots, s_r$ in R has a **product** $\prod_{j=1}^r s_j$, with $\prod_{j=1}^0 s_j = 1$ and $\prod_{j=1}^{r+1} s_j = (\prod_{j=1}^r s_j) s_{r+1}$.

- (b) (*Rules for sums in R .*) For $k \in \mathbb{N}$, $c \in R$ and elements $u_i, v_i \in R$:
- ($\Sigma 1$) $\sum_{i=0}^k (u_i + v_i) = \sum_{i=0}^k u_i + \sum_{i=0}^k v_i$;
 - ($\Sigma 2$) $c \sum_{i=0}^k u_i = \sum_{i=0}^k c u_i$;
 - ($\Sigma 3$) for $j \in \mathbb{N}$: if $u_i = 0$ for every $i \leq k$ with $i \neq j$, then $\sum_{i=0}^k u_i = u_j$ when $j \leq k$, and $\sum_{i=0}^k u_i = 0$ when $j > k$;
 - ($\Sigma 4$) $-\sum_{i=0}^k u_i = \sum_{i=0}^k (-u_i)$.
- (c) (*Powers.*) For $s \in R$ and $n \in \mathbb{N}$, $s^0 := 1$ and $s^{n+1} := s^n s$ define s^n for every n , and for all $s, t \in R$ and $m, n \in \mathbb{N}$,

$$s^{m+n} = s^m s^n, \quad (s^m)^n = s^{mn}, \quad (st)^n = s^n t^n.$$

- (d) (*Multiples.*) For all $a, b \in R$ and $m, n \in \mathbb{Z}$,

$$\begin{aligned} (m+n) \cdot a &= m \cdot a + n \cdot a, & m \cdot (a+b) &= m \cdot a + m \cdot b, \\ (m \cdot a)b &= m \cdot (ab), & (m \cdot 1)a &= m \cdot a, \\ (mn) \cdot a &= m \cdot (n \cdot a). \end{aligned}$$

In words: (a) says that a finite list in a set with an addition has a sum, built one term at a time, and that terms beyond the list do not matter; it needs no law of addition beyond $0 + u = u$. (b) says that a finite sum of ring elements can be split into two sums, multiplied through by a constant, collapsed to its one non-zero term, or negated term by term. (c) is the three laws of exponents in a commutative ring. (d) is the arithmetic of the multiples $m \cdot a$ of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3 (“Multiples”), extended to $m \in \mathbb{Z}$ in Chapter 2: a dot with an integer on its left is always a multiple, and the product of two ring elements is written by juxtaposition.

Parts (b) and (d) are cited from Chapter 2: $(\Sigma 1)$ – $(\Sigma 4)$ are Lemma 2.6.1 (a), (b), (d), (e) (for $(\Sigma 3)$, apply Lemma 2.6.1 (d) to the sequence that agrees with $u_0, \dots, u_k$ and is 0 beyond k ; by the finite-lists clause of part (a) above it has the same sum), and the five rules of part (d) above are Lemma 2.5.1 (c), (d). Parts (a) and (c) are the recursions of *Sets, Relations, and Cardinality*, Section 2.3, read in T and in R ; each is built by *Sets, Relations, and Cardinality*, Theorem 2.3.1, and each of its laws is one short induction. Chapter 1 proves the same three power laws for every commutative ring (Proposition 1.1.3); we only compare with it, and prove (c) again from the template, so that this chapter’s main line rests on Chapter 2 and not on Chapter 1.

🕒 **Second reading** · *Proofs of (a) and (c)*

Idea. Each statement comes from *Sets, Relations, and Cardinality*, Theorem 2.3.1, and each law is one induction on one index, following the clauses of the recursion: the base case uses the starting value, and the step peels off the last term or factor. Only the laws of R named at each step are used.

Proof. (a) Apply *Sets, Relations, and Cardinality*, Theorem 2.3.1 (read on $\mathbb{N} = \omega$ through *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Corollary 1.7.3 (b)) with $X = T$, starting value 0 and step $(j, y) \mapsto y + u_j$, a function $\mathbb{N} \times T \rightarrow T$ because $+$ maps $T \times T$ into T . It gives exactly one sequence $(S_j)_{j \in \mathbb{N}}$ in T with $S_0 = 0$ and $S_{j+1} = S_j + u_j$. Set $\sum_{i=0}^k u_i := S_{k+1}$. Then $\sum_{i=0}^0 u_i = 0 + u_0 = u_0$ by the hypothesis on 0, and $\sum_{i=0}^{k+1} u_i = S_{k+1} + u_{k+1} = \sum_{i=0}^k u_i + u_{k+1}$. Any assignment obeying the two displayed equations agrees with this one at every k , by Logic and Proof, Axiom 4.2.1 on k .

