Symbolic Computation 2:

ALGEBRA OF POLYNOMIALS, RATIONAL FUNCTIONS, AND POWER SERIES

by

Keith O. Geddes
Department of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
N2L 3G1

Research Report CS-81-27

September 1981

CS-81-27

PREFACE

This report consists of Chapter 2 of a textbook being written under the title 'Algebraic Algorithms for Symbolic Computation' by Keith O. Geddes. The table of contents for Chapter 2 appears below. A more complete table of contents for the textbook appears on the following pages.

ALGEBRAIC ALGORITHMS FOR SYMBOLIC COMPUTATION

KEITH O. GEDDES

Department of Computer Science
University of Waterloo

CONTENTS

2. ALGEBRA OF POLYNOMIALS, RATIONAL FUNCTIONS, AND POWER SERIES

In this chapter we present some basic concepts from algebra which are of central importance in the development of algorithms and systems for symbolic computation. The main issues distinguishing various symbolic systems arise out of the choice of algebraic structures to be manipulated and the choice of representations for the given algebraic structures.

2.1. RINGS AND FIELDS

A *group* [G; $\circ$] is a set G closed under a binary operation $\circ$ which satisfies the axioms:

A1: $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a,b,c \in G$ (**Associativity**).

A2: There is an element $1 \in G$ such that $1 \circ a = a \circ 1 = a$ for all $a \in G$ (**Identity**).

A3: For all $a \in G$, there is an element $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = 1$ (**Inverses**).

An *abelian group* (or, *commutative group*) is a group in which the binary operation $\circ$ satisfies the additional axiom:

A4: $a \circ b = b \circ a$ for all $a,b \in G$ (**Commutativity**).

A *ring* [R; +, $\times$] is a set R closed under two binary operations +, $\times$ such that [R; +] is an abelian group (i.e. axioms A1-A4 hold with respect to +), $\times$ is associative and has an identity (i.e. axioms A1-A2 hold with respect to $\times$), and which satisfies the additional axiom:

A5: $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$ for all $a,b,c \in R$ (**Distributivity**).

(Note: The identity element with respect to + is denoted by 0 and the inverse of a with respect to + is denoted by $-a$). A *commutative ring* is a ring in which $\times$ is commutative (i.e. axiom A4 holds with respect to $\times$). An *integral domain* is a commutative ring which satisfies the additional axiom:

A6: For all $a,b,c \in R$,

$$a \times b = a \times c \quad \text{and} \quad a \neq 0 \quad \Rightarrow \quad b = c$$ (**Cancellation Law**).

A *field* [F; +, $\times$] is a set F closed under two binary operations +, $\times$ such that [F; +] is an abelian group (i.e. axioms A1-A4 hold with respect to +), [F $-$ {0}; $\times$]^1 is an abelian group (i.e. axioms A1-A4 hold for all non-zero elements with respect to $\times$), and $\times$ is distributive over + (i.e. axiom A5 holds). In other words, a field is a commutative ring in which every nonzero element

1. The *set difference* of two sets A and B is defined by $A - B = \{a: a \in A \text{ and } a \notin B\}$.

has a multiplicative inverse.

A concise summary of the definitions of these algebraic structures is given in Table 2.1. The algebraic structures of most interest in symbolic computation are integral domains and fields. Thus the basic underlying structure is the commutative ring; if multiplicative inverses exist then we have a field, otherwise we will at least have the cancellation law (axiom A6). Another axiom which is equivalent to the cancellation law and which is used by some authors in the definition of an integral domain is:

A6′: For all $a,b \in R$,

$$a \times b = 0 \quad \Rightarrow \quad a = 0 \text{ or } b = 0 \quad \textbf{(No Zero Divisors)}.$$

Of course, axioms A6 and A6′ hold in a field as a consequence of multiplicative inverses.

Table 2.1. Definitions of Algebraic Structures.

ABSTRACT STRUCTURE	NOTATION	AXIOMS
Group	[G; ∘]	A1; A2; A3
Abelian Group	[G; ∘]	A1; A2; A3; A4
Ring	[R; +, ×]	A1; A2; A3; A4 w.r.t. + A1; A2 w.r.t. × A5
Commutative Ring	[R; +, ×]	A1; A2; A3; A4 w.r.t. + A1; A2; A4 w.r.t. × A5
Integral Domain	[D; +, ×]	A1; A2; A3; A4 w.r.t. + A1; A2; A4 w.r.t. × A5; A6
Field	[F; +, ×]	A1; A2; A3; A4 w.r.t. + A1; A2; A3; A4 for F − { 0 } w.r.t. × A5 (Note: A6 holds as a consequence).

Some Number Algebras

The set of integers (positive, negative, and zero) forms an integral domain and is denoted by **Z.** The most familiar examples of fields are the rational numbers **Q,** the real numbers **R,** and the complex numbers **C.** (In all cases, the standard operations of addition and multiplication are implied and will not be denoted in the notation.)

Another field which is of importance in symbolic computation is $\mathbf{Z}_p$, the set of integers modulo p where p is a positive prime integer. In $\mathbf{Z}_p$ addition and multiplication are performed as in **Z** but all numbers are replaced by their remainders after division by p. Thus $\mathbf{Z}_p$ contains exactly p elements and is a *finite field*. For example, the field $\mathbf{Z}_5$ consists of the set { 0,1,2,3,4 }; addition and multiplication tables for $\mathbf{Z}_5$ are presented in Table 2.2. Note that every nonzero element in $\mathbf{Z}_5$ has a multiplicative inverse, since $1 \times 1 = 1$, $2 \times 3 = 1$, $3 \times 2 = 1$, and $4 \times 4 = 1$. If we consider the integers modulo m, $\mathbf{Z}_m$, for some non-prime integer m, then some nonzero

elements will not have multiplicative inverses. $\mathbf{Z}_m$ is, in general, a commutative ring and not even an integral domain. For finite rings, the concepts of the cancellation law (or, no zero divisors) and the existence of multiplicative inverses are equivalent according to a theorem from algebra which states that 'every finite integral domain is a field'. $\mathbf{Z}_p$ is an integral domain, and therefore a field, if and only if p is a prime.

Table 2.2. Addition and Multiplication Tables for $\mathbf{Z}_5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2.2. DIVISIBILITY AND FACTORIZATION IN INTEGRAL DOMAINS

The concept of divisibility plays a central role in symbolic computation. Of course division is always possible in a field. In an integral domain division is not possible, in general, but the concept of factorization into primes which is familiar for the integers $\mathbf{Z}$ can be generalized to other integral domains. Throughout this section, D denotes an integral domain. Here and in the sequel, we adopt the standard mathematical convention of omitting the × symbol for multiplication.

Greatest Common Divisiors

Definition 2.1.

For $a,b \in$ D, a is called a *divisor* of b if $b = ax$ for some $x \in$ D, and we say that *a divides b* (notationally, $a \mid b$). Correspondingly, b is called a *multiple* of a. □

Definition 2.2.

For $a,b \in$ D, an element $c \in$ D is called a *greatest common divisor* (GCD) of a and b if $c \mid a$ and $c \mid b$ and c is a multiple of every other element which divides both a and b. □

Definition 2.3.

For $a,b \in$ D, an element $c \in$ D is called a *least common multiple* (LCM) of a and b if $a \mid c$ and $b \mid c$ and c is a divisor of every other element which is a multiple of both a and b. □

The most familiar application of GCD's is in reducing rational numbers (i.e. quotients of integers) to 'lowest terms'. Another role of GCD's in symbolic computation is the corresponding problem of reducing rational functions (i.e. quotients of polynomials) to 'lowest terms'. The use of the phrase 'a GCD' rather than 'the GCD' is intentional. A GCD of two elements $a,b \in$ D, when it exists, is not unique (but almost).

Definition 2.4.

Two elements $c,d \in D$ are called *associates* if $c \mid d$ and $d \mid c$. □

Definition 2.5.

An element $u \in D$ is called a *unit* (or *invertible)* if u has a multiplicative inverse in D. □

Example 2.1.

In the integral domain **Z** of integers, note the following facts.

(i) The units in **Z** are 1 and -1.

(ii) 6 is a GCD of 18 and 30.

(iii) -6 is also a GCD of 18 and 30.

(iv) 6 and -6 are associates. □

It can be easily proved that in any integral domain D, two elements c and d are associates if and only if $cu = d$ for some unit u. It is also easy to verify that if c is a GCD of a and b then so is any associate $d = cu$, and conversely if c and d are GCD's of a and b then c must be an associate of d. In the integral domains of interest in symbolic computation, it is conventional to impose an additional condition on the GCD in order to make it unique. This is accomplished by noting that the relation of associativity is an equivalence relation, which therefore decomposes an integral domain into *associate classes.* (For example, the associate classes in **Z** are $\{0\}$, $\{1, -1\}$, $\{2, -2\}$, $\cdots$) For a particular integral domain, a criterion is chosen to single out one element of each associate class as its canonical representative and define it to be *unit normal.*

Definition 2.6.

In the integral domain **Z** the nonnegative integers are defined to be *unit normal.* □

Definition 2.7.

In any field F, every nonzero element is an associate of every other nonzero element (in fact, every nonzero element is a unit), so the elements 0 and 1 are defined to be *unit normal.* □

Definition 2.8.

In any integral domain D for which unit normal elements have been defined, an element c is called the *unit normal GCD* of $a,b \in D$, denoted $c = \mathrm{GCD}(a, b)$, if c is a GCD of a and b and c is unit normal. □

Clearly the unit normal GCD of two elements $a,b \in D$ is unique (once the unit normal elements have been defined). For each integral domain D of interest in this book, unit normal elements will be appropriately defined and the following properties will always hold:

(1) 0 is unit normal;

(2) 1 is the unit normal element for the associate class of units;

(3) if $a,b \in D$ are unit normal elements then their product ab is also a unit normal element in D.

In the sequel, whenever we refer to the GCD of $a,b \in D$ it is understood that we are referring to the unique unit normal GCD.

Example 2.2.

In the integral domain **Z,** $\mathrm{GCD}(18, 30) = 6$. □

Definition 2.9.

Let D be an integral domain in which unit normal elements have been defined. The *normal part* of $a \in D$, denoted $n(a)$, is defined to be the unit normal representative of the associate class containing a. The *unit part* of $a \in D$ ($a \neq 0$), denoted $u(a)$, is the unique unit in D such that

$$a = u(a)\, n(a)$$

Clearly $n(0) = 0$ and it is convenient to define $u(0) = 1$. □

Example 2.3.

In the integral domain **Z**, $n(a) = |a|$ and $u(a) = \text{sign}(a)$ where the *sign* of an integer is defined by

$$\text{sign}(a) = \begin{cases} -1 & \text{if } a < 0 \\ 1 & \text{if } a \geqslant 0 \end{cases}. \quad \square$$

The LCM of two elements $a,b \in D$, when it exists, can be made unique in a similar manner. It can be verified that a LCM of $a,b \in D$ exists if and only if GCD(a, b) exists. Moreover, GCD(a, b) is clearly a divisor of the product ab and it easy to verify that the element

$$\frac{ab}{\text{GCD}(a,b)}$$

is a LCM of a and b. We therefore define the unique *unit normal LCM* of $a,b \in D$, denoted LCM(a, b) by

$$\text{LCM}(a,b) = \frac{n(ab)}{\text{GCD}(a,\, b).}$$

Unique Factorization Domains

Definition 2.10.

An element $p \in D - \{0\}$ is called a *prime* (or *irreducible*) if p is not a unit and whenever $p = ab$ then either a or b is a unit. □

Definition 2.11.

Two elements $a,b \in D$ are called *relatively prime* if GCD(a,b) = 1. □

Definition 2.12.

An integral domain D is called a *unique factorization domain* (UFD) if for all $a \in D - \{0\}$, either a is a unit or else a can be expressed as a finite product of primes (i.e. $a = p_1 p_2 \cdots p_n$ for some primes p_i, $1 \leqslant i \leqslant n$) such that this factorization into primes is unique up to associates and reordering (i.e. if $a = p_1 p_2 \cdots p_n$ and $a = q_1 q_2 \cdots q_m$ where p_i ($1 \leqslant i \leqslant n$) and q_j ($1 \leqslant j \leqslant m$) are primes then $n = m$ and there exists a reordering of the q_j's such that p_i is an associate of q_i for $1 \leqslant i \leqslant n$). □

It follows from Definition 2.10 that if p is a prime in an integral domain D then so is any associate of p. If unit normal elements have been defined in D then we may restrict our attention to *unit normal primes* – i.e. primes which are unit normal. Clearly, every prime factorization can be put into the canonical form of the following definition.

Definition 2.13.

If D is a UFD in which unit normal elements have been defined then for $a \in D$ a prime factorization of the form

$$a = u(a)\, p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

is called a *unit normal factorization* if $p_i (1 \leqslant i \leqslant n)$ are unit normal primes, $e_i > 0$ $(1 \leqslant i \leqslant n)$, and $p_i \neq p_j$ whenever $i \neq j$. □

A basic property of primes in a UFD is the following: if $p \mid ab$ and p is a prime, then either $p \mid a$ or $p \mid b$ – i.e. p (or an associate of p) must appear as one of the factors in the prime factorization of a or of b. The integral domain **Z** of integers is the most familiar example of a UFD. It turns out that the integral domains of primary interest in symbolic computation, the polynomial domains to be introduced in the following sections, are also UFD's. (In the case of the polynomial domains, elements are usually referred to as irreducible rather than prime). Exercise 2-9 shows that not every integral domain is a UFD and Exercise 2-10 shows that GCD's do not necessarily exist in an arbitrary integral domain. The following theorem assures us of the existence of GCD's in a UFD. Here and in the sequel, we assume without loss of generality that unit normal elements satisfying (1) - (3) have been defined for every integral domain D.

Theorem 2.1.

If D is a UFD and if $a,b \in D$ are not both zero then GCD(a,b) exists and is unique.

Proof:

The uniqueness has already been established. To show existence, first suppose that $a \neq 0$ and $b \neq 0$ and let their unique unit normal factorizations be

$$(4) \qquad a = u(a)\, p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \quad \text{and} \quad b = u(b)\, q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$$

where p_i $(1 \leqslant i \leqslant n)$, q_j $(1 \leqslant j \leqslant m)$ are unit normal primes. Let $r_1, \ldots, r_l$ denote the distinct elements in the set $\{p_1, \ldots, p_n, q_1, \ldots, q_m\}$. Then the factorizations (4) may be written in the form

$$a = u(a) \prod_{i=1}^{l} r_i^{g_i} \quad \text{and} \quad b = u(b) \prod_{i=1}^{l} r_i^{h_i}$$

where some of the g_i 's and h_i 's may be zero. Then clearly the element

$$d = \prod_{i=1}^{l} r_i^{\min(g_i,\, h_i)}$$

is the GCD of a and b. Finally, if one of a,b is zero assume without loss of generality that $a \neq 0$, $b = 0$. If a has the unique unit normal factorization as given in (4) then clearly the element

$$d = \prod_{i=1}^{n} p_i^{e_i}$$

is the GCD of a and b. □

Euclidean Domains

There is a special class of integral domains in which the divisibility properties are particularly appealing. Unfortunately, most of the polynomial domains of interest to us will not belong to this class. The concepts are nonetheless of central importance and where a polynomial domain does not satisfy the 'division property' discussed here we will be inventing a corresponding 'pseudo-division property' in order to achieve our purposes.

Definition 2.14.

A *Euclidean domain* is an integral domain D with a *valuation* v: D − {0} → **N**, where **N** denotes the set of nonnegative integers, having the following properties:

P1: For all $a,b \in D - \{0\}$, $v(ab) \geq v(a)$;

P2: For all $a,b \in D$ with $b \neq 0$, there exist elements $q,r \in D$ such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$. □

Example 2.4.

