1

Radix polynomial representation

1.1 Introduction

From the earliest cultures humans have used methods of recording numbers (integers), by notches in wooden sticks or collecting pebbles in piles or rows. Conventions for replacing a larger group or pile, e.g., five, ten, or twelve objects, by another object or marking, are also found in some early cultures. Number representations like these are examples of *positional number systems*, in which objects have different weight according to their relative positions in the number. The weights associated with different positions need not be related by a constant ratio between the weights of neighboring positions. In time, distance, old currency, and other measuring systems we find varying ratios between the different units of the same system, e.g., for time 60 minutes to the hour, 24 hours to the day, and 7 days to the week, etc.

Systems with a constant ratio between the position weights are called radix systems; each position has a weight which is a power of the radix. Such systems can be traced back to the Babylonians who used radix 60 for astronomical calculations, however without a specific notation for positioning of the unit, so it can be considered a kind of floating-point notation. Manipulating numbers in such a notation is fairly convenient for multiplication and division, as is known for anyone who has used a slide rule. Our decimal notation with its fixed radix point seems to have been developed in India about 600 CE, but without decimal fractions. Decimal notation with fractions appeared later in the Middle East, and in the fifteenth century a Persian mathematician computed the value of π correctly to 16 decimal digits. In the seventeenth century the binary system was developed, and it was realized that any integer greater than 1 could be used as a radix. Knuth in [Knu98, Chapter 4] gives an account of the development of positional systems, and provides further references on their history.

Usually digits used for denoting numbers in a positional system are restricted by the ratios between weights of neighboring positions, in radix systems by the value of the radix. If the factor or radix is β, then the digits normally used are from the set $\{0, 1, \ldots, \beta - 1\}$, but other digit sets are possible. If the cardinality of the set of permissible digits is larger than the radix, then some numbers can be represented in more than one way and the number system is said to be redundant. Such redundancy permits some arithmetic operations to be performed faster than with a "normal" (non-redundant) digit set. For example, as we know, when adding a number of distances measured in feet and inches, we can add up the feet and the inches independently, and only at the end convert excess inches into feet. In this way we avoid converting all the intermediate results, and hence the carry transfers, during accumulation of the individual measures.

In this chapter we will discuss positional number systems mainly through standard radix representations, with only a few deviations into other weighted systems. But we will thoroughly investigate systems where the digits may be drawn from fairly general sets of integers, and in particular also redundant systems. Although it is possible to define systems with a non-integral value of the radix, even a complex value, we shall restrict our treatment to integral values β, $|\beta| \geq 2$.

1.2 Radix polynomials

As a foundation for our development of a theory for the representation of numbers in positional notation, we will use the algebraic structure of sets of polynomials. Arithmetic on numbers in positional notation is closely related to arithmetic on polynomials, so a firm foundation for the former can be based on the theory for the latter. We will here be concerned with the characterization of systems employing an integral-valued radix and digits, but our analysis will go beyond the usual radix 2, 8, 10, and 16 systems and the related standard digit sets.

Let $\mathbb{Z}^*[x]$ be the set of *extended polynomials*[1]

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_\ell x^\ell \tag{1.2.1}$$

with $a_i \in \mathbb{Z}$ (the set of integers), $-\infty < \ell \leq i \leq m < \infty$, considered *formal expressions in the indeterminate variable* x. The coefficients a_m and a_ℓ may be zero, but the zero polynomial is also denoted $P(x) = 0$. However, in general we will only display non-zero coefficients a_i. If $m = \ell$ we call $P(x)$ an *extended monomial*.