For the dependence on $u_0, \dots, u_k$, let (v_i) be a second sequence with $v_i = u_i$ for $i \leq k$, and let (S'_j) be its sequence of partial sums. We prove by Logic and Proof, Axiom 4.2.1 on j the statement “if $j \leq k + 1$, then $S_j = S'_j$ ”. For $j = 0$ both are 0. If $j + 1 \leq k + 1$, then $j \leq k + 1$ and $j \leq k$, so $S_j = S'_j$ by the hypothesis and $u_j = v_j$; hence $S_{j+1} = S_j + u_j = S'_j + v_j = S'_{j+1}$. At $j = k + 1$ this gives $\sum_{i=0}^k u_i = \sum_{i=0}^k v_i$. The argument used only that $+$ is a function on T . The product of a list is *Sets, Relations, and Cardinality*, Theorem 2.3.1 with $X = R$, starting value 1 and step $(j, y) \mapsto y s_{j+1}$ (with $s_j := 1$, say, for $j > r$), the pattern of the product in *Sets, Relations, and Cardinality*, Definition 2.3.1; its dependence on $s_1, \dots, s_r$ only is the same induction.

(c) The powers are *Sets, Relations, and Cardinality*, Theorem 2.3.1 with $X = R$, starting value 1 and step $(n, y) \mapsto ys$, the pattern of *Sets, Relations, and Cardinality*, Definition 2.3.2. For the first law fix m and induct on n (Logic and Proof, Axiom 4.2.1). For $n = 0$: $s^{m+0} =$

$s^m = s^m \cdot 1 = s^m s^0$, by (F7). If $s^{m+n} = s^m s^n$, then

$$s^{m+(n+1)} = s^{(m+n)+1} = s^{m+n} s = (s^m s^n) s = s^m (s^n s) = s^m s^{n+1},$$

using $m + (n + 1) = (m + n) + 1$ (Number Systems: From $\setminus(\setminus n \mathbb{N} \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Theorem 1.5.3 (c)), the recursion, the hypothesis and (F5). For the second law fix m : $(s^m)^0 = 1 = s^0 = s^{m \cdot 0}$ (Number Systems: From $\setminus(\setminus n \mathbb{N} \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Definition 1.5.1 (b)), and if $(s^m)^n = s^{mn}$, then $(s^m)^{n+1} = (s^m)^n s^m = s^{mn} s^m = s^{mn+m} = s^{m(n+1)}$, by the first law and $m(n + 1) = mn + m$ (Number Systems: From $\setminus(\setminus n \mathbb{N} \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Theorem 1.5.3 (d), (e)). For the third: $(st)^0 = 1 = 1 \cdot 1 = s^0 t^0$, by (F7), and if $(st)^n = s^n t^n$, then $(st)^{n+1} = (st)^n (st) = (s^n t^n)(st) = (s^n s)(t^n t) = s^{n+1} t^{n+1}$, regrouping by (F5) and (F6). This proves (a) and (c). ■

We will use (a) twice over: for sums of ring elements, as in the product formula of Section 4.2, and for sums in $R[x]$ of finitely many monomials, which Section 4.2 forms with its coefficientwise addition before any ring law of $R[x]$ is known. In both cases $0 + u = u$ holds, in R by (F1) and (F3), and in $R[x]$ position by position.

4.1.4 Exercises

4.1.4.1 A. Check your understanding

Exercise. A1

- (a) Write the coefficient sequences of $x^3 - 2x \in \mathbb{Z}[x]$ and of $[2]x^2 + [4]x \in (\mathbb{Z}/4\mathbb{Z})[x]$. Is the second one a monomial?
- (b) Is “ $1 + x + x^2 + \dots$ ”, the sequence $(1, 1, 1, \dots)$ of rationals, a polynomial over $\mathbb{Q}$? Name the clause of Definition 4.1.1 that decides it.
- (c) True or false: two polynomials p, q over $\mathbb{F}_2$ whose rules $c \mapsto \sum_{k=0}^N p_k c^k$ and $c \mapsto \sum_{k=0}^N q_k c^k$, for an N admissible for both, agree at 0 and at 1 are equal. Justify your answer.
- (d) Which N are admissible for $3x^2 - x + 2 \in \mathbb{Q}[x]$?