The integers **Z** form a Euclidean domain with the valuation $v(a) = |a|$. □

Property P2 of Definition 2.14 is known as the *division property* and is a familiar property of the integers. In the case of a polynomial domain, the valuation of a polynomial will be its degree. Note that the *quotient* q and the *remainder* r in property P2 are not uniquely determined, in general, if $r \neq 0$. For example in the Euclidean domain **Z** if $a = -8$, $b = 3$ then we have

(5) $\quad -8 = (3)(-2) - 2 \quad \text{or} \quad -8 = (3)(-3) + 1$

so that both pairs $q = -2$, $r = -2$ and $q = -3$, $r = 1$ satisfy property P2. There are two different conventions which are adopted in various contexts to make the quotient and remainder unique in **Z**. One convention is to choose the pair q,r such that either $r = 0$ or $\text{sign}(r) = \text{sign}(a)$ (as in the first case of (5)). The other convention is to choose the pair q,r such that either $r = 0$ or $\text{sign}(r) = \text{sign}(b)$ (as in the second case of (5)). Fortunately, when we turn to polynomial domains the quotient and remainder will be uniquely determined.

Any Euclidean domain is a unique factorization domain and therefore GCD's exist (and are unique). Moreover, in a Euclidean domain the GCD can always be expressed in a special convenient form as stated in the following theorem.

Theorem 2.2.

In a Euclidean domain D, let $a,b \in D$ (not both zero). If $g = \text{GCD}(a,b)$ then there exist elements $s,t \in D$ such that

$$g = sa + tb.$$

Proof:

A constructive proof of Theorem 2.2 is presented in the following section. □

Example 2.5.

We stated in Example 2.2 that GCD(18, 30) = 6. We have

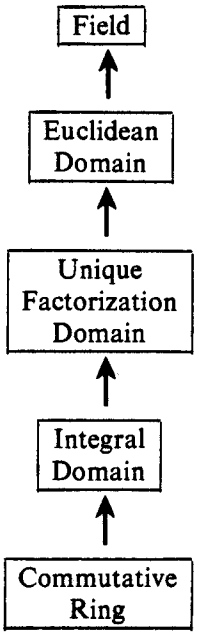
$$6 = s(18) + t(30) \quad \text{with } s = 2 \text{ and } t = -1.$$

Note that in the Euclidean domain **Z** the elements s and t of Theorem 2.2 are not uniquely determined. Two other possible choices for s and t in this example are $s = -3$, $t = 2$ and $s = 7$, $t = -4$. □

Hierarchy of Domains

In this section, we have introduced two new abstract structures intermediate to integral domains and fields. Table 2.3 shows the hierarchy of these domains. It is indicated there that a field F is a Euclidean domain, which can be seen by choosing the trivial valuation $v(a) = 1$ for all $a \in F - \{0\}$. (F is uninteresting as a Euclidean domain; for example, the remainder on division is always zero). It also follows that a field F is a unique factorization domain. (F is a trivial UFD in which every nonzero element is a unit and therefore no element has a prime factorization − there are no primes in F).

Table 2.3. Hierarchy of Domains.



Notation: Upward pointing arrows indicate that a lower domain becomes a higher domain if additional axioms are satisfied.

2.3. THE EUCLIDEAN ALGORITHM

From a computational point of view, we are interested not only in the existence of g = GCD(a,b) and the existence of elements s,t satisfying Theorem 2.2 in any Euclidean domain, but we are also interested in algorithms for computing these values. It might seem at first glance that the proof of Theorem 2.1 is a constructive proof yielding an algorithm for computing GCD(a,b) in any unique factorization domain. However the construction in that proof is based on prime factorizations of a and b and it is computationally much more difficult to determine a prime factorization than to compute GCD(a,b). A very effective algorithm for computing GCD(a,b) in any Euclidean domain will now be developed.

GCD Theory In Euclidean Domains

Theorem 2.3.

Given $a,b \in D$ ($b \neq 0$) where D is a Euclidean domain, let q,r be a quotient and remainder satisfying property P2; i.e.

(6) $\quad a = bq + r$ with $r = 0$ or $v(r) < v(b)$.

Then $\quad$ GCD(a,b) = GCD(b,r).

Proof:

Suppose that g = GCD(b,r). Then from (6) we see that $g \mid a$ and therefore g is a common divisor of a and b. Now if d is *any* common divisor of a and b, we see by rearranging (6) as $r = a - bq$ that $d \mid r$ and therefore d is a common divisor of b and r. But then we must have $d \mid g$ since any common divisor of two elements divides their greatest common divisor. Thus g

must be a *greatest* common divisor of a and b. Therefore $g = \mathrm{GCD}(a,b)$. (Note that g is unit normal by definition.) □

In any integral domain D, it is useful to define

(7) $\mathrm{GCD}(0,0) = 0$

and obviously for any $a,b \in D$:

(8) $\mathrm{GCD}(a,b) = \mathrm{GCD}(b,a)$.

It is also easy to show from the definitions that the following properties hold for any $a,b \in D$:

(9) $\mathrm{GCD}(a,b) = \mathrm{GCD}(n(a), n(b))$;

(10) $\mathrm{GCD}(a,0) = n(a)$;

where $n(a)$ denotes the normal part of a as defined in Definition 2.9.

In any Euclidean domain D, if $a,b \in D$ with $b \neq 0$ let q and r be a quotient and remainder such that

$$a = bq + r \text{ with } r = 0 \text{ or } v(r) < v(b)$$

and define the functions *quo* and *rem* as follows:

(11) $\mathrm{quo}(a,b) = q$;

(12) $\mathrm{rem}(a,b) = r$.

(Note: The above functions are not well-defined, in general, because q and r are not uniquely determined. For the Euclidean domain **Z** we may adopt either of the two conventions mentioned in the preceding section in order to make the above functions well-defined. For the polynomial domains which will be of interest to us later we will see that q and r are uniquely determined by the division property.) For $a,b \in D$ with $b \neq 0$, by a *remainder sequence* for a and b we understand a sequence $\{r_i\}$ generated as follows:

(13) $$\begin{cases} r_0 = b\,; \; r_1 = \mathrm{rem}(a,r_0); \\ r_i = \mathrm{rem}(r_{i-2}, r_{i-1}), \quad i = 2,3,4, \cdots \end{cases}$$

(The sequence is undefined beyond a point where $r_i = 0$ for some i).

Theorem 2.4.

Let $a,b \in D$ ($b \neq 0$) where D is a Euclidean domain. Let $\{r_i\}$ be a remainder sequence for a and b generated as in (13). Then there is a finite index $l \geq 1$ such that $r_l = 0$ and

(14) $\mathrm{GCD}(a,b) = n(r_{l-1})$.

Proof:

Consider the sequence of valuations $\{v(r_i)\}$ formed from the nonzero elements of the sequence $\{r_i\}$. By definition, $\{v(r_i)\}$ is a strictly decreasing sequence of nonnegative integers. Since the first element of this sequence is $v(b)$, there can be at most $v(b)+1$ elements in the sequence. Therefore it must happen that $r_l = 0$ for some $l \leq v(b) + 1$ ($l \geq 1$ because $r_0 = b \neq 0$).

From Theorem 2.3 we have:

(15) $\mathrm{GCD}(a,b) = \mathrm{GCD}(b,r_1) = \mathrm{GCD}(r_0,r_1)$.

If $r_1 = 0$ then $l = 1$ and (14) holds because of (10). Otherwise, we have from Theorem 2.3:

(16) $\mathrm{GCD}(r_{i-2},r_{i-1}) = \mathrm{GCD}(r_{i-1},r_i), \quad 2 \leq i \leq l.$

Now (15) - (16) yield, using (10):

$$\mathrm{GCD}(a,b) = \mathrm{GCD}(r_{l-1}, 0) = n(r_{l-1})$$

which is the desired result. □

The Basic Algorithm

From Theorem 2.4, the GCD of $a,b \in D$ ($b \neq 0$) is simply the normal part of the last nonzero element of a remainder sequence $\{r_i\}$ generated as in (13). If $b = 0$ then GCD(a,b) is given directly by (10). Thus we have a complete specification of the ***Euclidean algorithm*** to compute GCD's in any Euclidean domain, and it is given formally as Algorithm 2.1. Noting (9), we have chosen to take the normal parts of a and b initially in Algorithm 2.1 since this sometimes simplifies the computation. For an actual implementation of Algorithm 2.1 we need only specify the functions rem(a,b) and n(a). Note that Algorithm 2.1 can also be applied to compute LCM(a,b) since if a and b are not both zero then

$$\text{LCM}(a,b) = \frac{\text{n}(ab)}{\text{GCD}(a,b)} .$$

It is conventional to define

$$\text{LCM}(0,0) = 0.$$

Example 2.6.

In the Euclidean domain **Z**, the following function specifications are used for Algorithm 2.1. For any $a \in \mathbf{Z}$, n(a) = $|a|$ as noted in Example 2.3. The rem function for integers is defined as in (12) where the pair q,r is made unique by imposing one of the two conventions discussed in the preceding section. Note that since the **while**-loop in Algorithm 2.1 is entered with nonnegative integers and since either of the two conventions for defining rem will then produce a nonnegative remainder, the value of c on exit from the **while**-loop will be nonnegative. Therefore when applying Algorithm 2.1 in the particular Euclidean domain **Z** the final operation n(c) is unnecessary. □

(Note: The essential ideas in Algorithm 2.1, as it applies to positive integers, date back to Euclid, circa 300 B.C.)

Algorithm 2.1. Euclidean Algorithm.

```
begin
    comment Given a and b in a Euclidean domain D,
        compute g = GCD(a,b);
    c ← n(a); d ← n(b);
    while d ≠ 0 do
        begin
            r ← rem(c,d);
            c ← d;
            d ← r
        end;
    g ← n(c)
end.
```

Example 2.7.

In the Euclidean domain **Z**, if $a = 18$ and $b = 30$ then the sequence of values computed for r, c, and d in Algorithm 2.1 is as follows:

End of iteration no.	r	c	d
0	–	18	30
1	18	30	18
2	12	18	12
3	6	12	6
4	0	6	0

Thus $g = 6$, i.e. GCD(18, 30) = 6 as noted in Example 2.2. □

Extended Euclidean Algorithm

The Euclidean algorithm can be readily extended so that while it computes $g = GCD(a,b)$ it will also compute the elements s,t of Theorem 2.2 which allow g to be expressed as a linear combination of a and b. We present the extended algorithm as Algorithm 2.2 and then justify it by giving a constructive proof of Theorem 2.2. Here and in the sequel, we employ the standard binary operation of *division* which is defined in any integral domain D as follows: if $a,b \in D$ and if a is a multiple of b then by definition, $a = bx$ for some $x \in D$, and we define

$$a/b = x.$$

In particular, if b is a unit in D then any $a \in D$ is a multiple of b (i.e. $a = b(ab^{-1})$) and

$$a/b = ab^{-1}.$$

Note that the quo function (11) is an extension of the division operation since if $a = bx$ then property P2 holds for a and b with $q = x$, $r = 0$ and hence $quo(a,b) = a/b$.

Algorithm 2.2. Extended Euclidean Algorithm.

```
begin
    comment Given a and b in a Euclidean domain D, compute
        g = GCD(a, b) and also compute elements s, t ∈ D
        such that g = sa + tb;
    c ← n(a);   d ← n(b);
    c1 ← 1;     c2 ← 0;
    d1 ← 0;     d2 ← 1;
    while d ≠ 0 do
        begin
            q ← quo(c,d);
            r ← c − q×d;
            r1 ← c1 − q×d1;  r2 ← c2 − q×d2;
            c ← d;
            c1 ← d1;   c2 ← d2;
            d ← r;
            d1 ← r1;   d2 ← r2;
        end;
    g ← n(c);
    s ← c1 / (u(a) × u(c));   t ← c2 / (u(b) × u(c))
end.
```

Note that the two divisions at the end of Algorithm 2.2 are valid in D because u(a), u(b), and u(c) are units in D. Note also that the computation of $g = GCD(a,b)$ in Algorithm 2.2 is identical with the computation in Algorithm 2.1. The proof that the additional statements in Algorithm 2.2 correctly compute the elements s,t is contained in the constructive proof of Theorem 2.2 which we

now present.

Proof of Theorem 2.2:

Let a,b be elements in a Euclidean domain D. We first claim that for $d \neq 0$ the relationships

(17) $c = c_1\, n(a) + c_2\, n(b)$;

(18) $d = d_1\, n(a) + d_2\, n(b)$;

are invariant under the transformations of the while-loop in Algorithm 2.2 – i.e. if (17) - (18) hold at the beginning of the i-th iteration of the while-loop then they hold at the end of the i-th iteration. To see this, define $q = quo(c,d)$, multiply through in equation (18) by q, and subtract from equation (17), yielding

(19) $(c - qd) = (c_1 - qd_1)\, n(a) + (c_2 - qd_2)\, n(b)$.

Now in the terminology of Algorithm 2.2, (19) is

(20) $r = r_1\, n(a) + r_2\, n(b)$.

The remaining transformations in the while-loop simply update c, c_1, c_2, d, d_1, and d_2 in such a way that (18) and (20) imply, at the end of the i-th iteration, (17) and (18), respectively. Thus (17) -(18) are invariant as claimed.

Now if we define

(21) $c = n(a)$; $d = n(b)$; $c_1 = 1$; $c_2 = 0$; $d_1 = 0$; $d_2 = 1$;

then (17) - (18) clearly hold. If $d = 0$ then $b = 0$ and by (10)

(22) $GCD(a,b) = n(a) = c$

and

(23) $c = c_1\, n(a) + c_2\, n(b)$

with c, c_1, c_2 defined as in (21). Otherwise, by Theorem 2.4, the transformations of the while-loop in Algorithm 2.2 may be applied some finite number, l, times yielding, at the end of the l-th iteration, elements c and d satisfying

(24) $d = 0$ and $GCD(a,b) = n(c)$.

But since (17) is invariant, we also have elements $c_1, c_2 \in D$ such that

(25) $c = c_1\, n(a) + c_2\, n(b)$

To complete the proof recall that for all $a \in D$, $a = u(a)\, n(a)$ and $u(a)$ is a unit (i.e. $u(a)$ is invertible). Thus we can divide through by $u(c)$ in (25), yielding

(26) $$n(c) = c_1 \frac{n(a)}{u(c)} + c_2 \frac{n(b)}{u(c)}.$$

Noting that $n(a) = \frac{a}{u(a)}$, $n(b) = \frac{b}{u(b)}$, we have from (22), (23) and from (24), (26) that, in all cases,

$$GCD(a,b) = c_1 \frac{a}{u(a)\, u(c)} + c_2 \frac{b}{u(b)\, u(c)}.$$

Thus

$$GCD(a,b) = sa + tb$$

as required, with $s = \frac{c_1}{u(a)\, u(c)}$ and $t = \frac{c_2}{u(b)\, u(c)}$. □

Example 2.8.

In the Euclidean domain **Z** if $a = 18$ and $b = 30$ then the sequence of values computed for q,c,c_1,c_2,d,d_1, and d_2 in Algorithm 2.2 is as follows.