It is then possible to define addition and multiplication on polynomials from $\mathbb{Z}^*[x]$, i.e., with $P(x), Q(x) \in \mathbb{Z}^*[x]$,

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_\ell x^\ell,$$
$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_k x^k,$$

[1] The extension here is that, in general, we allow negative powers of x.

and $p = \max(m, n)$, $q = \min(\ell, k)$, we may define:

$$S(x) = P(x) + Q(x) = (a_p + b_p)x^p + (a_{p-1} + b_{p-1})x^{p-1} + \cdots + (a_q + b_q)x^q, \tag{1.2.2}$$

$$R(x) = P(x) \times Q(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_{\ell+k}x^{\ell+k}, \tag{1.2.3}$$

where

$$c_j = a_\ell b_{j-\ell} + a_{\ell+1} b_{j-\ell-1} + \cdots + a_{j-k} b_k. \tag{1.2.4}$$

Based on the fact that $(\mathbb{Z}, +, \times)$ is a commutative ring with identity employing integer addition and multiplication as operators, it may now be seen that $(\mathbb{Z}^*[x], +, \times)$ is also a commutative ring with identity satisfying the cancellation law (i.e., an integral domain), when $+$ and $\times$ here is taken as addition and multiplication defined by (1.2.2) respectively (1.2.3) and (1.2.4).

When in (1.2.1) the indeterminate variable x is taken as a real variable, $P(x)$ is a function whose value can be found at any real value b. We will denote this evaluation as

$$P(x)\Big|_{x=b} \in \mathbb{R}$$

and define the *evaluation mapping* E_b as

$$E_b : P(x) \to P(x)|_{x=b}. \tag{1.2.5}$$

Observation 1.2.1 *For $b \neq 0$, E_b is a homomorphism of $\mathbb{Z}^*[x]$ to the reals:*

$$S(x) = P(x) + Q(x) \Rightarrow S(x)|_{x=b} = P(x)|_{x=b} + Q(x)|_{x=b}, \tag{1.2.6}$$

$$R(x) = P(x) \times Q(x) \Rightarrow R(x)|_{x=b} = P(x)|_{x=b} \times Q(x)|_{x=b}. \tag{1.2.7}$$

Thus for fixed b the extended polynomials $P(x)$ and $Q(x)$ may be used as *representations* of the real numbers $P(x)|_{x=b}$ and $Q(x)|_{x=b}$ respectively. Note that addition of extended polynomials is independent in each position or "carry-free" since the coefficients are unrestricted integers. Also note that E_b is not one-to-one, e.g.,

$$(9x + 3 + 4x^{-1})|_{x=8} = (x^2 + x + 3 + 4x^{-1})|_{x=8} \ (= 75.5).$$

For fixed a and b let us define

$$\mathcal{V}_b(a) = \{P(x) \in \mathbb{Z}^*[x] \mid P(x)|_{x=b} = a\},$$

i.e., the set of polynomials whose value at b is a. Or using different terminology, for fixed b, $\mathcal{V}_b(a)$ is the set of *redundant representations* of a. Also $\mathcal{V}_b(a)$ can be characterized as a *residue class* in the set of extended polynomials.

Theorem 1.2.2 *Given any two extended polynomials $P(x)$, $Q(x)$, then $P(x)|_{x=b} = Q(x)|_{x=b}$ if and only if $P(x) \equiv Q(x)$ (mod $(x - b)$).*

Proof For $P(x) \equiv Q(x) \pmod{(x-b)}$ we have $P(x) = Q(x) + R(x) \times (x - b)$. So then $P(x)|_{x=b} = Q(x)|_{x=b} + R(x)|_{x=b} \times (x-b)|_{x=b} = Q(x)|_{x=b}$ since $(x-b)|_{x=b} = 0$.

Alternatively, assume $P(x)|_{x=b} = Q(x)|_{x=b}$. Then the polynomial $S(x) = P(x) - Q(x)$ satisfies $S(x)|_{x=b} = 0$, so b is a root of $S(x)$. This means $(x-b)$ must divide $S(x)$, so we obtain $S(x) = R(x) \times (x-b)$ for some $R(x)$. Hence $P(x) = Q(x) + R(x) \times (x-b)$. □

Example 1.2.1 Let $b = 8$ and consider the extended polynomials

$$P(x) = x^2 - 5x - 6 + 13x^{-1},$$
$$Q(x) = 2x + 4 - 3x^{-1}.$$

Now $P(x)$ has the same value as $Q(x)$ for $x = b = 8$, $P(x)|_{x=8} = Q(x)|_{x=8} = 19\frac{5}{8}$, so $Q(x)$ and $P(x)$ both belong to $\mathcal{V}_8(19\frac{5}{8})$. We further note that

$$P(x) - Q(x) = x^2 - 7x - 10 + 16x^{-1} = (x + 1 - 2x^{-1})(x - 8),$$

so $P(x) \equiv Q(x) \pmod{(x-8)}$ as required by Theorem 1.2.2. □

From the proof of Theorem 1.2.2 we note the following.