Solution.

- (a) $x^3 - 2x$ is $(0, -2, 0, 1, 0, 0, \dots)$: the constant term is 0, the coefficient of x is -2 , and that of x^3 is 1. The second is $([0], [4], [2], [0], \dots)$, and $[4] = [0]$ in $\mathbb{Z}/4\mathbb{Z}$, since $4 - 0 = 4$. So it is $([0], [0], [2], [0], \dots)$, the monomial $[2]x^2$.
- (b) No. The clause **only finitely many** fails: for every $N \in \mathbb{N}$ the entry in position $N + 1$ is $1 \neq 0$, so no N is admissible.
- (c) False. The polynomials $x^2 + x$ and 0 over $\mathbb{F}_2$ give the rules $c \mapsto cc + c$ and $c \mapsto 0$, which agree at 0 and at 1 (the computation at the start of the section). But $x^2 + x = (0, 1, 1, 0, \dots)$ differs from 0 in position 1, so the polynomials are not equal.
- (d) Every $N \geq 2$. The coefficient of x^2 is $3 \neq 0$, so $N = 0$ and $N = 1$ fail (position $2 > N$ holds a non-zero entry); and every $N \geq 2$ works, since all positions $k \geq 3$ hold 0.

4.1.4.2 B. Practice

Exercise. B1: Polynomials of bounded length as tuples

Let $N \in \mathbb{N}$ and $P_N := \{p \in R[x] : p_k = 0 \text{ for every } k > N\}$. Prove that

$$\Theta: P_N \rightarrow R^{N+1}, \quad p \mapsto (p_0, p_1, \dots, p_N),$$

is a bijection (Sets, Relations, and Cardinality, Definition 1.4.5), where R^{N+1} is the set of $(N+1)$ -tuples of elements of R , indexed here from 0 (Sets, Relations, and Cardinality, Definition 1.3.2; for $N = 0$, where the book has no 1-tuples, we read R^1 as R , with (a_0) standing for a_0 , and Θ as $p \mapsto p_0$). Hence list the elements of P_2 for $R = \mathbb{F}_2$.

Solution. Injective. Let $p, q \in P_N$ with $\Theta(p) = \Theta(q)$. Then $p_k = q_k$ for $k \leq N$, and $p_k = 0 = q_k$ for $k > N$ by the definition of P_N . So $p_k = q_k$ for every k , and $p = q$ by Sets, Relations, and Cardinality, Proposition 1.4.1.

Surjective. Let $(a_0, \dots, a_N) \in R^{N+1}$. Define $p: \mathbb{N} \rightarrow R$ by $p_k := a_k$ for $k \leq N$ and $p_k := 0$ for $k > N$: extend by zeros. Then N is admissible for p , so $p \in R[x]$ and $p \in P_N$, and $\Theta(p) = (a_0, \dots, a_N)$.

So Θ is a bijection; its inverse is “extend by zeros”. For $R = \mathbb{F}_2$ and $N = 2$, each a_i is 0 or 1, and the eight triples (a_0, a_1, a_2) give the eight polynomials

$$0, \quad 1, \quad x, \quad x+1, \quad x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1.$$

Section 4.4 returns to this list and asks which functions $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ they define.

Exercise. B2: Determine which

Each formula below defines a sequence $\mathbb{N} \rightarrow \mathbb{Z}/4\mathbb{Z}$. Determine which of them are polynomials over $\mathbb{Z}/4\mathbb{Z}$. Justify your answer, and for each polynomial give the least admissible N and the polynomial in the notation of the display.

- (a) $p_k := [2^k]$.
- (b) $p_k := [k^2]$.
- (c) $p_k := [k(k-1)(k-2)(k-3)]$.
- (d) $p_k := [2k]$.

Solution. By Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.3 (b), $[0], [1], [2], [3]$ are four different classes; in particular $[1] \neq [0]$ and $[2] \neq [0]$.