End of iteration no.	q	c	c_1	c_2	d	d_1	d_2
0	–	18	1	0	30	0	1
1	0	30	0	1	18	1	0
2	1	18	1	0	12	−1	1
3	1	12	−1	1	6	2	−1
4	2	6	2	−1	0	−5	3

Thus $g = 6$, $s = 2$, and $t = -1$; i.e.

$$\text{GCD}(18, 30) = 6 = 2(18) - 1(30)$$

as noted in Example 2.5. □

2.4. UNIVARIATE POLYNOMIAL DOMAINS

For any commutative ring R, the notation R[x] denotes the set of all expressions of the form

$$\textbf{(27)} \quad a(x) = \sum_{k=0}^{m} a_k x^k$$

with $a_k \in R$ $(0 \leqslant k \leqslant m)$, where m is a nonnegative integer. In other words, R[x] denotes the set of all *polynomials* in the indeterminate x with coefficients lying in the ring R (or, more concisely, the set of all *univariate polynomials* over R). The *degree* deg[a(x)] of a nonzero polynomial a(x) as in (27) is the largest integer n such that $a_n \neq 0$. The standard form of a polynomial a(x) is

$$\textbf{(28)} \quad \sum_{k=0}^{n} a_k x^k \quad \text{with} \quad n = \deg[a(x)] \text{ (i.e. with } a_n \neq 0).$$

The exceptional case where $a_k = 0$ for all k is called the *zero polynomial* and its standard form is 0. It is conventional to define deg[0] = $-\infty$. For a polynomial a(x) in the standard form (28), $a_n x^n$ is called the *leading term*, a_n is called the *leading coefficient* (denoted functionally by Lc[a(x)]), and a_0 is called the *constant term*. A polynomial with leading coefficient 1 is called a *monic polynomial*. A polynomial of degree 0 is called a *constant polynomial*. If l denotes the smallest integer such that $a_l \neq 0$ in (28) then the term $a_l x^l$ is called the *trailing term* and a_l is called the *trailing coefficient*. Note that if $a_0 \neq 0$ then the trailing term, trailing coefficient, and constant term are all identical.

The binary operations of addition and multiplication in the commutative ring R are extended to polynomials in the set R[x] as follows. If

$$a(x) = \sum_{k=0}^{m} a_k x^k \quad \text{and} \quad b(x) = \sum_{k=0}^{n} b_k x^k$$

then polynomial addition is defined by

$$\textbf{(29)} \quad c(x) = a(x) + b(x) = \sum_{k=0}^{\max\{m,n\}} c_k x^k$$

where

$$c_k = \begin{cases} a_k + b_k & \text{for } k \leqslant \min\{m,n\} \\ a_k & \text{for } n < k \leqslant m \text{ if } m > n \\ b_k & \text{for } m < k \leqslant n \text{ if } m < n \end{cases}$$

Similarly, if $a(x)$ and $b(x)$ are as above then polynomial multiplication is defined by

$$\textbf{(30)} \quad d(x) = a(x)\,b(x) = \sum_{k=0}^{m+n} d_k x^k$$

where $$d_k = \sum_{i+j=k} a_i b_j.$$

Algebraic Properties of $R[x]$

We now consider the properties of the algebraic structure $R[x]$ under the operations defined by (29) - (30). Since addition and multiplication of polynomials in $R[x]$ are defined in terms of addition and multiplication in the coefficient ring R, it is not surprising that the properties of $R[x]$ are dependent on the properties of R. The following theorem summarizes a number of facts about univariate polynomial domains. The proofs are straightforward but tedious and will be omitted.

Theorem 2.5.

(i) If R is a commutative ring then $R[x]$ is also a commutative ring. The zero (additive identity) in $R[x]$ is the zero polynomial 0 and the (multiplicative) identity in $R[x]$ is the constant polynomial 1.

(ii) If D is an integral domain then $D[x]$ is also an integral domain. The units (invertibles) in $D[x]$ are the constant polynomials a_0 such that a_0 is a unit in the coefficient domain D.

(iii) If D is a unique factorization domain (UFD) then $D[x]$ is also a UFD. The primes (irreducibles) in $D[x]$ are the polynomials which cannot be factored (apart from units and associates) with respect to the coefficient domain D.

(iv) If D is a Euclidean domain then $D[x]$ is a UFD but not (necessarily) a Euclidean domain.

(v) If F is a field then $F[x]$ is a Euclidean domain with the valuation

$$\textbf{(31)} \quad v[a(x)] = \deg[a(x)].$$

Definition 2.15.

In any polynomial domain $D[x]$ over an integral domain D, the polynomials with unit normal leading coefficients are defined to be *unit normal.* □

Example 2.9.

In the polynomial domain $\mathbf{Z}[x]$ over the integers, the units are the constant polynomials 1 and -1. The unit normal polynomials in $\mathbf{Z}[x]$ are 0 and all polynomials with positive leading coefficients. □

Example 2.10.

In the polynomial domain $\mathbf{Q}[x]$ over the field of rational numbers, the units are all nonzero constant polynomials. The unit normal polynomials in $\mathbf{Q}[x]$ are 0 and all monic polynomials (i.e. polynomials with leading coefficient 1). □

At this point let us note some properties which can be easily verified for the degree function in a polynomial domain $D[x]$ over any integral domain D. For the degree of a sum we have

$$\textbf{(32)} \quad \deg[a(x) + b(x)] \leqslant \max\{\deg[a(x)],\ \deg[b(x)]\},$$

with equality holding if $\deg[a(x)] \neq \deg[b(x)]$. For the degree of a product we have

$$\textbf{(33)} \quad \deg[a(x)\,b(x)] = \deg[a(x)] + \deg[b(x)].$$

For the degree of a quotient we have, assuming $b(x) \neq 0$,

$$\textbf{(34)} \quad \deg[\mathrm{quo}(a(x),\ b(x))] = \begin{cases} -\infty & \text{if } \deg[a(x)] < \deg[b(x)] \\ \deg[a(x)] - \deg[b(x)] & \text{otherwise.} \end{cases}$$

In particular note that if $b(x) \mid a(x)$ then we have

(35) $\deg[a(x)/b(x)] = \deg[a(x)] - \deg[b(x)]$

since when $b(x) \mid a(x)$ it follows that either $a(x)=0$ or else $\deg[a(x)] \geqslant \deg[b(x)]$.

We note from Theorem 2.5 that the algebraic structure of a coefficient domain D is inherited in full by the polynomial domain $D[x]$ if D is an integral domain or a UFD, but if D is a Euclidean domain or a field then $D[x]$ does not inherit the Euclidean axioms or the field axioms (see Example 2.12 and Example 2.13). However in the case of a field F, the polynomial domain $F[x]$ becomes a Euclidean domain by choosing the valuation (31). Since by definition $\deg[a(x)] \geqslant 0$ for any nonzero polynomial $a(x)$, the valuation (31) is indeed a mapping from $F[x] - \{0\}$ into the nonnegative integers **N** as required by Definition 2.14. Property P1 can be verified by using (33) since if $a(x), b(x) \in F[x] - \{0\}$ then

$$\deg[a(x)\, b(x)] = \deg[a(x)] + \deg[b(x)] \geqslant \deg[a(x)].$$

Property P2, the division property, is the familiar process of polynomial long division which can be carried out as long as the coefficient domain is a field F. Unlike the Euclidean domain **Z**, in the Euclidean domain $F[x]$ the quotient q and remainder r of property P2 are *unique*.

Example 2.11.

In the Euclidean domain $\mathbf{Q}[x]$ of polynomials over the field **Q** of rational numbers, let

(36) $a(x) = 3x^3 + x^2 + x + 5$, and

(37) $b(x) = 5x^2 - 3x + 1$.

To find the quotient $q(x)$ and remainder $r(x)$ of property P2 in Definition 2.14, we perform polynomial long division:

$$\begin{array}{rl} & \frac{3}{5}x + \frac{14}{25} \\ 5x^2 - 3x + 1 \;\; \overline{)} & 3x^3 + x^2 + x + 5 \\ & 3x^3 - \frac{9}{5}x^2 + \frac{3}{5}x \\ \hline & \frac{14}{5}x^2 + \frac{2}{5}x + 5 \\ & \frac{14}{5}x^2 - \frac{42}{25}x + \frac{14}{25} \\ \hline & \frac{52}{25}x + \frac{111}{25} \end{array}$$

Thus

$$a(x) = b(x)\, q(x) + r(x)$$

where

$$q(x) = \frac{3}{5}x + \frac{14}{25}, \quad \text{and}$$

$$r(x) = \frac{52}{25}x + \frac{111}{25}. \qquad \square$$

Example 2.12.

The polynomial domain $\mathbf{Z}[x]$ over the integers **Z** is an integral domain, in fact a UFD (because **Z** is a UFD), but $\mathbf{Z}[x]$ is not a Euclidean domain with the 'natural' valuation $v[a(x)] = \deg[a(x)]$. For consider the polynomials $a(x)$, $b(x)$ given in (36) - (37). Note that $a(x)$, $b(x) \in \mathbf{Z}[x]$. Property P2 is not satisfied by using the polynomials $q(x)$, $r(x)$ of Example 2.11 because $q(x), r(x) \notin \mathbf{Z}[x]$. If we assume the existence of polynomials $q(x), r(x) \in \mathbf{Z}[x]$ satisfying property P2 for the polynomials (36) - (37), then since $\deg[r(x)] < \deg[b(x)] = 2$ it is easy to argue

that we must have

$$3x^3 + x^2 + x + 5 = (5x^2 - 3x + 1)(q_1 x + q_0) + (r_1 x + r_0)$$

for some coefficients $q_1, q_0, r_1, r_0 \in \mathbf{Z}$. But this implies

(38) $3 = 5q_1$

which is a contradiction since (38) has no solution in **Z**. Thus property P2 does not hold in the domain $\mathbf{Z}[x]$ for the polynomials (36) - (37) and therefore $\mathbf{Z}[x]$ is not a Euclidean domain. □

Example 2.12 shows that the coefficient domain must be a field in order to carry out polynomial long division because only in a field will equations of the form (38) always have a solution. A more concise argument for Example 2.12 could have been obtained by noting the uniqueness of $q(x)$, $r(x)$ in polynomial long division. The next example verifies that a polynomial domain $F[x]$ over a field F is not itself a field.

Example 2.13.

In a polynomial domain $F[x]$ over any field F, the polynomial x has no inverse. For if it had an inverse, say $q(x)$, then

$$\begin{aligned} x\ q(x) = 1 &\Rightarrow \deg[x] + \deg[q(x)] = \deg[1]. \\ &\Rightarrow 1 + \deg[q(x)] = 0 \\ &\Rightarrow \deg[q(x)] = -1 \end{aligned}$$

which is impossible. Therefore $F[x]$ is not a field. □

GCD Computation in $F[x]$

Since the univariate polynomial domain $F[x]$ over a field F is a Euclidean domain, the Euclidean algorithm (Algorithm 2.1) and the extended Euclidean algorithm (Algorithm 2.2) can be used to compute GCD's in $F[x]$. For a nonzero polynomial $a(x) \in F[x]$ with leading coefficient a_n, the normal part and unit part of $a(x)$ satisfy:

$$n(a(x)) = \frac{a(x)}{a_n};$$

$$u(a(x)) = a_n$$

Note that $a_n \neq 0$ is a unit in $F[x]$ because it is a unit in F. As usual, $n(0) = 0$ and $u(0) = 1$. For $a(x), b(x) \in F[x]$ with $b(x) \neq 0$, the quotient and remainder of property P2 are unique so the quo and rem functions in (11) - (12) are well-defined and the remainder sequence $\{r_i(x)\}$ defined by (13) is unique.

Example 2.14.

In the Euclidean domain $\mathbf{Q}[x]$, let

(39) $a(x) = 48x^3 - 84x^2 + 42x - 36;$

(40) $b(x) = -4x^3 - 10x^2 + 44x - 30.$

The sequence of values computed for $r(x)$, $c(x)$, and $d(x)$ in Algorithm 2.1 is as follows. (Of course $a(x)$, $b(x)$, $r(x)$, $c(x)$, and $d(x)$ are denoted by a, b, r, c, and d, respectively, in Algorithm 2.1. It is common practice to use the former notation (called 'functional notation') for polynomials but clearly the latter notation is also acceptable when the underlying domain is understood).

End of iteration no.	r(x)	c(x)	d(x)
0	–	$x^3-\frac{7}{4}x^2+\frac{7}{8}x-\frac{3}{4}$	$x^3+\frac{5}{2}x^3-11x+\frac{15}{2}$
1	$-\frac{17}{4}x^2+\frac{95}{8}x-\frac{33}{4}$	$x^3+\frac{5}{2}x^2-11x+\frac{15}{2}$	$-\frac{17}{4}x^2+\frac{95}{8}x-\frac{33}{4}$
2	$\frac{535}{289}x-\frac{1605}{578}$	$-\frac{17}{4}x^2+\frac{95}{8}x-\frac{33}{4}$	$\frac{535}{289}x-\frac{1605}{578}$
3	0	$\frac{535}{289}x-\frac{1605}{578}$	0

Thus $g(x) = n(\frac{535}{289}x - \frac{1605}{578}) = x - \frac{3}{2}$. □

Example 2.15.

In the Euclidean domain $\mathbf{Q}[x]$, if Algorithm 2.2 is applied to the polynomials (39) - (40) of Example 2.14 then three iterations of the while-loop are required as in Example 2.14. At the end of the third iteration we have

$$r(x) = 0; \quad c(x) = \frac{535}{289}x - \frac{1605}{578}; \quad d(x) = 0$$

as before. We also have

$$c_1(x) = \frac{4}{17}x + \frac{360}{289};$$

$$c_2(x) = -\frac{4}{17}x - \frac{71}{289}.$$

Thus,

$$g(x) = n(c(x)) = x - \frac{3}{2};$$

$$s(x) = \frac{c_1(x)}{48\left(\frac{535}{289}\right)} = \frac{17}{6420}x + \frac{3}{214};$$

$$t(x) = \frac{c_2(x)}{-4\left(\frac{535}{289}\right)} = \frac{17}{535}x + \frac{71}{2140}.$$

It is readily verified that

$$s(x)\,a(x) + t(x)\,b(x) = x - \frac{3}{2}. \quad \square$$

In the Euclidean domain $F[x]$ of univariate polynomials over a field F, an important application of the extended Euclidean algorithm in later chapters will be to solve the *polynomial diophantine equation*

$$\sigma(x)\,a(x) + \tau(x)\,b(x) = c(x)$$

where $a(x)$, $b(x)$, $c(x) \in F[x]$ are given polynomials and $\sigma(x)$, $\tau(x) \in F[x]$ are to be determined (if possible). The following theorem gives sufficient conditions for the existence and uniqueness of a solution to this polynomial diophantine equation and a constructive proof is given. Note that an important special case of the theorem occurs when $a(x)$ and $b(x)$ are relatively prime in which case

the given polynomial diophantine equation can be solved for any given right hand side $c(x)$.

Theorem 2.6.

Let $F[x]$ be the Euclidean domain of univariate polynomials over a field F. Let $a(x)$, $b(x) \in F[x]$ be given nonzero polynomials and let $g(x) = GCD(a(x),b(x)) \in F[x]$. Then for any given polynomial $c(x) \in F[x]$ such that $g(x) \mid c(x)$ there exist unique polynomials $\sigma(x)$, $\tau(x) \in F[x]$ such that

$$\textbf{(41)} \quad \sigma(x)\, a(x) + \tau(x)\, b(x) = c(x)$$

and

$$\textbf{(42)} \quad \deg[\sigma(x)] < \deg[b(x)] - \deg[g(x)].$$

Moreover, if $\deg[c(x)] < \deg[a(x)] + \deg[b(x)] - \deg[g(x)]$ then $\tau(x)$ satisfies

$$\textbf{(43)} \quad \deg[\tau(x)] < \deg[a(x)] - \deg[g(x)].$$

Proof:

Existence:

The extended Euclidean algorithm can be applied to compute polynomials $s(x)$, $t(x) \in F[x]$ satisfying the equation

$$s(x)\, a(x) + t(x)\, b(x) = g(x).$$

Then since $g(x) \mid c(x)$ it is easily seen that

$$\textbf{(44)} \quad (s(x)\, c(x) / g(x))\, a(x) + (t(x)\, c(x) / g(x))\, b(x) = c(x).$$

We therefore have a solution of equation (41), say $\tilde{\sigma}(x) = s(x)\, c(x) / g(x)$ and $\tilde{\tau}(x) = t(x)\, c(x) / g(x)$. However the degree constraint (42) will not in general be satisfied by this solution so we will proceed to show how to reduce the degree. Writing (44) in the form

$$\textbf{(45)} \quad \tilde{\sigma}(x)\, (a(x) / g(x)) + \tilde{\tau}(x)\, (b(x) / g(x)) = c(x) / g(x),$$

we apply Euclidean division of $\tilde{\sigma}(x)$ by $(b(x) / g(x))$ yielding $q(x)$, $r(x) \in F[x]$ such that

$$\textbf{(46)} \quad \tilde{\sigma}(x) = (b(x) / g(x))\, q(x) + r(x) \quad \text{where } \deg[r(x)] < \deg[b(x)] - \deg[g(x)].$$

Now define $\sigma(x) = r(x)$ and note that (42) is satisfied. Also define $\tau(x) = \tilde{\tau}(x) + q(x)\, (a(x) / g(x))$. It is easily verified by using (45) and (46) that

$$\sigma(x)\, (a(x) / g(x)) + \tau(x)\, (b(x) / g(x)) = c(x) / g(x).$$

Equation (41) follows immediately.