Observation 1.2.3 *If $P(x)|_{x=b} = Q(x)|_{x=b}$, then there exists a transfer polynomial*

$$R(x) = \sum_{i=\ell}^{m} c_i x^i$$

satisfying

$$\begin{aligned} P(x) &= Q(x) + R(x)(x-b) \\ &= Q(x) + \sum_{i=\ell}^{m} c_i (x-b) x^i, \end{aligned}$$

where each term $c_i x^{i+1} - c_i b x^i$ performs a transfer (a "carry") of information from position i to position $i+1$ of the polynomial.

In the rest of this book we will consider various systems characterized by the value of b chosen. We will use the symbol β for such a value, termed[2] the *radix* or the *base* of the system. The radix can be positive or negative, even non-integral or complex. In the following we will only consider integral values of the radix β. Since we intend to evaluate extended polynomials at β, but still retain a distinction between the formal expression $P(x)$ and its value obtained

[2] We will, in general, use the term radix rather than base, except where traditionally the latter is used, such as in base conversion.

by the evaluation mapping E_β, we will for $P(x) \in \mathbb{Z}^*[x]$ distinguish between the extended polynomial

$$P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \cdots + d_\ell[\beta]^\ell$$

i.e., an unevaluated expression, and the real value obtained by evaluating

$$P(\beta) = d_m\beta^m + d_{m-1}\beta^{m-1} + \cdots + d_\ell\beta^\ell.$$

Definition 1.2.4 *For β such that $|\beta| \geq 2$, the set of* radix-β polynomials $\mathcal{P}[\beta]$ *is the set composed of the zero-polynomial and all extended polynomials of the form*

$$P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \cdots + d_\ell[\beta]^\ell,$$

where $d_i \in \mathbb{Z}$ for $-\infty < \ell \leq i \leq m < \infty$.

Notation For $P([\beta]) = \sum_{i=\ell}^{m} d_i[\beta]^i \in \mathcal{P}[\beta]$ we introduce the following notation:

β: the radix or base;
d_i: the digit in position i; or
$d_i(P)$: the digit in position i of polynomial $P([\beta])$;
m: the most-significant position: $\mathrm{msp}(P([\beta]))$;
ℓ: the least-significant position: $\mathrm{lsp}(P([\beta]))$;
d_m: the most-significant digit: $d_m \neq 0$;
d_ℓ: the least-significant digit: $d_\ell \neq 0$.

We assume that $d_m \neq 0$ and $d_\ell \neq 0$, except when $P = 0$, where $d_m = d_\ell = m = \ell = 0$. In the following $\mathrm{lsp}(P[\beta])$ will be called be the *last place*.

$\mathcal{P}[\beta]$ thus forms a ring with the same additive and multiplicative structure as the ring $\mathbb{Z}^*[x]$. Particular examples are:

$\mathcal{P}[16]$: the *hexadecimal* radix polynomials;
$\mathcal{P}[10]$: the *decimal* radix polynomials;
$\mathcal{P}[8]$: the *octal* radix polynomials;
$\mathcal{P}[3]$: the *ternary* radix polynomials;
$\mathcal{P}[2]$: the *binary* radix polynomials;
$\mathcal{P}[-2]$: the *nega-binary* radix polynomials.

Our general definition of radix polynomials allows positive and/or negative digits as well as digit values exceeding the magnitude of the radix.

In arithmetic algorithms there is a need to deal with individual terms of a radix-β polynomial, corresponding to individual digits, and, in general, in order to have a kind of "pointer" to a specific position of a radix polynomial. Hence we introduce the following definition.

