1. INTRODUCTION TO ALGEBRAIC ALGORITHMS

Keith O. Geddes

Symbolic Computation Group
Department of Computer Science
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

OUTLINE

1. Basic Algebra Definitions
2. Algebra of Polynomials and Rational Functions
3. Power Series Domains

Reference: Chapter 2 of
Geddes, Czapor, and Labahn

BASIC ALGEBRA DEFINITIONS

The fundamental algebraic structures are defined in terms of the following six axioms:

A1: Associativity
A2: Existence of an Identity Element
A3: Existence of Inverses
A4: Commutativity
A5: Distributivity of $\times$ over $+$
A6: Cancellation Law

or equivalently
A6′: No Zero Divisors

The following table summarizes the fundamental algebraic structures, and shows which axioms apply

Definitions of algebraic structures

STRUCTURE	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
Comm. Ring [R; +, ×]	A1; A2; A3; A4 w.r.t. + A1; A2; A4 w.r.t. × A5

Definitions, cont.

Int. 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 follows)

Examples

Integral Domains:

Z (the integers)
Z[x] (polynomials)

Fields:

Q (rational numbers)
R (real numbers)
Z_p (integers modulo p)

where p is a prime integer
(this is a finite field)

Commutative Ring:

Z_m (integers modulo m)

where m is a non-prime integer

Divisibility and Factorization

Definition:

For a, b *in* **D**, c *in* **D** is 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:

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

Definition:

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

c and d are associates if and only if $cu = d$ for some unit u

If c is a GCD of a and b then so is any associate $d = cu$

GCD, continued

It is useful to impose uniqueness:

associativity is an equivalence relation

e.g. in Z, the associate classes are

{0}, {1, −1}, {2, −2}, · · ·

define a canonical representative for each associate class and call it *unit normal*

Examples:

- in Z, the nonnegative integers

- in any field F, 0 and 1

GCD, continued

Definition:

If unit normal elements have been defined, c is the *unit normal GCD* of a, b *in* D, denoted c = GCD(a, b), if c is a GCD of a and b and c is unit normal. □

Definition:

The *normal part* of a *in* D, denoted n(a), is 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

$$a = \mathrm{u}(a)\,\mathrm{n}(a)$$

n(0) = 0 and define u(0) = 1. □

e.g. in Z, n(a) = $|a|$, u(a) = sign(a)

Unique Factorization Domains

Definition:

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

Definition:

a,b *in* **D** are *relatively prime* if GCD(a,b) = 1. □

Definition:

An integral domain **D** is a UFD (*unique factorization domain*) if for 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, $1 \le i \le n$) 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 $(1 \le i \le n)$ and q_j $(1 \le j \le m)$ 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 $1 \le i \le n$). □

Impose uniqueness using *unit normal primes*

UFD, cont.

Remarks:

- not every integral domain is a UFD
- GCD's do not necessarily exist in an arbitrary integral domain

Theorem:

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

Euclidean Domains

Definition:

A *Euclidean domain* is an integral domain D with a *valuation* v: D–{0} → N (nonnegative integers), such that:

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 q,r *in* D such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$. □

Example:

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

Property P2 is the *division property*

For polynomial domains, the valuation is the degree

Any Euclidean domain is a UFD

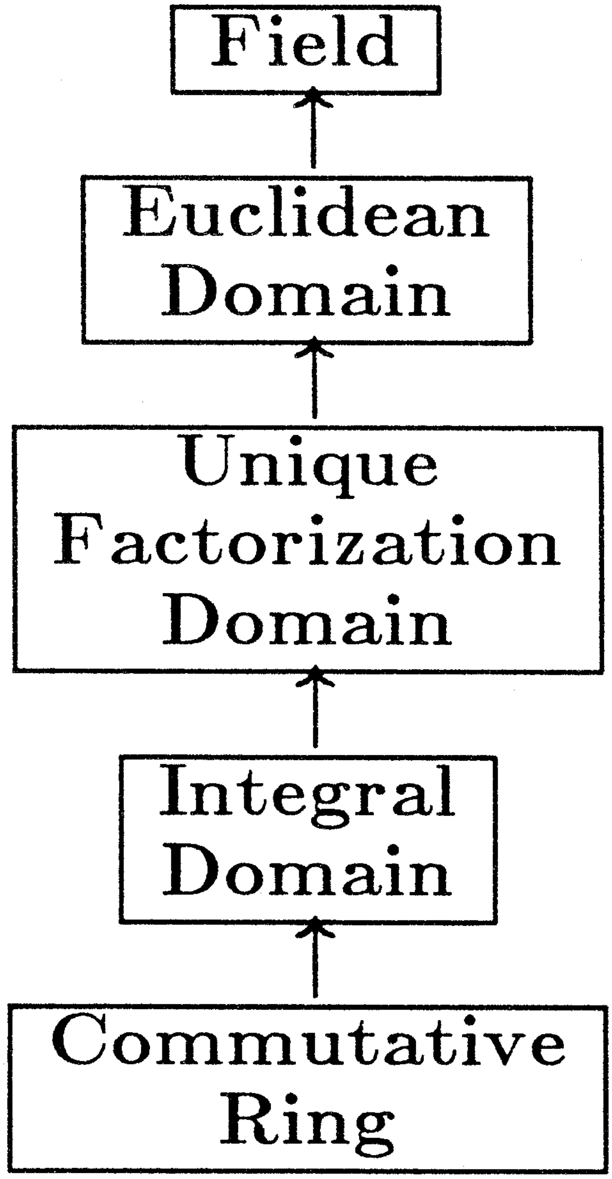
therefore GCD's exist (and are unique)