Uniqueness:

Let $\sigma_1(x)$, $\tau_1(x) \in F[x]$ and $\sigma_2(x)$, $\tau_2(x) \in F[x]$ be two pairs of polynomials satisfying (41) - (42). The two different equations of the form (41) can be written in the form

$$\sigma_1(x)\, (a(x) / g(x)) + \tau_1(x)\, (b(x) / g(x)) = c(x) / g(x);$$

$$\sigma_2(x)\, (a(x) / g(x)) + \tau_2(x)\, (b(x) / g(x)) = c(x) / g(x)$$

which yields on subtraction

$$\textbf{(47)} \quad (\sigma_1(x) - \sigma_2(x))\, (a(x) / g(x)) = -(\tau_1(x) - \tau_2(x))\, (b(x) / g(x)).$$

Now since $a(x) / g(x)$ and $b(x) / g(x)$ are relatively prime it follows from (47) that

$$\textbf{(48)} \quad (b(x) / g(x)) \mid (\sigma_1(x) - \sigma_2(x)).$$

But from the degree constraint (42) satisfied by $\sigma_1(x)$ and $\sigma_2(x)$ it follows that

(49) $\deg[\sigma_1(x) - \sigma_2(x)] < \deg[b(x) / g(x)]$.

Now (48) and (49) together imply that $\sigma_1(x) - \sigma_2(x) = 0$. It then follows from (47) that $\tau_1(x) - \tau_2(x) = 0$ since $b(x) / g(x) \neq 0$. Therefore $\sigma_1(x) = \sigma_2(x)$ and $\tau_1(x) = \tau_2(x)$.

Final Degree Constraint:

It remains to prove (43). From (41) we can write

$$\tau(x) = (c(x) - \sigma(x)\, a(x)) / b(x)$$

so that

(50) $\deg[\tau(x)] = \deg[c(x) - \sigma(x)\, a(x)] - \deg[b(x)]$.

Now if $\deg[c(x)] \geqslant \deg[\sigma(x)\, a(x)]$ then from (50)

$$\deg[\tau(x)] \leqslant \deg[c(x)] - \deg[b(x)] < \deg[a(x)] - \deg[g(x)]$$

as long as $\deg[c(x)] < \deg[a(x)] + \deg[b(x)] - \deg[g(x)]$ as stated. Otherwise if $\deg[c(x)] < \deg[\sigma(x)\, a(x)]$ (in which case the stated degree bound for $c(x)$ also holds because of (42)) then from (50)

$$\deg[\tau(x)] = \deg[\sigma(x)\, a(x)] - \deg[b(x)] < \deg[a(x)] - \deg[g(x)]$$

where the last inequality follows from (42). Thus (43) is proved. □

The polynomial domains of most interest in symbolic computation are multivariate polynomials (i.e. polynomials in one *or more* indeterminates) over the integers **Z**, or over the rationals **Q**, or over a finite field F. In this section on univariate polynomials we have noted that **Q**[x] and F[x] are Euclidean domains so that the Euclidean algorithm can be used to perform the important operation of computing GCD's. In the univariate polynomial domain **Z**[x] over the integers it would be possible to compute GCD's (and other important computations) by embedding **Z**[x] in the larger domain **Q**[x] so that the coefficient domain is a field. However, coefficient arithmetic in **Q** is rather more expensive than arithmetic in **Z** so that in practice we prefer to develop a GCD algorithm that is valid in the UFD **Z**[x]. More significantly, when dealing with multivariate polynomials in two or more indeterminates it turns out that the multivariate polynomial domain is a UFD but not a Euclidean domain *even if* the coefficient domain is a field. Hence further discussion of GCD computation in **Z**[x] will be postponed to a later section after we have discussed multivariate polynomial domains, where the underlying algebraic structure will be the UFD rather than the Euclidean domain.

2.5. MULTIVARIATE POLYNOMIAL DOMAINS

Bivariate Polynomials

For any commutative ring R, the notation R[x_1, x_2] denotes the set of all expressions of the form

(51) $$a(x_1, x_2) = \sum_{i=0}^{m_1} \sum_{j=0}^{m_2} a_{i,j} x_1^i x_2^j$$

with $a_{i,j} \in R$ ($0 \leqslant i \leqslant m_1$, $0 \leqslant j \leqslant m_2$), where m_1 and m_2 are nonnegative integers. In other words, R[x_1, x_2] denotes the set of *bivariate polynomials* over the ring R. For example, one polynomial in the set **Z**[x,y] is the bivariate polynomial

degree $\deg[a_{\mathbf{e}}\mathbf{x}^{\mathbf{e}}]$ *of a term* in a multivariate polynomial $a(\mathbf{x})$, where $\mathbf{e} = (e_1, \ldots, e_v)$, is the value $\sum_{i=1}^{v} e_i$. The *total degree* $\deg[a(\mathbf{x})]$ *of a polynomial* $a(\mathbf{x}) \neq 0$ is the maximum of the total degrees of all of its nonzero terms. It is conventional to define $\deg[0] = -\infty$, while $\partial[0]$ is undefined. A polynomial with total degree 0 is called a *constant polynomial.*

A Recursive View of $R[\mathbf{x}]$

It is convenient to define the operations of addition and multiplication on multivariate polynomials in $R[x_1, \ldots, x_v]$ in terms of the basic operations in a univariate polynomial ring defined by (29) - (30). This can be done by using a different, but equivalent, definition of the set $R[x_1, \ldots, x_v]$. The new definition will be recursive. Let us first consider the case of bivariate polynomials in the indeterminates x_1 and x_2. Recalling that the set $R[x_2]$ of univariate polynomials over a commutative ring R forms a commutative ring, we may use it as a coefficient ring and define a new univariate polynomial ring $R[x_2][x_1]$ of polynomials in the indeterminate x_1, with coefficients lying in the commutative ring $R[x_2]$. By Theorem 2.5, $R[x_2][x_1]$ is a commutative ring with the operations of addition and multiplication defined by (29) - (30) in terms of the operations in the coefficient ring $R[x_2]$. It is easy to see that the set of expressions in $R[x_2][x_1]$ is the set of all expressions of the form (51) which we have denoted by $R[x_1, x_2]$. Therefore we identify

$$\textbf{(55)} \quad R[x_1, x_2] = R[x_2][x_1]$$

and this identification serves to define the arithmetic operations on bivariate polynomials. (Clearly, we should be able to identify $R[x_1, x_2]$ as well with $R[x_1][x_2]$. The operations of addition and multiplication in $R[x_1][x_2]$ are defined differently than the operations in $R[x_2][x_1]$ but it is straightforward to prove that the commutative rings $R[x_1][x_2]$ and $R[x_2][x_1]$ are isomorphic.[3] Therefore we are justified in identifying all three of these rings).

Turning now to multivariate polynomials in $v \geqslant 2$ indeterminates, a recursive definition of $R[x_1, \ldots, x_v]$ is given by

$$\textbf{(56)} \quad R[x_1, \ldots, x_v] = R[x_2, \ldots, x_v][x_1].$$

Applying (56) recursively to $R[x_2, \ldots, x_v]$ leads to the identification

$$R[x_1, \ldots, x_v] = R[x_v][x_{v-1}] \cdots [x_1].$$

Thus from knowledge of the operations in $R[x_v]$ we define the operations in $R[x_v][x_{v-1}]$, and from $R[x_v][x_{v-1}]$ to $R[x_v][x_{v-1}][x_{v-2}]$, etc. (Again, the order of singling out indeterminates as in (56) is not important algebraically since the rings obtained by different orderings of the indeterminates can be shown to be isomorphic). If the multivariate polynomial ring $R[x_1, \ldots, x_v]$ is viewed as in (56) then we refer to x_1 as the *main variable* and to $x_2, \ldots, x_v$ as the *auxiliary variables*, and we consider a polynomial $a(\mathbf{x}) \in R[x_1, \ldots, x_v]$ as a univariate polynomial in the main variable with coefficients lying in the ring of polynomials in the auxiliary variables.

Example 2.17.

The polynomial $a(x,y) \in \mathbf{Z}[x,y]$ given in (52) may be viewed as a polynomial in the ring $\mathbf{Z}[y][x]$:

$$a(x,y) = (5y^2)x^3 - (y^4 + 3y^2)x^2 + (7y^2 + 2y - 2)x + (4y^4 + 5). \quad \square$$

For a polynomial $a(\mathbf{x}) \in R[x_1, \ldots, x_v]$ we sometimes refer to the *degree of* $a(\mathbf{x})$ *in the i-th variable*, denoted $\partial_i[a(\mathbf{x})]$, by which we mean the degree of $a(\mathbf{x})$ considered as a univariate

3. Two rings R_1 and R_2 are *isomorphic* if there is a mapping $\phi: R_1 \rightarrow R_2$ which is bijective (i.e. one-to-one and onto) and which preserves all of the ring operations. For a precise definition see chapter 5.

polynomial in the ring $R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v][x_i]$

Example 2.18.

Let $a(x,y) \in \mathbf{Z}[x,y]$ be the bivariate polynomial given in (52). The leading term of $a(x,y)$ is $5x^3y^2$ and the leading coefficient is 5. The values of the various degree functions are:

$$\partial[a(x,y)] = (3,2); \quad \deg[a(x,y)] = 6;$$

$$\partial_1[a(x,y)] = 3; \quad \partial_2[a(x,y)] = 4. \quad \square$$

Algebraic Properties of $R[\mathbf{x}]$

The algebraic properties of a multivariate polynomial ring $R[\mathbf{x}]$, for various choices of algebraic structure R, can be deduced immediately from the recursive view of $R[\mathbf{x}]$ and Theorem 2.5. These properties are summarized in the following theorem whose proof is now trivial.

Theorem 2.7.

(i) If R is a commutative ring then $R[\mathbf{x}]$ is also a commutative ring. The zero in $R[\mathbf{x}]$ is the zero polynomial 0 and the identity in $R[\mathbf{x}]$ is the constant polynomial 1.

(ii) If D is an integral domain then $D[\mathbf{x}]$ is also an integral domain. The units in $D[\mathbf{x}]$ are the constant polynomials a_0 such that a_0 is a unit in the coefficient domain D.

(iii) If D is a UFD then $D[\mathbf{x}]$ is also a UFD.

(iv) If D is a Euclidean domain then $D[\mathbf{x}]$ is UFD but not a Euclidean domain.

(v) If F is field then $F[\mathbf{x}]$ is a UFD but not a Euclidean domain if the number of indeterminates is greater than one. $\square$

Definition 2.17.

In any multivariate polynomial domain $D[\mathbf{x}]$ over an integral domain D, the polynomials with unit normal leading coefficients are defined to be *unit normal.* $\square$

At this point we note some of the properties of the various degree functions which have been introduced for multivariate polynomials. It can be readily verified that the following properties hold for nonzero polynomials in a domain $D[\mathbf{x}]$ over any integral domain D.

(57) $\partial[a(\mathbf{x}) + b(\mathbf{x})] \leqslant \max\{\partial[a(\mathbf{x})], \partial[b(\mathbf{x})]\}$.

(58) $\partial[a(\mathbf{x})\,b(\mathbf{x})] = \partial[a(\mathbf{x})] + \partial[b(\mathbf{x})]$.

(59) $\partial_i[a(\mathbf{x}) + b(\mathbf{x})] \leqslant \max\{\partial_i[a(\mathbf{x})], \partial_i[b(\mathbf{x})]\}$.

(60) $\partial_i[a(\mathbf{x})\,b(\mathbf{x})] = \partial_i[a(\mathbf{x})] + \partial_i[b(\mathbf{x})]$.

(61) $\deg[a(\mathbf{x}) + b(\mathbf{x})] \leqslant \max\{\deg[a(\mathbf{x})], \deg[b(\mathbf{x})]\}$.

(62) $\deg[a(\mathbf{x})\,b(\mathbf{x})] = \deg[a(\mathbf{x})] + \deg[b(\mathbf{x})]$.

In (57) - (58), the addition operation on degree vectors is the familiar operation of vector addition (component-by-component addition) and the 'order' operations $\leqslant$ and max are well-defined by the lexicographical ordering of exponent vectors defined in Definition 2.16.

The concept of the derivative of a polynomial can be defined algebraically. For a univariate polynomial

$$a(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$$

(where D is an arbitrary integral domain) the *derivative* of $a(x)$ is defined by

$$a'(x) = \sum_{k=0}^{n-1} (k + 1)\, a_{k+1}\, x^k \in D[x].$$

It is straightforward to show (using completely algebraic arguments) that the familiar properties of derivatives hold:

(i) if $a(x) = b(x) + c(x)$ then $a'(x) = b'(x) + c'(x)$;

(ii) if $a(x) = b(x)\, c(x)$ then $a'(x) = b(x)\, c'(x) + b'(x)\, c(x)$;

(iii) if $a(x) = b(c(x))$ then $a'(x) = b'(c(x))\, c'(x)$.

For a multivariate polynomial $a(x_1, \ldots, x_v) \in D[x_1, \ldots, x_v]$ over an arbitrary integral domain D the *partial derivative* of $a(x_1, \ldots, x_v)$ *with respect to* x_i, denoted $a_{x_i}(x_1, \ldots, x_v)$, is simply the ordinary derivative of $a(x_1, \ldots, x_v)$ considered as a univariate polynomial in the domain $D[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v][x_i]$. In later chapters it will be necessary to use the concept of a *Taylor series expansion* in the sense of the following Theorem 2.8 and also the bivariate version as presented in Theorem 2.9.

Theorem 2.8.

Let $a(x) \in D[x]$ be a univariate polynomial over an arbitrary integral domain D. In the polynomial domain $D[x][y] = D[x,y]$,

$$a(x + y) = a(x) + a'(x)y + b(x,y)y^2$$

for some polynomial $b(x,y) \in D[x,y]$.

Proof:

First note that $x + y$ is a polynomial in the domain $D[x,y]$ and since $a(x) \in D[x]$ it follows that $a(x + y) \in D[x,y]$. Now any bivariate polynomial in $D[x,y]$, and in particular $a(x + y)$, may be expressed in the following form:

(63) $$a(x + y) = a_0(x) + a_1(x)y + b(x,y)y^2$$

where $a_0(x)$, $a_1(x) \in D[x]$ and $b(x,y) \in D[x,y]$ (by simply writing first all terms independent of y, then all terms in which y appears linearly, and noting that what remains must have y^2 as a factor). It remains to show that $a_0(x) = a(x)$ and that $a_1(x) = a'(x)$.