Definition 1.2.5 *For β such that $|\beta| \geq 2$, the set of* radix-β monomials of order j, $\mathcal{M}^j[\beta]$, *is the set of all extended polynomials of the form*

$$M([\beta]) = i[\beta]^j,$$

where $i, j \in \mathbb{Z}$. The exponent j is called the order *of the monomial.*

Note that i may be any integer, including zero, and may contain β as a factor. The order j serves to position the digit value i, e.g., for adding into a particular position using (1.2.2). Multiplying with a *unit monomial* $[\beta]^j$ using (1.2.3) corresponds to a "shifting" operation on a number in positional notation. Adding a monomial $[\beta]^\ell$ to a radix polynomial $P[\beta]$ with $\mathrm{lsp}(P[\beta]) = \ell$ corresponds to adding a *unit in the last place* (ulp).

By Theorem 1.2.2, the relation for equality-of-value of extended polynomials under the evaluation mapping $E_\beta : P(x) \to P(x)|_{x=\beta}$ yields the residue classes of $\mathbb{Z}^*[x]$ modulo $(x - \beta)$ as equivalence classes. The extended monomials provide for characterizing a useful *complete residue system* for these equivalence classes.

Theorem 1.2.6 *For β with $|\beta| \geq 2$, let*[3] $\mathcal{M}' = \{i\,[\beta]^j \mid i \neq 0, \beta \nmid i \in \mathbb{Z}, j \in \mathbb{Z}\} \cup \{0[\beta]^0\}$*, i.e., $\mathcal{M}'$ is the set of all radix-β monomials with coefficients not divisible by β, along with the zero polynomial. Then $\mathcal{M}'$ is a complete residue system for $\mathbb{Z}^*[x]$ modulo $(x - \beta)$.*

Proof To show that members of $\mathcal{M}'$ are in distinct residue classes it is sufficient by Theorem 1.2.2 to show the evaluation mapping maps distinct members of $\mathcal{M}'$ into distinct real values. Suppose $i[\beta]^j, k[\beta]^\ell \in \mathcal{M}'$ are distinct non-zero members of $\mathcal{M}'$ of the same value. Now $i[\beta]^j$ evaluates to $i\beta^j$ and $k[\beta]^\ell$ has the value $k\beta^\ell$, so $i\beta^j = k\beta^\ell$. We may assume $\ell \geq j$, so $i = k\beta^{\ell-j}$. Then $\ell = j$, since β does not divide i, and $i = k$, a contradiction, and it follows that members of $\mathcal{M}'$ are congruent modulo $(x - \beta)$. Moreover $P(x) \in \mathbb{Z}^*[x]$ is either the zero polynomial or has a least-significant digit $d_\ell \neq 0$. Then $P(x)|_{x=\beta} = i\beta^l$ for integers i, ℓ. If $i = 0$, then $P(x)$ is congruent to the zero polynomial modulo $(x - \beta)$. If $i = k\beta^n$ for $n \geq 1$ and $\beta \nmid k$, then $P(x)|_{x=\beta} = k\beta^{\ell+n}$ and $P(x) \equiv k[\beta]^{l+n}$ modulo $(x - \beta)$ with $k[\beta]^{\ell+n} \in \mathcal{M}'$. Thus $\mathcal{M}'$ is a complete residue system for $\mathbb{Z}^*[x]$ modulo $(x - \beta)$. □

The members of $\mathcal{M}'$ provide convenient unique expressions for the real values a such that the redundancy classes $\mathcal{V}_\beta(a)$ are non-vacuous.

Problems and exercises

1.2.1 For $P \in \mathcal{P}[\beta]$, $P \neq 0$ show that $\lfloor P \times [\beta]^{-\mathrm{msp}(P)} \rfloor$ is a radix polynomial whose value is the most-significant digit of P (here $\lfloor \cdot \rfloor$ means truncate

[3] The symbol $\nmid$ means "does not divide."

the polynomial to its integer part). Derive a similar formula for the least-significant digit.

1.2.2 For P and Q given as

$$\begin{aligned} P &= 5 \times [\beta]^6 + 3 \times [\beta]^4 + 2 \times [\beta]^3 - 2 \times [\beta]^2, \\ Q &= 4 \times [\beta]^3 + 2 \times [\beta]^2 - 6 \times [\beta] - 7 \times [\beta]^{-3} \\ &\quad - 3 \times [\beta]^{-4} + 5 \times [\beta]^{-7}, \end{aligned}$$

find $\mathrm{msp}(P+Q)$, $\mathrm{msp}(P \times P)$, $\mathrm{lsp}(P \times Q)$, $\mathrm{lsp}(\lfloor P+Q \rfloor)$, and $d_{\mathrm{lsp}(\lfloor P \times Q \rfloor)}(\lfloor P \times Q \rfloor)$.