- (a) A polynomial. The first entries are $[1], [2], [4], [8], \dots$, and for $k \geq 2$, $2^k = 4 \cdot 2^{k-2}$ (Lemma 4.1.1 (c)), so $[2^k] = [0]$. The least admissible N is 1: $N = 1$ works, and $N = 0$ does not, since $p_1 = [2] \neq [0]$. The polynomial is $1 + [2]x$.
- (b) Not a polynomial. For odd $k = 2j + 1$, $k^2 = 4(j^2 + j) + 1$, so $p_k = [1] \neq [0]$. Given any N , the odd number $k = 2N + 1 > N$ has $p_k \neq [0]$, so no N is admissible.
- (c) A polynomial: the zero polynomial. Let $k \in \mathbb{N}$. By Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.1.2 (a), $k = 4q + r$ with $0 \leq r \leq 3$, so $k - r = 4q$ is one of the

four factors $k, k-1, k-2, k-3$. Hence the product is a multiple of 4, and $p_k = [0]$ for every k (for $k \leq 3$ the multiple is 0, since then $q = 0$). Every N is admissible; the least is 0, and the display is 0.

- (d) Not a polynomial. For odd $k = 2j + 1$, $2k = 4j + 2$, so $p_k = [2] \neq [0]$, and as in (b) no N is admissible.

The sequences in (b) and (d) have infinitely many non-zero entries even though their values repeat; (c) shows that a formula in k can describe the zero polynomial.

4.1.4.3 C. Going deeper

Exercise. C1: Finitely many, in the sense of finite sets

For a sequence $p: \mathbb{N} \rightarrow R$, let $S := \{k \in \mathbb{N} : p_k \neq 0\}$, the set of positions that hold a non-zero entry. Prove that some $N \in \mathbb{N}$ is admissible for p if and only if S is finite (Sets, Relations, and Cardinality, Definition 3.1.2). So “only finitely many p_k are non-zero” in Definition 4.1.1 means exactly what it says.

Solution. ($\Rightarrow$) Let N be admissible. If $k \in S$, then $p_k \neq 0$, so $k \leq N$; hence $S \subseteq \{0, \dots, N\}$. The set $\{0, \dots, N\}$ has $N + 1$ elements (the third example after Sets, Relations, and Cardinality, Definition 3.1.2), so its subset S is finite by Sets, Relations, and Cardinality, Proposition 3.1.6.

($\Leftarrow$) We prove by Logic and Proof, Axiom 4.2.1 on $n \in \mathbb{N}$: *every subset $A \subseteq \mathbb{N}$ with n elements has an upper bound $b \in \mathbb{N}$, that is, $a \leq b$ for every $a \in A$* . For $n = 0$, $A = \emptyset$ (the first example after Sets, Relations, and Cardinality, Definition 3.1.2), and $b = 0$ works vacuously. Suppose the statement holds for n , and let $\varphi: \{1, \dots, n+1\} \rightarrow A$ be a bijection. Put $z := \varphi(n+1)$ and $A' := A \setminus \{z\}$. The restriction of φ to $\{1, \dots, n\}$ maps into A' (if $\varphi(j) = z$ then $j = n+1$, by injectivity), is injective, and is onto A' (an element of A' is $\varphi(j)$ with $j \neq n+1$, so $j \leq n$). So A' has n elements and an upper bound b' . By trichotomy (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.6.1 (a)), the larger b of b' and z is defined, and it bounds every element of $A = A' \cup \{z\}$.

Now let S be finite, with an upper bound N . If $k > N$, then $k \notin S$, that is, $p_k = 0$. So N is admissible.

The proof of ($\Leftarrow$) never needed a greatest element of S , only an upper bound. The greatest element exists when S is non-empty and finite (an upper bound in $\mathbb{N} \subseteq \mathbb{Z}$ gives one by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6), and Section 4.3 calls it the degree.

Marking scheme. (10 points) - 3: ($\Rightarrow$) shows $S \subseteq \{0, \dots, N\}$ and concludes that S is finite, citing that $\{0, \dots, N\}$ is finite and that a subset of a finite set is finite (Sets, Relations, and Cardinality, Proposition 3.1.6). - 2: ($\Leftarrow$) sets up an induction on the number of elements of a finite $A \subseteq \mathbb{N}$, with the claim that A has an upper bound, and handles $A = \emptyset$. - 2: in the step, removes one element z and shows that the rest A' has n elements (by restricting the bijection, or by Sets, Relations, and Cardinality, Corollary 3.1.7). - 1: takes the larger of b' and z , by trichotomy, as a bound for $A = A' \cup \{z\}$. - 2: concludes that an upper bound N of S is admissible: $k > N$ implies $k \notin S$, so $p_k = 0$.

Fatal errors (0 for the step): using a greatest element of S without justification; overlooking

$S = \emptyset$ in $(\Leftarrow)$.