Setting $y = 0$ in (63) immediately yields $a_0(x) = a(x)$. Taking the partial derivative with respect to y on both sides of equation (63) yields

$$a'(x + y) = a_1(x) + 2\,b(x,y)y + b_y(x,y)y^2.$$

Setting $y = 0$ then yields $a_1(x) = a'(x)$. □

Theorem 2.9.

Let $a(x,y) \in D[x,y]$ be a bivariate polynomial over an arbitrary integral domain D. In the polynomial domain $D[x,y][\xi, \eta] = D[x,y,\xi,\eta]$,

$$a(x+\xi,\ y+\eta) = a(x,y) + a_x(x,y)\xi + a_y(x,y)\eta + b_1(x,y,\xi,\eta)\xi^2 + b_2(x,y,\xi,\eta)\xi\eta + b_3(x,y,\xi,\eta)\eta^2$$

for some polynomials $b_1(x,y,\xi,\eta)$, $b_2(x,y,\xi,\eta)$, $b_3(x,y,\xi,\eta) \in D[x,y,\xi,\eta]$.

Proof:

First consider the (univariate) polynomial

$$c(x) = a(x,y) \in D[y][x].$$

From Theorem 2.8 we have

$$c(x + \xi) = c(x) + c'(x)\xi + d(x,\xi)\xi^2$$

for some polynomial $d(x, \xi) \in D[y][x, \xi]$, or equivalently

(64) $a(x + \xi, y) = a(x,y) + a_x(x,y)\xi + e(x,y,\xi)\xi^2$

for some polynomial $e(x,y,\xi) \in D[x,y,\xi]$. Next consider the (univariate) polynomial

$f(y) = a(x + \xi, y) \in D[x, \xi][y]$.

Applying Theorem 2.8 to express $f(y + \eta)$ we get

(65) $a(x + \xi, y + \eta) = a(x + \xi, y) + a_y(x + \xi, y)\eta + g(x, y, \xi, \eta)\eta^2$

for some polynomial $g(x, y, \xi, \eta) \in D[x, y, \xi, \eta]$. In (65), if we express the polynomial $a(x + \xi, y)$ directly as given by (64) and if we express the polynomial $a_y(x + \xi, y)$ also in the form indicated by (64), we get

(66) $a(x+\xi, y+\eta) = a(x,y) + a_x(x,y)\xi + e(x,y,\xi)\xi^2 + a_y(x,y)\eta$
$+ a_{yx}(x,y)\xi\eta + \tilde{e}(x,y,\xi)\xi^2\eta + g(x,y,\xi,\eta)\eta^2$

where $a_{yx}(x,y)$ denotes the partial derivative with respect to x of the polynomial $a_y(x, y) \in D[x,y]$. Equation (66) can be put into the form appearing in the statement of the theorem. □

We see from Theorem 2.7 that a domain **D[x]** of multivariate polynomials forms a unique factorization domain (UFD) (as long as the coefficient domain D is a UFD) but that **D[x]** forms no higher algebraic structure in the hierarchy of Table 2.3 even if D is a higher algebraic structure (except in the case of univariate polynomials). Thus the UFD is the abstract structure which forms the setting for multivariate polynomial manipulation. In the next section we develop an algorithm for GCD computation in this new setting.

2.6. THE PRIMITIVE PRS EUCLIDEAN ALGORITHM

The Euclidean algorithm of section 2.3 cannot be used to compute GCD's in a multivariate polynomial domain **D[x]** because **D[x]** is not a Euclidean domain. However **D[x]** is a UFD (if D is a UFD) and we are assured by Theorem 2.1 that GCD's exist and are unique in any UFD.

Example 2.19.

In the UFD **Z**[x] let $a(x)$, $b(x)$ be the polynomials (39) - (40) defined in Example 2.14; namely,

$a(x) = 48x^3 - 84x^2 + 42x - 36;$

$b(x) = -4x^3 - 10x^2 + 44x - 30.$

The unique unit normal factorizations of $a(x)$ and $b(x)$ in **Z**[x] are

$a(x) = (2)(3)(2x - 3)(4x^2 - x + 2);$

$b(x) = (-1)(2)(2x - 3)(x - 1)(x + 5)$

where we note that $u(a(x)) = 1$ has not been explicitly written, and $u(b(x)) = -1$. Thus

$GCD(a(x), b(x)) = 2(2x - 3) = 4x - 6.$ □

Example 2.20.

In the Euclidean domain $\mathbf{Q}[x]$ let $a(x)$, $b(x)$ be the polynomials (39) - (40) as in the previous example. The unique unit normal factorizations of $a(x)$ and $b(x)$ in $\mathbf{Q}[x]$ are

$$a(x) = (48)(x - \frac{3}{2})(x^2 - \frac{1}{4}x + \frac{1}{2});$$

$$b(x) = (-4)(x - \frac{3}{2})(x - 1)(x + 5)$$

where we note that $u(a(x)) = 48$ and $u(b(x)) = -4$. Thus

$$GCD(a(x), b(x)) = x - \frac{3}{2}.$$

as noted in Example 2.14. □

As in the case of Euclidean domains, it is not practical to compute the GCD of $a(\mathbf{x})$, $b(\mathbf{x}) \in D[\mathbf{x}]$ by determining the prime factorizations of $a(\mathbf{x})$ and $b(\mathbf{x})$ but rather we will see that there is a GCD algorithm for the UFD $D[\mathbf{x}]$ which is very similar to the Euclidean algorithm. The new algorithm will be developed for the univariate polynomial domain $D[x]$ over a UFD D and then we will see that it applies immediately to the multivariate polynomial domain $D[\mathbf{x}]$ by the application of recursion.

Primitive Polynomials

We have noted in an earlier section that if elements in an integral domain are split into their unit parts and normal parts then the GCD of two elements is simply the GCD of their normal parts (see equation (9)). It is convenient in a polynomial domain $D[x]$ to further split the normal part into a part lying in the coefficient domain D and a purely polynomial part. For example, the unit normal factorizations of $a(x)$, $b(x) \in \mathbf{Z}[x]$ in Example 2.19 consist of a unit followed by integer factors followed by polynomial factors and similarly $GCD(a(x), b(x))$ consists of integer factors followed by polynomial factors.

Definition 2.18.

In an integral domain D, the *GCD of n elements* $a_1, \ldots, a_n \in D$ is defined recursively for $n > 2$ by:

$$GCD(a_1, \ldots, a_n) = GCD(GCD(a_1, \ldots, a_{n-1}), a_n).$$

The $n \geqslant 2$ elements $a_1, \ldots, a_n \in D$ are called *relatively prime* if $GCD(a_1, \ldots, a_n) = 1$. □

Definition 2.19.

In a polynomial domain $D[x]$ over a UFD D, a nonzero polynomial $a(x)$ is called *primitive* if it is a unit normal polynomial and its coefficients are relatively prime. In particular, if $a(x)$ has exactly one nonzero term then it is primitive if and only if it is monic. □

Definition 2.20.

In a polynomial domain $D[x]$ over a UFD D, the *content* of a nonzero polynomial $a(x)$, denoted $cont[a(x)]$, is defined to be the (unique unit normal) GCD of the coefficients of $a(x)$. Any nonzero polynomial $a(x) \in D[x]$ has a unique representation in the form

$$a(x) = u(a(x))\ cont[a(x)]\ pp[a(x)]$$

where $pp[a(x)]$ is a primitive polynomial called the *primitive part* of $a(x)$. It is convenient to define $cont[0] = 0$ and $pp[0] = 0$. □

It is a classical result (known as Gauss's Lemma) that the product of any two primitive polynomials is itself primitive. It follows from the above definitions that the GCD of two polynomials is the product of the GCD of their contents and the GCD of their primitive parts; notationally,

(67) $\mathrm{GCD}(a(x), b(x)) = \mathrm{GCD}(\mathrm{cont}[a(x)], \mathrm{cont}[b(x)])\ \mathrm{GCD}(\mathrm{pp}[a(x)], \mathrm{pp}[b(x)])$.

By definition, the computation of the GCD of the contents of $a(x)$, $b(x) \in D[x]$ is a computation in the coefficient domain D. Assuming that we know how to compute GCD's in D, we may restrict our attention to the computation of GCD's of *primitive* polynomials in $D[x]$.

Example 2.21.

For the polynomials $a(x)$, $b(x) \in \mathbf{Z}[x]$ considered in Example 2.19 we have:

$$\mathrm{cont}[a(x)] = 6; \quad \mathrm{cont}[b(x)] = 2;$$
$$\mathrm{pp}[a(x)] = 8x^3 - 14x^2 + 7x - 6;$$
$$\mathrm{pp}[b(x)] = 2x^3 + 5x^2 - 22x + 15.$$

For the same polynomials considered as elements in the domain $\mathbf{Q}[x]$ as in Example 2.20 we have:

$$\mathrm{cont}[a(x)] = 1; \quad \mathrm{cont}[b(x)] = 1;$$
$$\mathrm{pp}[a(x)] = x^3 - \frac{7}{4}x^2 + \frac{7}{8}x - \frac{3}{4};$$
$$\mathrm{pp}[b(x)] = x^3 + \frac{5}{2}x^2 - 11x + \frac{15}{2}. \quad \square$$

Pseudo-Division of Polynomials

The Euclidean algorithm is based on the computation of a remainder sequence which is defined in terms of the division property in a Euclidean domain. For a non-Euclidean domain $D[x]$ the division property does not hold. However there is a very similar 'pseudo-division property' which holds in any polynomial domain $D[x]$ over a UFD D. This new property can be understood by considering the UFD $\mathbf{Z}[x]$ of univariate polynomials over the integers.

Consider the polynomials $a(x)$, $b(x)$ given by (36) - (37) in Example 2.11. As polynomials in the Euclidean domain $\mathbf{Q}[x]$, we found in Example 2.11 that the division property holds in the form:

(68) $$(3x^3 + x^2 + x + 5) = (5x^2 - 3x + 1)\left(\frac{3}{5}x + \frac{14}{25}\right) + \left(\frac{52}{25}x + \frac{111}{25}\right).$$

Note that the leading coefficient of $b(x)$ is 5 and that the only denominators appearing in the coefficients of the quotient and remainder in (68) are 5 and 5^2. Therefore in this example, if we started with the polynomials $\tilde{a}(x)$ and $b(x)$ where

$$\tilde{a}(x) = 5^2\, a(x)$$

then we would have the following relationships among polynomials with *integer coefficients:*

(69) $$5^2(3x^3 + x^2 + x + 5) = (5x^2 - 3x + 1)(15x + 14) + (52x + 111).$$

Equation (69) is an instance of the pseudo-division property which holds in any polynomial domain $D[x]$ over a UFD D, just as equation (68) is an instance of the division property in a Euclidean domain. The generalization of (69) is obtained by close examination of the process of polynomial long division in a domain $D[x]$. If $\deg[a(x)] = m$, $\deg[b(x)] = n$, $m \geq n \geq 0$ and if the leading coefficient of $b(x)$ is β then viewing the division of $a(x)$ by $b(x)$ as operations in the coefficient domain D we find that the only divisions are divisions by β and such divisions occur $m - n + 1$ times. We thus have the following result.

Pseudo-Division Property (Property P3).

Let $D[x]$ be a polynomial domain over a UFD D. For all $a(x)$, $b(x) \in D[x]$ with $b(x) \neq 0$ and $\deg[a(x)] \geqslant \deg[b(x)]$, there exist polynomials $q(x)$, $r(x) \in D[x]$ such that

P3: $\beta^l a(x) = b(x)\, q(x) + r(x)$

with $\deg[r(x)] < \deg[b(x)]$, where $\beta = \mathrm{Lc}[b(x)]$ and $l = \deg[a(x)] - \deg[b(x)] + 1$. □

For given polynomials $a(x)$, $b(x) \in D[x]$ the polynomials $q(x)$ and $r(x)$ appearing in property P3 are called, respectively, the *pseudo-quotient* and *pseudo-remainder*. Functionally we use the notation $\mathrm{pquo}[a(x), b(x)]$ and $\mathrm{prem}[a(x), b(x)]$ for the pseudo-quotient and pseudo-remainder, respectively, and we extend the definitions of these functions to the case $\deg[a(x)] < \deg[b(x)]$ by defining in the latter case $\mathrm{pquo}[a(x), b(x)] = 0$ and $\mathrm{prem}[a(x), b(x)] = a(x)$. (Note that these special definitions satisfy the relationship P3 with $\beta = 1$ rather than with $\beta = \mathrm{Lc}[b(x)]$). Just as in the case of the division property (Property P2) for univariate polynomials over a field, the polynomials $q(x)$, $r(x)$ in property P3 are *unique*. Algorithms for division and pseudo-division of polynomials will be discussed in a later chapter but for our purposes at the moment we may note that for given $a(x)$, $b(x) \in D[x]$, we may obtain the pseudo-quotient $q(x)$ and pseudo-remainder $r(x)$ of property P3 by performing ordinary polynomial long division of $\beta^l a(x)$ by $b(x)$. (In this process, all divisions will be exact in the coefficient domain D).

GCD Computation in $D[x]$

The pseudo-division property leads directly to an algorithm for computing GCD's in any polynomial domain $D[x]$ over a UFD D. As we have already noted, we may restrict our attention to primitive polynomials in $D[x]$.

Theorem 2.10.

Let $D[x]$ be a polynomial domain over a UFD D. Given primitive polynomials $a(x)$, $b(x) \in D[x]$ with $b(x) \neq 0$ and $\deg[a(x)] \geqslant \deg[b(x)]$, let $q(x)$, $r(x)$ be the pseudo-quotient and pseudo-remainder satisfying property P3. Then

(70) $\mathrm{GCD}(a(x), b(x)) = \mathrm{GCD}(b(x), \mathrm{pp}[r(x)])$.

Proof:

From property P3 we have

$$\beta^l a(x) = b(x)\, q(x) + r(x)$$

and applying to this equation the same argument as in the proof of Theorem 2.3 yields

(71) $\mathrm{GCD}(\beta^l a(x), b(x)) = \mathrm{GCD}(b(x), r(x))$.

Applying (67) to the left side of (71) yields

$$\begin{aligned}\mathrm{GCD}(\beta^l a(x), b(x)) &= \mathrm{GCD}(\beta^l, 1)\, \mathrm{GCD}(a(x), b(x)) \\ &= \mathrm{GCD}(a(x), b(x))\end{aligned}$$

where we have used the fact that $a(x)$, $b(x)$ are primitive polynomials. Similarly, applying (67) to the right side of (71) yields

$$\begin{aligned}\mathrm{GCD}(b(x), r(x)) &= \mathrm{GCD}(1, \mathrm{cont}[r(x)])\, \mathrm{GCD}(b(x), \mathrm{pp}[r(x)]) \\ &= \mathrm{GCD}(b(x), \mathrm{pp}[r(x)]).\end{aligned}$$

The result follows. □

It is obvious that for primitive polynomials $a(x)$, $b(x)$ we can define an iteration for GCD computation in $D[x]$ based on equation (70) and this iteration must terminate since $\deg[r(x)] < \deg[b(x)]$ at each step. This result is the basis of Algorithm 2.3. In Algorithm 2.3 the *polynomial remainder sequence* (PRS) which is generated is such that the remainder computed in each iteration is normalized to be primitive, so the algorithm is commonly referred to as the Primitive PRS Euclidean Algorithm. Algorithm 2.3 uses the prem function (in the sense of the extended definition given above) and it also assumes the existence of an algorithm for GCD computation in the coefficient domain D which would be used to compute contents, and hence primitive parts, and also to compute the quantity γ in that algorithm.