1.3 Radix-β numbers

The radix polynomials introduced in the previous section provide a representation of numbers in which the evaluation mapping E_β provides a mapping from extended polynomials into the reals. Since β is fixed for a radix polynomial $P([\beta]) \in \mathcal{P}[\beta]$ we will introduce the operator $\|\cdot\|$ defined on $\mathcal{P}[\beta]$ as

$$\|P([\beta])\| = P(x)|_{x=\beta} = P(\beta) = \sum_{i=\ell}^{m} d_i \beta^i$$

for the evaluation mapping.

Restricting β and the digits d_i to integral values for given β with $|\beta| \geq 2$, the real value $v = \sum_{i=l}^{m} d_i \beta^i$ determined by the evaluation operation is a rational number belonging to a subset of rationals characterized by the radix β. The set

$$\mathbb{Q}_\beta = \{k\beta^\ell \mid k, \ell \in \mathbb{Z}\} \tag{1.3.1}$$

is called the *radix-β numbers*, but could equivalenly be termed the *radix-β rationals*. Note that either or both of k and ℓ may be negative in (1.3.1). Observing that $\mathbb{Q}_\beta = \mathbb{Q}_{-\beta}$, it is evident that the set of values of the radix polynomials of $\mathcal{P}[\beta]$ is precisely $\mathbb{Q}_{|\beta|}$. Also $\mathbb{Q}_{|\beta|}$ inherits the algebraic structure of addition and multiplication as defined on reals. Thus polynomial arithmetic in $\mathcal{P}[\beta]$ corresponds to the arithmetic of the real numbers in $\mathbb{Q}_{|\beta|}$.

Observation 1.3.1 *For any integer radix β with $|\beta| \geq 2$ the evaluation mapping $\|P\|$ for $P \in \mathcal{P}[\beta]$ is a homomorphism of $\mathcal{P}[\beta]$ onto $\mathbb{Q}_{|\beta|}$; $(\mathbb{Q}_{|\beta|}, +, \times)$ is a commutative ring with identity.*

Thus reference to $\mathbb{Q}_\beta$ as the *radix-β number system* denotes the set $\mathbb{Q}_\beta$ along with the arithmetic structure provided by the commutative ring $(\mathbb{Q}_\beta, +, \times)$. For the most often used radix values it is customary to employ the following terminology:

$\mathbb{Q}_2$: binary number system;
$\mathbb{Q}_3$: ternary number system;
$\mathbb{Q}_8$: octal number system;
$\mathbb{Q}_{10}$: decimal number system;
$\mathbb{Q}_{16}$: hexadecimal number system;

but note $v \in \mathbb{Q}_{|\beta|}$ just implies that v is a number which *can* be represented as a (finite length) radix-β polynomial.

The factors of a particular *radix factorization* $v = k\beta^\ell$ for $v \in \mathbb{Q}_\beta$ identify two components of the representation of v that are typically handled separately in implementing radix arithmetic. Specifically

- k is the integer *significand*, and
- β^ℓ is the *scale factor* with *exponent* ℓ.

For $\ell > 0$, v is an integer tuple factorization. For $\ell \leq 0$, the factorization is equivalent to the fraction $k/\beta^{-\ell}$ with numerator k and denominator $\beta^{|\ell|}$.

Observation 1.3.2 *The radix-β numbers $\mathbb{Q}_\beta$ form the subset of rationals given by fractions with denominators restricted to powers of the radix β.*

A radix factorization $k\beta^\ell$ is termed reducible when $\beta | k$, and is a unique *irreducible radix factorization* when $\beta \nmid k$, yielding a unique minimum magnitude significand.