Theorem (Extended Euclidean):

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

$$g = sa + tb.$$

Hierarchy of Domains



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

Euclidean Algorithm

Fundamental Result:

If a,b *in* D (Euclidean domain) with $b \neq 0$, then GCD(a, b) = GCD(b, rem(a,b)) where "rem" is the remainder r in Property P2.

Therefore, compute *remainder sequence*:

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

until r_k=0 for some k.

Then GCD(a,b) = n(r_{k-1}).

Algorithm 2.1

```
# Given a,b in Euclidean domain D,
#   compute g = GCD(a,b).
c := n(a);  d := n(b);
while d <> 0 do
    r := rem(c,d);
    c := d;
    d := r   od;
g := n(c)
```

1-14a

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:

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

Thus $g = 6$, and GCD(18,30) = 6 as noted in Example 2.2. ●

Example 2.14. In the Euclidean domain $\mathbf{Q}[x]$, let

$$a(x) = 48x^3 - 84x^2 + 42x - 36, \quad b(x) = -4x^3 - 10x^2 + 44x - 30. \tag{2.12}$$

The sequence of values computed for $r(x)$, $c(x)$, and $d(x)$ in Algorithm 2.1 is as follows. (Here $a(x)$, $b(x)$, $r(x)$, $c(x)$, 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.)

iteration no.	$r(x)$	$c(x)$	$d(x)$
–	–	$x^3-\frac{7}{4}x^2+\frac{7}{8}x-\frac{3}{4}$	$x^3+\frac{5}{2}x^3-11x+\frac{15}{2}$
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 $g(x) = \mathrm{n}(\frac{535}{289}x - \frac{1605}{578}) = x - \frac{3}{2}$.

Extended Euclidean Algorithm

[Algorithm 2.2]

```
# Given a,b in Euclidean domain D,
#   compute g = GCD(a,b) and
#   s,t such that g = sa + tb.
c := n(a);   d := n(b);
c1 := 1;     c2 := 0;
d1 := 0;     d2 := 1;
while d <> 0 do
   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
od;
g := n(c);
s := c1 / (u(a) × u(c));
t := c2 / (u(b) × u(c))
```

1-15a

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.

iteration no.	q	c	c_1	c_2	d	d_1	d_2
–	–	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. GCD(18,30) = 6 = 2(18) – 1(30) as noted in Example 2.5. ●

ALGEBRA OF POLYNOMIALS AND RATIONAL FUNCTIONS

For R a commutative ring, R[x] denotes *univariate polynomials* with coefficients in R

Algebraic Properties of R[x]:

(i) If R is commutative ring then R[x] is 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 integral domain then D[x] is integral domain. Units (invertibles) in D[x] are constant polynomials a_0 such that a_0 is a unit in coefficient domain D.

(iii) If D is UFD then D[x] is UFD. Primes (irreducibles) in D[x] are polynomials which cannot be factored with respect to coefficient domain D.

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

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

Definition:

In D[x], polynomials with unit normal leading coefficients are defined to be *unit normal*. □

Example:

In Z[x], units are constant polynomials 1 and –1. Unit normal polynomials in Z[x] are 0 and all polynomials with positive leading coefficients. □

Example:

In Q[x], units are all nonzero constant polynomials. Unit normal polynomials in Q[x] are 0 and all monic polynomials (i.e. polynomials with leading coefficient 1). □

Applications of Extended Euclidean Algorithm (EEA)

(1) Inverses mod p

Given relatively prime integers a, p *in* **Z**,
apply EEA to get $s\, a + t\, p = 1$
Then $s = a^{-1} \pmod{p}$.