Algorithm 2.3. Primitive PRS Euclidean Algorithm.

```
begin
    comment Given polynomials a(x), b(x) ∈ D[x]
        where D is a UFD, compute g(x) = GCD(a(x), b(x));
    c(x) ← pp[a(x)]; d(x) ← pp[b(x)];
    while d(x) ≠ 0 do
        begin
            r(x) ← prem[c(x), d(x)];
            c(x) ← d(x);
            d(x) ← pp[r(x)]
        end;
    γ ← GCD(cont[a(x)], cont[b(x)]);
    g(x) ← γ c(x)
end.
```

Example 2.22.

In the UFD $\mathbf{Z}[x]$, let $a(x)$, $b(x)$ be the polynomials (39) - (40) considered variously in Examples 2.14 - 2.15 and Examples 2.19 - 2.21; namely

$$a(x) = 48x^3 - 84x^2 + 42x - 36;$$

$$b(x) = -4x^3 - 10x^2 + 44x - 30.$$

The sequence of values computed for $r(x)$, $c(x)$, and $d(x)$ in Algorithm 2.3 is as follows:

End of iteration no.	$r(x)$	$c(x)$	$d(x)$
0	–	$8x^3 - 14x^2 + 7x - 6$	$2x^3 + 5x^2 - 22x + 15$
1	$-68x^2 + 190x - 132$	$2x^3 + 5x^2 - 22x + 15$	$34x^2 - 95x + 66$
2	$4280x - 6420$	$34^2 - 95x + 66$	$2x - 3$
3	0	$2x - 3$	0

Then $\gamma = \text{GCD}(6,2) = 2$ and $g(x) = 2(2x - 3) = 4x - 6$ as noted in Example 2.19. □

Multivariate GCD Computation

The primary significance of Algorithm 2.3 is that it may be applied to compute GCD's in a *multivariate* polynomial domain $D[\mathbf{x}]$ over a UFD. Choosing x_1 as the main variable, we identify $D[x_1, \ldots, x_v]$ with the univariate polynomial domain $D[x_2, \ldots, x_v][x_1]$ over the UFD $D[x_2, \ldots, x_v]$. In order to apply Algorithm 2.3, we must be able to compute GCD's in the 'coefficient domain' $D[x_2, \ldots, x_v]$ – but this may be accomplished by recursively applying Algorithm 2.3, identifying $D[x_2, \ldots, x_v]$ with $D[x_3, \ldots, x_v][x_2]$, etc. Thus the recursive view of a multivariate polynomial domain leads naturally to a recursive algorithm for GCD computation.

Example 2.23.

In the UFD $\mathbf{Z}[x,y]$ let

$$a(x,y) = -30x^3y + 90x^2y^2 + 15x^2 - 60xy + 45y^2;$$

$$b(x,y) = 100x^2y - 140x^2 - 250xy^2 + 350xy - 150y^3 + 210y^2.$$

Choosing x as the main variable, we view $a(x,y)$ and $b(x,y)$ as elements in the domain $\mathbf{Z}[y][x]$:

$$a(x,y) = (-30y)x^3 + (90y^2 + 15)x^2 - (60y)x + (45y^2),$$

$$b(x,y) = (100y - 140)x^2 - (250y^2 - 350y)x - (150y^3 - 210y^2).$$

The first step in Algorithm 2.3 requires that we remove the unit part and the content from each polynomial; this requires a recursive application of Algorithm 2.3 to compute GCD's in the domain $\mathbf{Z}[y]$. We find:

$$u[a(x,y)] = -1; \quad u[b(x,y)] = 1;$$

$$cont[a(x,y)] = GCD(30y, -(90y^2 + 15), 60y, -45y^2) = 15;$$

$$cont[b(x,y)] = GCD(100y - 140, -(250y^2 - 350y), -(150y^3 - 210y^2))$$

$$= 50y - 70.$$

Thus,

$$pp[a((x,y)] = (2y)x^3 - (6y^2 + 1)x^2 + (4y)x - (3y^2);$$

$$pp[b(x,y)] = (2)x^2 - (5y)x - (3y^2).$$

The sequence of values computed for $r(x)$, $c(x)$, and $d(x)$ in Algorithm 2.3 is then as follows:

End of iteration no.	$r(x)$	$c(x)$	$d(x)$
0	–	$(2y)x^3 - (6y^2+1)x^2 + (4y)x - (3y^2)$	$(2)x^2 - (5y)x - (3y^2)$
1	$(2y^3+6y)x - (6y^4+18y^2)$	$(2)x^2 - (5y)x - (3y^2)$	$x - (3y)$
2	0	$x - (3y)$	0

Thus,

$$\gamma = GCD(15, 50y - 70) = 5$$

and

$$g(x) = 5(x - (3y)) = 5x - (15y);$$

i.e.

$$GCD(a(x,y), b(x,y)) = 5x - 15y. \quad \square$$

The Euclidean Algorithm Revisited

Algorithm 2.3 is a generalization of Algorithm 2.1 and we may apply Algorithm 2.3 to compute GCD's in a Euclidean domain $F[x]$ over a field F. In this regard, note that the GCD of any two elements (not both zero) in a field F is 1 since every nonzero element in a field is a unit. In particular, $cont[a(x)] = 1$ for all nonzero $a(x) \in F[x]$ and hence

$$pp[a(x)] = n[a(x)] \text{ for all } a(x) \in F[x].$$

Functionally, the operations $pp[\cdot]$ and $n[\cdot]$ when applied in a Euclidean domain $F[x]$ both specify that their argument is to be made monic. The prem function can be seen to be identical with the standard rem function when applied to *primitive* polynomials in $F[x]$ since $\beta = 1$ in property P3 when $b(x)$ is monic.

A comparison of Algorithm 2.3 with Algorithm 2.1 thus shows that when applied in a polynomial domain F[x] over a field F, both algorithms perform the same computation except that in Algorithm 2.3 the remainder is normalized (i.e. made monic) in each iteration. This additional normalization within each iteration serves to simplify the computation somewhat and may be considered a useful improvement to Algorithm 2.1.

Example 2.24.

In the Euclidean domain **Q**[x], let a(x), b(x) be the polynomials (39) - (40) of Example 2.14. The sequence of values computed for r(x), c(x), and d(x) in Algorithm 2.3 is as follows:

End of iteration no.	r(x)	c(x)	d(x)
0	–	$x^3 - \frac{7}{4}x^2 + \frac{7}{8}x - \frac{3}{4}$	$x^3 + \frac{5}{2}x^2 - 11x + \frac{15}{2}$
1	$-\frac{17}{4}x^2 + \frac{95}{8}x - \frac{33}{4}$	$x^3 + \frac{5}{2}x^2 - 11x + \frac{15}{2}$	$x^2 - \frac{95}{34}x + \frac{33}{17}$
2	$\frac{535}{289}x - \frac{1605}{578}$	$x^2 - \frac{95}{34}x + \frac{33}{17}$	$x - \frac{3}{2}$
3	0	$x - \frac{3}{2}$	0

Then $\gamma = 1$ and $g(x) = x - \frac{3}{2}$ as computed by Algorithm 2.1 in Example 2.14. □

2.7. QUOTIENT FIELDS AND RATIONAL FUNCTIONS

An important property of an integral domain is that it can be extended to a field in a very simple manner. One reason for wanting a field is, for example, to be able to solve linear equations – a process which requires division. The most familiar example of extending an integral domain to a field is the process of constructing the field **Q** of rationals from the integral domain **Z** of integers. This particular construction extends immediately to any integral domain.

Quotient Fields

Let D be an integral domain and consider the set of quotients

$$S = \{a/b : a \in D, b \in D - \{0\}\}.$$

Keeping in mind the usual properties of field arithmetic, we define the following relation on S:

(72) $a/b \sim c/d$ if and only if $ad = bc$.

It is readily verified that the relation $\sim$ is an equivalence relation on S and it therefore divides S into equivalence classes $[a/b]$. The set of equivalence classes is called a *quotient set,* denoted by

$$S/\sim = \{[a/b]: a \in D, b \in D - \{0\}\}$$

(read 'S modulo the equivalence relation $\sim$'). In dealing with the quotient set $S/\sim$, any member of an equivalence class may serve as its *representative.* Thus when we write a/b we really mean the equivalence class $[a/b]$ containing the particular quotient a/b. The operations of addition and multiplication in the integral domain D are extended to the quotient set $S/\sim$ as follows: if a/b and c/d are in $S/\sim$ (in the above sense) then

(73) $(a/b) + (c/d) = (ad + bc)/bd$;

(74) $(a/b)(c/d) = ac/bd$.

(It is straightforward to show that the operations of addition and multiplication on equivalence

classes in $S/\sim$ are well-defined by (73) - (74) in the sense that the sum or product of equivalence classes is independent of the particular representatives used for the equivalence classes). The quotient set $S/\sim$ with the operations of addition and multiplication defined by (73) - (74) is a field, called the *quotient field* (or *field of quotients*) of the integral domain D and denoted variously by Q(D) or F_D.

The quotient field Q(D) contains (an isomorphic copy of) the integral domain D. Specifically, the integral domain D is identified with the subset of Q(D) defined by

$$\{a/1 : a \in D\}$$

using the natural relationship $a \leftrightarrow a/1$. Indeed the quotient field Q(D) is the *smallest* field which contains the integral domain D. The zero in the field Q(D) is the quotient 0/1 and the multiplicative identity is 1/1. By convention, a quotient $a/1 \in Q(D)$ with denominator 1 is denoted by a; in particular, the zero and identity are denoted by 0 and 1.

When dealing with an algebraic system whose constituent elements are equivalence classes, it is fine in principle to note that any member of an equivalence class may serve as its representative but in practice we need a *canonical form* for the equivalence classes so that the representation is unique. Otherwise, a problem such as determining when two expressions are equal becomes very nontrivial. If GCD's exist in the integral domain D and if a canonical form (i.e. unique representation) for elements of D has been determined, then a common means of defining a canonical form for elements in the quotient field Q(D) is as follows: the representative a/b of $[a/b] \in Q(D)$ is canonical if

(75) $GCD(a,b) = 1$;

(76) b is unit normal in D;

(77) a and b are canonical in D.

Any representative c/d may be put in the canonical form satisfying (75) - (77) by a straightforward computational procedure: compute $GCD(c,d)$ and divide it out of numerator and denominator, multiply numerator and denominator by the inverse of the unit $u(d)$, and put the resulting numerator and denominator into their canonical forms as elements of D. It can be verified (see Exercise 2-14) that for each equivalence class in Q(D) there is one and only one representative satisfying (75) - (77).

Example 2.25.

If D is the domain **Z** of integers then the quotient field Q(**Z**) is the field of rational numbers, denoted by **Q**. A rational number (representative) a/b is canonical if a and b have no common factors and b is positive. The following rational numbers all belong to the same equivalence class:

$$-2/4,\ 2/-4,\ 100/-200,\ -600/1200;$$

their canonical representative is $-1/2$. □

Rational Functions

For a polynomial domain D[**x**] over a UFD D, the quotient field Q(D[**x**]) is called the field of *rational functions* (or *rational forms*) over D in the indeterminates **x**, and is denoted by D(**x**). Elements of D(**x**) are (equivalence classes of) quotients of the form.

$$a(\mathbf{x}) / b(\mathbf{x}) \quad \text{where } a(\mathbf{x}),\ b(\mathbf{x}) \in D[\mathbf{x}] \text{ with } b(\mathbf{x}) \neq 0.$$

The canonical form of a rational function (representative) $a(\mathbf{x}) / b(\mathbf{x}) \in D(\mathbf{x})$ depends on the canonical form chosen for multivariate polynomials in D[**x**] (canonical forms for multivariate polynomials are discussed in chapter 3) but the definition of canonical forms for rational functions will always include conditions (75) - (76) – namely, $a(\mathbf{x})$ and $b(\mathbf{x})$ have no common factors and the leading coefficient of $b(\mathbf{x})$ is unit normal in the coefficient domain D.

The operation of addition in a quotient field is a relatively complex operation. From (73) we see that to add two quotients requires three multiplications and one addition in the underlying integral domain. Additionally, a GCD computation will be required to obtain the canonical form of the sum. It is the latter operation which is the most expensive and its cost is a dominating factor in all of symbolic computation. For the field $D(x)$ of rational functions, we try to minimize the cost of GCD computation by intelligently choosing the representation for rational functions (see chapter 3) and by using an efficient GCD algorithm (see chapter 7). On the other hand, the operation of multiplication in a quotient field is less expensive than addition. From (74) we see that to multiply two quotients requires only two multiplications in the underlying integral domain, but more significantly, with an appropriate choice of representation it is possible to greatly reduce the amount of GCD computation required in performing the operation (74) compared with the operation (73). Algorithms for performing arithmetic on rational functions will be considered in chapter 4.

Two polynomial domains of interest in symbolic computation are domains $\mathbf{Z}[x]$ and $\mathbf{Q}[x]$. Let us consider for a moment the corresponding fields of rational functions $\mathbf{Z}(x)$ and $\mathbf{Q}(x)$. In the univariate case, a typical example of a rational function (representative) in $\mathbf{Q}(x)$ is

$$\textbf{(78)} \quad a(x)/b(x) = \left(\frac{17}{100}x^2 - \frac{3}{112}x + \frac{1}{2}\right)/\left(\frac{5}{9}x^2 + \frac{4}{5}\right).$$

But note that the equivalence class $[a(x)/b(x)]$ also contains representatives with integer coefficients. The simplest such representative is obtained by multiplying numerator and denominator in (78) by the least common multiple (LCM) of all coefficient denominators; in this case:[4]

$$\text{LCM}(100, 112, 2, 9, 5) = 25200.$$

Thus another representative for the rational function (78) in $\mathbf{Q}(x)$ is

$$\textbf{(79)} \quad a(x)/b(x) = (4284x^2 - 675x + 12600)/(14000x^2 + 20160)$$

which is also a rational function (representative) in the domain $\mathbf{Z}(x)$. The argument just posed leads to a very general result which we will not prove more formally here; namely, if D is any integral domain and if F_D denotes the quotient field of D, then the fields of rational functions $D(x)$ and $F_D(x)$ are isomorphic. More specifically, there is a natural one-to-one correspondence between the equivalence classes in $D(x)$ and the equivalence classes in $F_D(x)$. The only difference between the two fields is that each equivalence class has many more representatives in $F_D(x)$ than in $D(x)$.

Example 2.26.

In the field $\mathbf{Q}(x)$, a canonical form for the rational function (78) satisfying conditions (75) - (76) is obtained by making the denominator unit normal (i.e. monic):

$$a(x)/b(x) = \left(\frac{153}{500}x^2 - \frac{27}{560}x + \frac{9}{10}\right)/\left(x^2 + \frac{36}{25}\right)$$

(since there are already no common factors). In the field $\mathbf{Z}(x)$, the same rational function has (79) as a canonical form since the denominator in (79) is unit normal in $\mathbf{Z}[x]$ and there are no common factors (including integer common factors). □

4. The LCM of n elements $a_1, \ldots, a_n$ in an integral domain D is defined recursively for $n > 2$ by:

$$\text{LCM}(a_1, \ldots, a_{n-1}, a_n) = \text{LCM}(\text{LCM}(a_1, \ldots, a_{n-1}), a_n).$$

2.8. POWER SERIES AND EXTENDED POWER SERIES

Ordinary Power Series

The definition of univariate polynomials can be readily extended to a definition of (univariate) power series. For any commutative ring R, the notation R[[x]] denotes the set of all expressions of the form

$$\textbf{(80)} \quad a(x) = \sum_{k=0}^{\infty} a_k x^k$$

with $a_k \in R$. In other words, R[[x]] denotes the set of all *power series* in the indeterminate x over the ring R. The *order* ord[a(x)] of a non-zero power series a(x) as in (80) is the least integer k such that $a_k \neq 0$. The exceptional case where $a_k = 0$ for all k is called the *zero power series* and is denoted by 0. It is conventional to define ord[0] = ∞. For a nonzero power series a(x) as in (80) with ord[a(x)] = l, the term $a_l x^l$ is called the *low order term* of a(x), a_l is called the *low order coefficient*, and a_0 is called the *constant term*. A power series in which $a_k = 0$ for all $k \geqslant 1$ is called a *constant power series*.