Observation 1.3.3 *$v = k\beta^\ell$ is an irreducible radix factorization if and only if $k \bmod \beta \neq 0$.*

Observation 1.3.4 *Let $\mathcal{M}_\beta$ be a complete residue system for $\mathbb{Z}^*[x]$ modulo $(x - \beta)$. Then the evaluation mapping $\|\cdot\|$ is an isomorphism between $\mathcal{M}_\beta$ and the irreducible radix factorizations.*

The relationship between the "scaled significand" radix factorizations $\{k \times \beta^\ell\}$ as tuples, and the set of radix-β numbers $\mathbb{Q}_\beta$ is analogous to the relation between fractions $\{i/j\}$ as tuples, and the set of rational numbers $\mathbb{Q}$, as summarized in Table 1.3.1.

Note that $\mathbb{Q}_{|\beta|}$ is not a field as $1/(|\beta| + 1) \notin \mathbb{Q}_{|\beta|}$, but $\bigcup_p \mathbb{Q}_p$ is a field, the rationals $\mathbb{Q}$. It is well known that $\mathbb{Q}_2 = \mathbb{Q}_8 = \mathbb{Q}_{16}$, and probably also that

Table 1.3.1. *Analogies between the radix-β numbers and the rational numbers*

Number characterization	Tuple terminology	Irreducible form	Number system
Radix factorizations	Significand × scale factor	$k \times \beta^\ell$ $\beta \nmid k$	Radix-β number system $\mathbb{Q}_\beta$
Rational fractions	Numerator / denominator	i/j $\gcd(i, j) = 1$	Rational number system $\mathbb{Q}$

$\mathbb{Q}_2 \subset \mathbb{Q}_{10}$, but what is the relation between $\mathbb{Q}_{12}$ and $\mathbb{Q}_{18}$? The following theorem provides a tool for determining such relations.

Theorem 1.3.5 *If the integers $p \geq 2$ and $q \geq 2$ have prime decompositions $p = \Pi p_i^{n_i}$ and $q = \Pi p_i^{m_i}$, where $\{p_i\}$ is the set of all primes, then:*

(1) If $\forall i : n_i \neq 0 \Rightarrow m_i \neq 0$ (the prime factors of p are factors of q), then $\mathbb{Q}_p \subseteq \mathbb{Q}_q$.
(2) If $\forall i : n_i \neq 0 \Rightarrow m_i \neq 0$ and $\exists j : 0 = n_j < m_j$, then $\mathbb{Q}_p \subset \mathbb{Q}_q$.
(3) If $\forall i : n_i \neq 0 \Leftrightarrow m_i \neq 0$ (p and q contain the same prime factors), then $\mathbb{Q}_p = \mathbb{Q}_q$.

Proof To show (1) first note that for $v = kp^j \in \mathbb{Q}_p$, then also $v \in \mathbb{Q}_q$ if $j \geq 0$, so assume $j < 0$. If t divides u, then for $v \in \mathbb{Q}_t$, $v = kt^j = k(u/t)^{-j}u^j = k'u^j$ with $k' \in \mathbb{Z}$, so $v \in \mathbb{Q}_u$ and hence $\mathbb{Q}_t \subseteq \mathbb{Q}_u$. Specifically with $r = \prod_{p_i \text{ divides } p} p_i$ we have $\mathbb{Q}_r \subseteq \mathbb{Q}_p$. Now let $n = \max\{n_i | p_i{}^{n_i}\ divides\ p\}$ and consider $v \in \mathbb{Q}_p$, so

$$v = kp^j = k\left(\prod p_i{}^{n_i}\right)^j = k\left(\prod p_i{}^{j(n_i-n)}\right)\left(\prod p_i\right)^{jn} = k'r^{jn},$$

where the products are over the p_i dividing p. Since $j < 0$, we have $j(n_i - n) \geq 0$, so $k' = k(\prod p_i{}^{j(n_i-n)}) \in \mathbb{Z}$ hence $v \in \mathbb{Q}_r$ and $\mathbb{Q}_p = \mathbb{Q}_r$. But r also divides q by assumption in (1), so $\mathbb{Q}_p = \mathbb{Q}_r \subseteq \mathbb{Q}_q$, which proves (1).