The binary operations of addition and multiplication in the commutative ring R are extended to power series in the set R[[x]] as follows. If

$$a(x) = \sum_{k=0}^{\infty} a_k x^k \quad \text{and} \quad b(x) = \sum_{k=0}^{\infty} b_k x^k$$

then power series addition is defined by

$$\textbf{(81)} \quad c(x) = a(x) + b(x) = \sum_{k=0}^{\infty} c_k x^k$$

where

$$c_k = a_k + b_k \quad \text{for all } k \geqslant 0;$$

and power series multiplication is defined by

$$\textbf{(82)} \quad d(x) = a(x)\, b(x) = \sum_{k=0}^{\infty} d_k x^k$$

where

$$d_k = \sum_{i=0}^{k} a_i b_{k-i} \quad \text{for all } k \geqslant 0.$$

Note that the set R[x] of univariate polynomials over R is the subset of R[[x]] consisting of all power series with only a finite number of nonzero terms. Definitions (81) - (82) reduce to the definitions of polynomial addition and multiplication when a(x) and b(x) have only a finite number of nonzero terms. Just as in the case of polynomials, the set R[[x]] of power series inherits a ring structure from its coefficient ring R under the operations (81) - (82). The following theorem states the basic results.

Theorem 2.11.

(i) If R is a commutative ring then R[[x]] is also a commutative ring. The zero in R[[x]] is the zero power series 0 ($= 0 + 0x + 0x^2 + \cdots$) and the identity in R[[x]] is the constant power series 1 ($= 1 + 0x + 0x^2 + \cdots$).

(ii) If D is an integral domain then D[[x]] is also an integral domain. The units (invertibles) in D[[x]] are all power series whose constant term a_0 is a unit in the coefficient domain D.

(iii) If F is a field then F[[x]] is a Euclidean domain with the valuation

(83) $v[a(x)] = \text{ord}[a(x)]$. □

It is instructive to note the following constructive proof of the second statement in part (ii) of Theorem 2.11. If $a(x) = \sum_{k=0}^{\infty} a_k x^k$ is a unit in D[[x]] then there must exist a power series $b(x) = \sum_{k=0}^{\infty} b_k x^k$ such that $a(x)\, b(x) = 1$. By the definitions of power series multiplication, we must have

$$a_0 b_0 = 1$$

$$a_0 b_1 + a_1 b_0 = 0$$

$$\vdots$$

$$a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0$$

$$\vdots$$

Thus, a_0 is a unit in D with $a_0^{-1} = b_0$. Conversely, if a_0 is a unit in D then the above equations can be solved for the b_k's as follows:

$$b_0 = a_0^{-1}$$

$$b_1 = -a_0^{-1}\ [a_1 b_0]$$

$$\vdots$$

$$b_n = -a_0^{-1}\ [a_1 b_{n-1} + \cdots + a_n b_0]$$

$$\vdots$$

Thus we can construct $b(x)$ such that $a(x)\, b(x) = 1$, which implies that $a(x)$ is a unit in D[[x]].

Example 2.27.

In the polynomial domain **Z**[x] the only units are 1 and -1. In the power series domain **Z**[[x]], any power series with constant term 1 or -1 is a unit in **Z**[[x]]. For example, the power series $1 - x$ is a unit in **Z**[[x]] with

$$(1 - x)^{-1} = 1 + x + x^2 + x^3 + \cdots .$$ □

Example 2.28.

In any power series domain F[[x]] over a field F, every power series of order 0 is a unit in F[[x]]. For if $a(x) \in$ F[[x]] is of order 0 then its constant term $a_0 \neq 0$ is a unit in the coefficient field F. □

The order function defined on power series has properties similar to the degree functions defined on polynomials. It can be readily verified that the following properties hold for power series in a domain D[[x]] over any integral domain D:

(84) $\text{ord}[a(x) + b(x)] \geqslant \min\{\text{ord}[a(x)], \text{ord}[b(x)]\}$;

(85) $\text{ord}[a(x)\, b(x)] = \text{ord}[a(x)] + \text{ord}[b(x)]$.

Using (85) we can verify that in a power series domain F[[x]] over a field F, (83) is a valid valuation according to Definition 2.14. Since by definition ord[a(x)] $\geqslant$ 0 for any nonzero power series a(x), the valuation (83) is indeed a mapping from F[[x]]$-\{0\}$ into the nonnegative integers **N** as required by Definition 2.14. Property P1 can be verified by using (85) since if a(x), b(x) $\in$ F[[x]]$-\{0\}$ then

$$\text{ord}[a(x)\,b(x)] = \text{ord}[a(x)] + \text{ord}[b(x)] \geqslant \text{ord}[a(x)].$$

In order to verify property P2 first note that for nonzero a(x), b(x) $\in$ F[[x]] either a(x) | b(x) or b(x) | a(x). To see this let ord[a(x)] = l and ord[b(x)] = m so that

$$a(x) = x^l \tilde{a}(x) \quad \text{and} \quad b(x) = x^m \tilde{b}(x)$$

where $\tilde{a}(x)$ and $\tilde{b}(x)$ are units in F[[x]]. Then if $l \geqslant m$ we have

$$a(x) / b(x) = x^{l-m} \tilde{a}(x) [\tilde{b}(x)]^{-1} \in F[[x]]$$

and similarly if $l < m$ then

$$b(x) / a(x) = x^{m-l} \tilde{b}(x) [\tilde{a}(x)]^{-1} \in F[[x]].$$

Therefore given a(x), b(x) $\in$ F[[x]] with b(x) $\neq$ 0 we have

$$a(x) = b(x)\,q(x) + r(x)$$

where if ord[a(x)] $\geqslant$ ord[b(x)] then q(x) = a(x) / b(x), r(x) = 0 while if ord[a(x)] < ord[b(x)] then q(x) = 0, r(x) = a(x). This verifies property P2 proving that F[[x]] is a Euclidean domain if F is a field.

The Quotient Field D((**x**))

For a power series domain D[[x]] over an integral domain D, the quotient field Q(D[[x]]) is called the field of *power series rational functions* over D and is denoted by D((x)). Elements of D((x)) are (equivalence classes of) quotients of the form

$$a(x) / b(x) \quad \text{where a}(x),\ b(x) \in D[[x]] \text{ with } b(x) \neq 0.$$

Unlike ordinary (polynomial) rational functions, power series rational functions cannot in general be put into a canonical form by removing 'common factors' since the power series domain D[[x]] is not a unique factorization domain. Indeed it is not even clear how to define 'unit normal' elements in the integral domain D[[x]]. Recall that in any integral domain the relation of associativity is an equivalence relation and the idea of 'unit normal' elements is to single out one element from each associate class as its canonical representative. In D[[x]], two power series are in the same associate class if one can be obtained from the other by multiplying it by a power series whose constant term is a unit in D.

Example 2.29.

In the power series domain **Z**[[x]], the following power series all belong to the same associate class:

$$a(x) = 2 + 2x + 2x^2 + 3x^3 + 4x^4 + \cdots ;$$

$$b(x) = 2 + 4x + 6x^2 + 9x^3 + 13x^4 + \cdots ;$$

$$c(x) = 2 + x^3 + x^4 + x^5 + x^6 + \cdots .$$

This can be seen by noting that

$$b(x) = a(x)\,(1 + x + x^2 + x^3 + x^4 + \cdots)$$

and

$$c(x) = a(x)\,(1 - x).$$

It is not clear how to single out one of $a(x)$, $b(x)$, $c(x)$, or some other associate of these, as the unit normal element. □

The Quotient Field F((x))

The case of a power series domain F[[x]] over a field F and its corresponding quotient field F((x)) can be dealt with in a manner just like polynomials and ordinary (polynomial) rational functions. For if $a(x) \in F((x))$ is a nonzero power series then $a(x)$ can be expressed in the form

$$a(x) = x^l b(x)$$

where $l = \text{ord}[a(x)]$ and

$$b(x) = a_l + a_{l+1}x + a_{l+2}x^2 + \cdots .$$

Then $a_l \neq 0$ and hence $b(x)$ is a unit power series in F[[x]]. This leads us to the following definition.

Definition 2.21.

In any power series domain F[[x]] over a field F, the monomials x^l ($l \geqslant 0$) and the zero power series 0 are defined to be *unit normal.* □

From the above definition we have the following 'functional specifications' for the normal part $n(a(x))$ and the unit part $u(a(x))$ of a nonzero power series $a(x) \in F[[x]]$:

(86) $n(a(x)) = x^{\text{ord}[a(x)]}$;

(87) $u(a(x)) = a(x) / x^{\text{ord}[a(x)]}$.

(Note that the monomial x^0 is identified with the constant power series 1 and therefore the unit normal element for the associate class of units is 1 as usual). With this definition of unit normal elements it becomes straightforward to define the GCD of any two power series $a(x)$, $b(x) \in F[[x]]$ (not both zero); namely,

(88) $\text{GCD}(a(x), b(x)) = x^{\min\{\text{ord}[a(x)],\ \text{ord}[b(x)]\}}$.

To see that (88) is valid, recall that we may restrict our attention to the *unit normal GCD* which must be a monomial x^l and clearly the 'greatest' monomial which divides both $a(x)$ and $b(x)$ is that given by formula (88).

Canonical forms for elements of the quotient field F((x)) can now be defined to satisfy conditions (75) - (77) just as in the case of ordinary (polynomial) rational functions. Namely, if a representation for power series in the domain F[[x]] has been chosen then the canonical form of a power series rational function (representative) $a(x) / b(x) \in F((x))$ is obtained by dividing out $\text{GCD}(a(x), b(x))$ and then making the denominator unit normal. It follows that the canonical form of a power series rational function over a field F is always of the form

(89) $\tilde{a}(x) / x^n$

where $\tilde{a}(x) \in F[[x]]$ and $n \geqslant 0$; moreover if $n > 0$ then $\text{ord}[\tilde{a}(x)] = 0$. Clearly the representation of canonical quotient (89) is only trivially more complicated than the representation of a power series in the domain F[[x]], and similarly the arithmetic operations on canonical quotients of the form (89) are only slightly more complicated then the operations in the domain F[[x]].

Since the power series rational functions in a field F((x)) over any field F have the simple canonical representation (89) while the elements in a field D((x)) over a general integral domain D have a much more complicated representation, we will always embed the field D((x)) into the larger field $F_D((x))$ for computational purposes (where F_D denotes the quotient field of the coefficient domain D). Thus we will never need to represent quotients $a(x) / b(x)$ where $a(x)$ and $b(x)$ are both power series. We have noted earlier that for ordinary (polynomial) rational functions the fields $D(x)$ and $F_D(x)$ are isomorphic. The following example indicates that for

power series rational functions, the field $D((x))$ is a proper subset of (i.e. not isomorphic to) the field $F_D((x))$ when D is not a field.

Example 2.30.

In the domain $\mathbf{Q}((x))$ of power series rational functions over the field **Q**, let

$$a(x)/b(x) = (1 + x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \cdots)/(1 - x).$$

The power series rational function $a(x)/b(x)$ has no representation with integer coefficients because the denominators of the coefficients in the numerator power series grow without bound. Thus the equivalence class $[a(x)/b(x)] \in \mathbf{Q}((x))$ has no corresponding equivalence class in the field $\mathbf{Z}((x))$. Note that the reduced form of $a(x)/b(x)$ in the field $\mathbf{Q}((x))$ is a power series since $(1-x)$ is a unit in $\mathbf{Q}((x))$; specifically, the reduced form is

$$a(x)/b(x) = 1 + 2x + \frac{5}{2}x^2 + \frac{17}{6}x^3 + \frac{37}{12}x^4 + \cdots . \quad \square$$

Extended Power Series

We have seen that to represent the elements of a field $F((x))$ of power series rational functions over a field F, we need only to represent expressions of the form

$$\textbf{(90)} \quad (\sum_{k=0}^{\infty} a_k x^k)/x^n$$

where n is a nonnegative integer. One way to represent such expressions is in the form of 'extended power series' which we now define.

For any field F, the set $F\langle x\rangle$ of *extended power series* over F is defined to be the set of all expressions of the form

$$\textbf{(91)} \quad a(x) = \sum_{k=m}^{\infty} a_k x^k$$

with $a_k \in F$ $(k \geqslant m)$, where $m \in Z$ (i.e. m is any finite integer, positive, negative or zero). As in the case of ordinary power series, we define the *order* $\mathrm{ord}[a(x)]$ of a nonzero extended power series $a(x)$ as in (91) to be the least integer k such that $a_k \neq 0$. Thus $\mathrm{ord}[a(x)] < 0$ for many extended power series $a(x) \in F\langle x\rangle$ but clearly the set $F\langle x\rangle$ also contains the set $F[[x]]$ of ordinary power series satisfying $\mathrm{ord}[a(x)] \geqslant 0$. As with ordinary power series, the *zero extended power series* is denoted by 0, $\mathrm{ord}[0] = \infty$ by definition, and if $a(x)$ is a nonzero extended power series as in (91) with $\mathrm{ord}[a(x)] = m$ then $a_m x^m$ is the *low order term*, a_m is the *low order coefficient*, and a_0 is the *constant term*. An extended power series in which $a_k = 0$ for all $k \geqslant 1$ and for all $k < 0$ is called a *constant extended power series*.

Addition and multiplication of extended power series are defined exactly as for ordinary power series as follows. If

$$a(x) = \sum_{k=m}^{\infty} a_k x^k \text{ and } b(x) = \sum_{k=n}^{\infty} b_k x^k$$

then addition is defined by

$$\textbf{(92)} \quad c(x) = a(x) + b(x) = \sum_{k=\min\{m,n\}}^{\infty} c_k x^k$$

where

$$c_k = \begin{cases} a_k + b_k & \text{for } k \geqslant \max\{m,n\} \\ a_k & \text{for } m \leqslant k < n \text{ if } m < n \\ b_k & \text{for } n \leqslant k < m \text{ if } m > n \end{cases}.$$

Similarly, multiplication is defined by

$$(93) \quad d(x) = a(x)\, b(x) = \sum_{k=m+n}^{\infty} d_k x^k$$

where

$$d_k = \sum_{i+j=k} a_i b_j.$$

It is easy to verify that the order function defined on extended power series satisfies properties (84) - (85) for the order of a sum and product, just as for ordinary power series. Under the operations (92) - (93), $F\langle x \rangle$ is a field with zero element the zero extended power series 0 and with identity the constant extended power series 1.

Let us consider a constructive proof that every nonzero extended power series $a(x) \in F\langle x \rangle$ has an inverse in $F\langle x \rangle$. Firstly, if $\mathrm{ord}[a(x)] = 0$ then $a(x)$ is a unit in the power series domain $F[[x]]$ and the inverse power series $[a(x)]^{-1} \in F[[x]]$ may be considered an element of $F\langle x \rangle$. Then $[a(x)]^{-1}$ is the desired inverse in $F\langle x \rangle$ because power series multiplication is defined the same in $F\langle x \rangle$ as in $F[[x]]$. More generally, if $\mathrm{ord}[a(x)] = m$ (which may be positive, negative, or zero) then $a(x) = x^m\, b(x)$ where $\mathrm{ord}[b(x)] = 0$. Then it is easily verified that the inverse of $a(x)$ in $F\langle x \rangle$ is given by

$$[a(x)]^{-1} = x^{-m}\, [b(x)]^{-1}.$$

Note in particular that

$$\mathrm{ord}[[a(x)]^{-1}] = -\mathrm{ord}[a(x)].$$

Example 2.31.

In the field $Q\langle x \rangle$ let

$$a(x) = x^2 + \frac{1}{2}x^3 + \frac{1}{4}x^4 + \frac{1}{8}x^5 + \frac{1}{16}x^6 + \cdots .$$

The inverse of $a(x)$ can be determined by noting that

$$a(x) = x^2 \left(1 + \frac{1}{2}x + \frac{1}{4}x^2 + \frac{1}{8}x^3 + \frac{1}{16}x^4 + \cdots\right)$$

and

$$\left(1 + \frac{1}{2}x + \frac{1}{4}x^2 + \frac{1}{8}x^3 + \frac{1}{16}x^4 + \cdots\right)^{-1} = 1 - \frac{1}{2}x.$$

Thus,

$$[a(x)]^{-1} = x^{-2}\left(1 - \frac{1}{2}x\right) = x^{-2} - \frac{1}{2}x^{-1}. \qquad \square$$

As we have already implied, a power series rational function in the canonical form (90) may be represented as an extended power series. Specifically, we may identify the quotient (90) in the field $F((x))$ with the extended power series $a(x) \in F\langle x \rangle$ defined by

$$(94) \quad a(x) = \sum_{k=-n}^{\infty} a_{k+n} x^k.$$

Formally, it can be proved that the mapping between the fields $F((x))$ and $F\langle x \rangle$ defined by identifying (90) with (94) is an isomorphism. Thus $F\langle x \rangle$ is not a new algebraic system but rather it is simply a convenient representation for the quotient field $F((x))$.

2.9. RELATIONSHIPS AMONG DOMAINS

As we come to the close of this chapter it is appropriate to consider the relationships which exist among the various extensions of polynomial domains which have been introduced.

Given an arbitrary integral domain D, we have introduced univariate domains of polynomials, rational functions, power series, and power series rational functions, denoted respectively by $D[x]$, $D(x)$, $D[[x]]$, and $D((x))$. Several relationships among these four domains are obvious; for example,

$$D[x] \subset D(x) \subset D((x)), \text{ and}$$

$$D[x] \subset D[[x]] \subset D((x)).$$

The notation $S \subset R$ used here denotes not only that S is a *subset* of R but moreover that S is a *subring*[5] of the ring R. The diagram in Figure 2.1 summarizes these simple relationships. The only pair for which the relationship is unclear is the 'diagonal' pair $D(x)$ and $D[[x]]$. The relationship between rational functions and power series will be considered shortly.

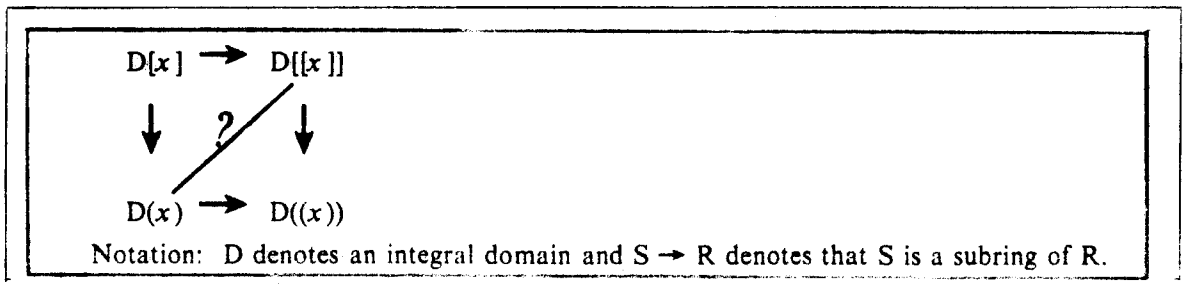


Figure 2.1. Relationships among four domains over an integral domain D.

If F_D denotes the quotient field of the integral domain D we may consider, along with the four domains of Figure 2.1 the corresponding domains $F_D[x]$, $F_D(x)$, $F_D[[x]]$, and $F_D((x))$; we also have the field $F_D\langle x \rangle$ of extended power series. These domains satisfy a diagram like that in Figure 2.1. The diagram in Figure 2.2 shows the relationships among the latter domains and also shows their relationships with the domains of Figure 2.1. Along with the unspecified relationship noted in Figure 2.1, there are three additional unspecified relationships in Figure 2.2:

(i) $F_D[x] \stackrel{?}{\_\_} D[[x]]$;

(ii) $D((x)) \stackrel{?}{\_\_} F_D[[x]]$;

(iii) $D(x) \stackrel{?}{\_\_} F_D[[x]]$.

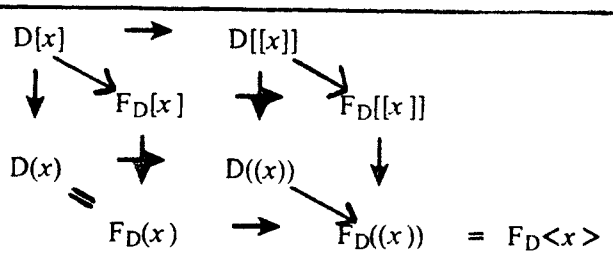
In order to determine the relationship between a pair of domains A and B, we may consider a larger domain C which contains both of them and pose the question: In the domain C, what is the intersection of the subset A with the subset B? Thus for (i) - (iii) above we may pose the question in the domain $F_D((x))$. Relationship (i) is trivial and uninteresting; namely,

$$\{F_D[x] \cap D[[x]]\} = D[x].$$

Relationship (ii) is a little more complicated; for example,

$$D[[x]] \subset \{D((x)) \cap F_D[[x]]\}$$

5. If [R; +, ×] is a ring then a subset S of R is a *subring* (more formally, [S; +, ×] is a subring) if S is closed under the ring operations defined on R. (See chapter 5).



Notation: D denotes an integral domain, F_D its quotient field, S → R denotes that S is a subring of R, and S = R denotes that S and R are isomorphic.

Figure 2.2. Relationships among nine domains.

and

$$F_D[x] \subset \{D((x)) \cap F_D[[x]]\}$$

but the intersection contains more than just $D[[x]] \cup F_D[x]$. Since the domain $D((x))$ is avoided for computational purposes (by embedding it in $F_D((x))$), relationship (ii) is not of practical interest and will not be pursued further. (See Exercise 2-18).

Relationship (iii) leads to an interesting pair of questions. In one direction, we are asking under what conditions a rational function $a(x)/b(x) \in D(x)$ can be expressed as a power series $c(x) \in F_D[[x]]$. By putting $a(x)/b(x)$ into the canonical form (90) as an element in $F_D((x))$, we see that $a(x)/b(x)$ is a power series in $F_D[[x]]$ if and only if $\text{ord}[b(x)] \leqslant \text{ord}[a(x)]$ – i.e. if and only if the rational function $a(x)/b(x) \in D(x)$ has a canonical representative with denominator of order 0. In the other direction, we are asking under what conditions a power series $c(x) \in F_D[[x]]$ can be expressed as a rational function $a(x)/b(x) \in D(x)$. This question is of considerable practical interest because it is asking when an infinite expression (a power series) can be represented by a finite expression (a rational function). By examining the formula for the coefficients in the power series expansion of a rational function, we obtain the following answer. A power series $c(x) = \sum_{k=0}^{\infty} c_k x^k \in F_D[[x]]$ is equal in $F_D((x))$ to a rational function $a(x)/b(x) \in D(x)$ if and only if the c_k's ultimately satisfy a finite linear recurrence; specifically, there must exist nonnegative integers l,n and constants $d_1, d_2, \ldots, d_n \in F_D$ such that

$$\textbf{(95)} \quad c_k = d_1 c_{k-1} + d_2 c_{k-2} + \cdots + d_n c_{k-n} \text{ for all } k > l.$$

More specifically, if the power series $c(x)$ satisfies (95) then in $F_D((x))$,

$$c(x) = a(x)/(1 - d_1 x - d_2 x^2 - \cdots - d_n x^n)$$

where $\deg[a(x)] \leqslant l$. (Of course, the rational function can be normalized so that its coefficients lie in D since $D(x) = F_D(x)$).

Let us finally return to the relationship marked by a question mark in Figure 2.1, namely, the relationship between $D(x)$ and $D[[x]]$. In view of the relationship between $D(x)$ and $F_D[[x]]$ stated above, the following statements are easily verified. A rational function $a(x)/b(x) \in D(x)$ can be expressed as a power series $c(x) \in D[[x]]$ if and only if the rational function has a canonical representative in which the constant term of the denominator is a unit in D. A power series $c(x) = \sum_{k=0}^{\infty} c_k x^k \in D[[x]]$ can be expressed as a rational function $a(x)/b(x) \in D(x)$ if and only if the c_k's ultimately satisfy a finite linear recurrence of the form

$$\textbf{(96)} \quad d_0 c_k + d_1 c_{k-1} + \cdots + d_n c_{k-n} = 0 \text{ for all } k > l,$$

for some nonnegative integers l,n and some constants $d_0, d_1, \ldots, d_n \in D$. Note that the recurrence (96) expressed over D is equivalent to the recurrence (95) expressed over F_D.

BIBLIOGRAPHY FOR CHAPTER 2

G. Birkhoff and T.C. Bartee, *Modern Applied Algebra*. McGraw-Hill, New York, 1970.

G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 3rd ed. Macmillian, New York, 1965.

W.S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors. *J. Assoc. Comput. Mach.* 18(4), October 1971, pp. 478-504.

D. Knuth, *The Art of Computer Programming, vol. 2: Seminumerical Algorithms*. Addison-Wesley, Reading, Mass., 1969.

J.D. Lipson, *Elements of Algebra and Algebraic Computing*. To be published, 1981.

B.L. van der Waerden, *Algebra*, vol. 1 and vol. 2, trans. by J.R. Schulenberger. Ungar, New York, 1970.

EXERCISES

2-1. Let M denote the set of all 2×2 matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with entries $a,b,c,d \in \mathbf{R}$. Verify that the algebraic system [M, +, .], where + and . denote the standard operations of matrix addition and matrix multiplication, is a ring. Give a counter-example to show that [M, +, .] is not a commutative ring.

2-2. Prove that in any commutative ring, axiom **A6** (Cancellation Law) implies and is implied by axiom **A6′** (No Zero Divisors).

2-3. Form addition and multiplication tables for the commutative ring $\mathbf{Z}_6$. Show that $\mathbf{Z}_6$ is not an integral domain by displaying counter-examples for axioms **A6** and **A6′**. Show that $\mathbf{Z}_6$ is not a field by explicitly displaying a counter-example for one of the field axioms.

2-4. Make a table of inverses for the field $\mathbf{Z}_{37}$. *Hint:* Determine the inverses of 2 and 3, and then use the following law which holds in any field:

$$(xy)^{-1} = x^{-1}y^{-1}.$$

2-5. Prove that in any integral domain D, elements $c,d \in D$ are associates if and only if $cu = d$ for some unit u.

2-6. Prove that in any integral domain D, if $p \in D$ is a prime then so is any associate of p.

2-7. The set G of *Gaussian integers* is the subset of the complex numbers **C** defined by

$$G = \{a + b\sqrt{-1} : a,b \in \mathbf{Z}\}$$

(where we usually use the notation $\sqrt{-1} = i$). Verify that G, with the standard operations of addition and multiplication of complex numbers, is an integral domain. Further, verify that G is a Euclidean domain with the valuation

$$v(a + b\sqrt{-1}) = a^2 + b^2.$$

2-8. Let S be the subset of the complex numbers **C** defined by

$$S = \{a + b\sqrt{-5} : a,b \in \mathbf{Z}\}$$

(where we may take $\sqrt{-5} = \sqrt{5}i$). Verify that S, with the usual operations, is an integral domain. Prove that the only units in S are 1 and -1.

2-9. In the integral domain S defined in problem 2-8, show that the element 21 has two different factorizations into primes. *Hint:* For one of the factorizations, let one of the primes be $1 - 2\sqrt{-5}$.

2-10. In the integral domain S defined in problem 2-8, show that the elements 147 and $21 - 42\sqrt{-5}$ have no greatest common divisor. *Hint:* First show that 21 is a common divisor and that $7 - 14\sqrt{-5}$ is a common divisor.

2-11. **(a)** Apply Algorithm 2.1 (by hand) to compute, in the Euclidean domain **Z**,

$$g = \text{GCD}(3801, 525).$$

(b) Apply Algorithm 2.2 (by hand) to compute g as in part (a) and thus determine integers s and t such that

$$g = s(3801) + t(525).$$

2-12. **(a)** Apply Algorithm 2.1 (by hand) to compute, in the Euclidean domain $\mathbf{Q}[x]$,

$$\text{GCD}(4x^4 + 13x^3 + 15x^2 + 7x + 1,\ 2x^3 + x^2 - 4x - 3).$$

(b) Apply Algorithm 2.3 (by hand) to compute, in the Euclidean domain $\mathbf{Q}[x]$, the GCD of the polynomials in part (a).

(c) Apply Algorithm 2.3 (by hand) to compute, in the UFD $\mathbf{Z}[x]$, the GCD of the polynomials in part (a).

2-13. Apply Algorithm 2.3 (by hand) to compute, in the UFD $\mathbf{Z}[x, y]$,

$$\text{GCD}\,(15xy - 21x - 15y^2 + 21y,\ 6x^2 - 3xy - 3y^2).$$

2-14. In the quotient field Q(D) of any integral domain D in which GCD's exist, prove that each equivalence class $[a / b] \in$ Q(D) has one and only one representative a / b satisfying properties (75) - (76) of section 2.7.

2-15. **(a)** In the field $\mathbf{Z}(x)$ of rational functions over **Z**, let

$$a(x) / b(x) = (1080x^3 - 3204x^2 + 1620x - 900) / (-264x^2 + 348x + 780);$$

$$c(x) / d(x) = (10x^2 - 10) / (165x^2 + 360x + 195).$$

Put $a(x) / b(x)$ and $c(x) / d(x)$ into their canonical forms satisfying properties (75)-(76) of section 2.7.

(b) Let $a(x) / b(x)$ and $c(x) / d(x)$ be the rational functions defined in part (a). Calculate:

$$[a(x) / b(x)] + [c(x) / d(x)] \quad \text{and}$$

$$[a(x) / b(x)][c(x) / d(x)]$$

and put the results into their canonical forms as elements of the field $\mathbf{Z}(x)$.

(c) What are the canonical forms of the two rational functions in part (a) as elements of the field $\mathbf{Q}(x)$? What are the canonical forms of the sum and product of these two rational functions as elements of the field $\mathbf{Q}(x)$?

2-16. Determine the inverse in the power series domain $\mathbf{Z}[[x]]$ of the unit power series

$$a(x) = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$$

where $a_k = a_{k-1} + a_{k-2}$ $(k \geqslant 2)$. (Note: The sequence $\{a_k\}$ is the famous *Fibonacci sequence*).

2-17. **(a)** In the field $\mathbf{Q}((x))$ of power series rational functions over **Q**, let

$$a(x) / b(x) = (1 + x + x^2 + x^3 + x^4 + \cdots) / (2x^4 + 2x^5 + 4x^6 + 6x^7 + 10x^8 + \cdots)$$

where $b_k = b_{k-1} + b_{k-2}$ $(k \geqslant 6)$. Put $a(x) / b(x)$ into its canonical form

satisfying properties (75)-(76) of section 2.7.

(b) Express $a(x) / b(x)$ of part (a) as an extended power series in the field $\mathbf{Q}\langle x \rangle$.

2-18. Give a complete specification of the elements in the intersection of the domains $D((x))$ and $F_D[[x]]$, as subsets of $F_D((x))$.

2-19. Determine a rational function representation in $\mathbf{Z}(x)$ for the following power series in $\mathbf{Z}[[x]]$:

$$c(x) = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + \cdots .$$

Hint: Noting that $c_k = k$ does not lead directly to a finite linear recurrence of the form (96), but use the fact that $k = 2(k - 1) - (k - 2)$.