To prove (2) assume there exists a j such that $0 = n_j < m_j$, then $p_j^{-1} \in \mathbb{Q}_q$ but $p_j^{-1} \notin \mathbb{Q}_p$. Finally (3) follows from (1) by symmetry. $\square$

Example 1.3.1 From Theorem 1.3.5 it follows that $\mathbb{Q}_{12} = \mathbb{Q}_{18}$ with $\mathbb{Q}_2 \subset \mathbb{Q}_{12}$ and $\mathbb{Q}_3 \subset \mathbb{Q}_{12}$. However, $\mathbb{Q}_2 \not\subseteq \mathbb{Q}_3$ and $\mathbb{Q}_3 \not\subseteq \mathbb{Q}_2$ since $\frac{1}{2} \notin \mathbb{Q}_3$ and $\frac{1}{3} \notin \mathbb{Q}_2$. $\square$

The radix numbers are effectively represented with two types of redundancy, both of which are important in efficient implementation of radix arithmetic as operations on digit strings. The choice of exponent, ℓ, in the factorization implicitly recognizes any number of low-order zero digits, and the choice of radix polynomial for the irreducible significand brings flexibility to the choice of coefficients (digits) of the polynomial.

In general, any number $v \in \mathbb{Q}_{|\beta|}$ has an infinity of different representations as a radix-β or radix-$(-\beta)$ polynomial. The evaluation mapping $\|\cdot\| : \mathcal{P}[\beta] \to \mathbb{Q}_{|\beta|}$ partitions the members of $\mathcal{P}[\beta]$ into equivalence classes such that all radix polynomials of a given class have the same real value.

Definition 1.3.6 *For any $v \in \mathbb{Q}_{|\beta|}$ let the* redundancy class $V_\beta(v)$ *be the set*

$$V_\beta(v) = \{P \in \mathcal{P}[\beta] \mid \|P\| = v\}.$$

Example 1.3.2 Let

$$\begin{aligned} P([5]) &= \phantom{1[5]^3 - {}} 2[5]^2 + 3[5] + 1 \in V_5(66), \\ Q([5]) &= 1[5]^3 - 2[5]^2 - 2[5] + 1 \in V_5(66), \\ R([5]) &= \phantom{1[5]^3 - {}} 3[5]^2 - 1[5] - 4 \in V_5(66), \end{aligned}$$

so $P([5])$, $Q([5])$, and $R([5])$ are all in the same redundancy class $V_5(66)$, and form alternative radix-5 representations of the value 66 (which here has been written in ordinary decimal notation).

If the coefficients (the digits) of the polynomials above had to be chosen from the set $\{0, 1, 2, 3, 4\}$, then it is well known that this particular P is the only radix-5 polynomial evaluating to 66. If the digits are drawn from the set $\{-2, -1, 0, 1, 2\}$, then we shall see later that Q is similarly a unique representation. However, if the digit set is $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, then R as well as P and Q are possible representations. □

Problems and exercises

1.3.1 Show that $1/(n+1) \notin \mathbb{Q}_n$ for $n \geq 2$.

1.3.2 List all the members of the redundancy class $V_2(5)$ that can be written with four digits or fewer, using $\{-1, 0, 1\}$ as the permissible set of digit values (for convenience write them in string notation).

1.3.3 For p, q distinct primes, show that $\mathbb{Q}_p \cap \mathbb{Q}_q = \mathbb{Z}$.

1.4 Digit symbols and digit strings

When using radix-β polynomials for the representation of numbers from $\mathbb{Q}_{|\beta|}$:

$$P([\beta]) = \sum_{i=\ell}^{m} d_i [\beta]^i,$$

the representation might also be denoted as a list:

$$((d_m, d_{m-1}, \ldots, d_\ell), \ell)$$

explicitly including all zero-valued digits d_i for $\ell < i < m$, or alternatively only non-zero digits could be listed, e.g., (digit,index)-pairs:

$$((d_{i_1}, i_1), (d_{i_2}, i_2), \ldots, (d_{i_k}, i_k)).$$

The convention is to denote a radix polynomial as a string of symbols drawn from some alphabet, implicitly associated with the chosen radix. We will use the alphabet in Table 1.4.1 in our examples where we only employ "small" radices.