(2) Inverses mod b(x)

Given relatively prime polynomials $a(x)$, $b(x)$ *in* $F[x]$, apply EEA to get
$s(x)\, a(x) + t(x)\, b(x) = 1$
Then $s(x) = a(x)^{-1} \pmod{b(x)}$.

(3) Polynomial diophantine equations

Theorem:

Let $F[x]$ be Euclidean domain over F. Let $a(x)$, $b(x)$ *in* $F[x]$ be nonzero and let $g(x) = \mathrm{GCD}(a(x), b(x))$ *in* $F[x]$. Then for any 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
$\sigma(x)\, a(x) + \tau(x)\, b(x) = c(x)$ and
$\deg[\sigma(x)] < \deg[b(x)] - \deg[g(x)]$.

Multivariate Polynomial Domains

Distributive View

For commutative ring R, R[x] where

$\mathbf{x} = (x_1, \ldots, x_\nu)$, denotes all expressions

$$a(\mathbf{x}) = \sum_{\mathbf{e} \ in\ \mathbf{N}^\nu} a_\mathbf{e} \mathbf{x}^\mathbf{e}$$

with $a_\mathbf{e}$ *in* R, where it is understood that only a finite number of coefficients $a_\mathbf{e}$ are nonzero.

I.e., *multivariate polynomials* over the ring R in the indeterminates x.

Recursive View

Identify (for example)

$$R[x_1, x_2] = R[x_2][x_1]$$

This identification serves to define the arithmetic operations

Similarly, identify

$$R[x_1, x_2, x_3] = R[x_2, x_3][x_1]$$

and so on recursively

Example 2.17. The polynomial $a(x,y) \in \mathbf{Z}[x,y]$ given in (2.25) may be viewed as a polynomial in the ring $\mathbf{Z}[y][x]$

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

Considered as a polynomial in the ring $\mathbf{Z}[x][y]$ we have

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

●

Algebraic Properties of R[x]

Theorem:

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

(ii) If D is integral domain then D[x] is integral domain. Units in D[x] are constant polynomials a_0 such that a_0 is a unit in coefficient domain D.

(iii) If D is UFD then D[x] is UFD.

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

(v) If F is a field then F[x] is a UFD but not a Euclidean domain if the number of indeterminates is greater than one. □

Definition:

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

Computation in Z versus Q

Example: In UFD Z[x],

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

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

Unique unit normal factorizations in Z[x]:

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

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

where u(a(x)) = 1 has not been explicitly written, and u(b(x)) = −1.

Thus

$$\mathrm{GCD}(a(x), b(x)) = 2\,(2x - 3) = 4x - 6. \quad \square$$

Example:

In Euclidean domain Q[x], same a(x), b(x).
Unique unit normal factorizations in Q[x]:

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

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

where u(a(x)) = 48 and u(b(x)) = −4.
Thus

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

Primitive Polynomials

Previously, we split elements in integral domain into *unit part* and *normal part*

In polynomial domain D[x], further split *normal part* into *content* (*in* D) and *primitive part* (purely polynomial)

Definition:

In polynomial domain D[x] over UFD D, nonzero polynomial a(x) is called *primitive* if it is a unit normal polynomial and its coefficients are relatively prime. □

Definition:

In polynomial domain D[x] over UFD D, the *content* of nonzero polynomial a(x), denoted cont[a(x)], is the GCD of the coefficients of a(x).

Primitive Polynomials, cont.

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).**
Define cont[0] = 0 and pp[0] = 0. □

Gauss's Lemma: The product of any two primitive polynomials is itself primitive.

We have:

$$GCD(a(x), b(x)) = GCD(cont[a(x)], cont[b(x)]) \times GCD(pp[a(x)], pp[b(x)])$$

We may restrict our attention to the computation of GCD's of *primitive* **polynomials in D[x].**

Example

For a(x), b(x) *in* Z[x] as before:

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

For the same polynomials considered as elements in the domain Q[x]:

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

Pseudo-Division

Pseudo-Division (Property P3):

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

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

**with deg[r(x)] < deg[b(x)],
where β = lcoeff[b(x)] and
l = deg[a(x)] – deg[b(x)] + 1.** □

q(x) and r(x) appearing in Property P3 are called, respectively, the *pseudo-quotient* and *pseudo-remainder*:
pquo(a, b, x) and prem(a, b, x)

If a(x) and b(x) are primitive, the pseudo-division property leads directly to a GCD algorithm similar to the Euclidean Algorithm, using:

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

Primitive PRS Euclidean Algorithm

Algorithm 2.3

```
# Given a,b in D[x], compute
#    g = GCD(a,b).
c := pp(a,x);  d := pp(b,x);
while d <> 0 do
    r := prem(c,d,x);
    c := d;
    d := pp(r,x)  od;
γ := GCD(cont(a,x), cont(b,x));
g := γ× c
```

Main point:

Computation remains in integral domain D, thus avoiding fractions

Remarks:

- cost of content calculations makes this algorithm too expensive
- improved PRS algorithms: Reduced PRS and Subresultant PRS
- better yet: Hensel-based algorithms; Sparse Modular algorithm; single-point evaluation/interpolation

Example 2.22. In the UFD $\mathbf{Z}[x]$, let $a(x)$, $b(x)$ be the polynomials considered variously in Examples 2.14 - 2.15 and Examples 2.19 - 2.21. Thus

$$a(x) = 48x^3 - 84x^2 + 42x - 36, \quad b(x) = -4x^3 - 10x^2 + 44x - 30.$$

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

iteration	$r(x)$	$c(x)$	$d(x)$
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	$4280x - 6420$	$34x^2 - 95x + 66$	$2x - 3$
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.

Example 2.23. In the UFD $\mathbf{Z}[x,y]$ let $a(x,y)$ and $b(x,y)$ be given by

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

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

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:

$$\mathrm{u}(a(x,y)) = -1,$$

$$\mathrm{cont}(a(x,y)) = \mathrm{GCD}(30y, -(90y^2 + 15), 60y, -45y^2) = 15;$$

$$\mathrm{pp}(a(x,y)) = (2y)\,x^3 - (6y^2 + 1)\,x^2 + (4y)\,x - (3y^2);$$

and

$$\mathrm{u}(b(x,y)) = 1,$$

$$\mathrm{cont}(b(x,y)) = \mathrm{GCD}(100y - 140, -(250y^2 - 350y), -(150y^3 - 210y^2))$$

$$= 50y - 70.$$

$$\mathrm{pp}(b(x,y)) = (2)\,x^2 - (5y)\,x - (3y^2).$$

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

iteration	$r(x)$	$c(x)$	$d(x)$
0	–	$(2y)x^3-(6y^2+1)x^2+(4y)x-(3y^2)$	$2x^2-(5y)x-(3y^2)$
1	$(2y^3+6y)x-(6y^4+18y^2)$	$2x^2-(5y)x-(3y^2)$	$x-(3y)$
2	0	$x-(3y)$	0

Thus,

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

and

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

Example 2.24. In the Euclidean domain **Q**$[x]$, let $a(x)$, $b(x)$ be the polynomials of Example 2.14. The sequence of values computed for $r(x)$, $c(x)$, and $d(x)$ in Algorithm 2.3 is as follows:

iteration	$r(x)$	$c(x)$	$d(x)$
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.

RATIONAL FUNCTIONS

Any integral domain D can be extended to a field:

- **the** *quotient field* **of D**
- **general notation:** Q(D) **or** F_D

Quotient field of D[x] is denoted D(x), the field of *rational functions* **or** *rational forms*

The quotient field contains equivalence classes of elements: need a *canonical form* **for each equivalence class**

- **the representative** *a/b* **is canonical if**
  - *GCD(a,b) = 1*
  - *b is unit normal in D*
  - *a and b are canonical in D*

Note that the fields Z(x) and Q(x) are isomorphic

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

$$\mathrm{GCD}(a,b) = 1, \tag{2.44}$$

$$b \text{ is unit normal in D}, \tag{2.45}$$

$$a \text{ and } b \text{ are canonical in D}. \tag{2.46}$$

Any representative c/d may be put in this canonical form 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 2.20) that for each equivalence class in Q(D) there is one and only one representative satisfying (2.44), (2.45) and (2.46).

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 $-1/2$.

●

Two polynomial domains of interest in symbolic computation are the 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

$$a(x)\,/\,b(x) = (\tfrac{17}{100}x^2 - \tfrac{3}{112}x + \tfrac{1}{2})\,/\,(\tfrac{5}{9}x^2 + \tfrac{4}{5}). \tag{2.47}$$

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 (2.47) 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 (2.47) in $\mathbf{Q}(x)$ is

$$a(x)\,/\,b(x) = (4284x^2 - 675x + 12600)\,/\,(14000x^2 + 20160) \tag{2.48}$$

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 $D(\mathbf{x})$ and $F_D(\mathbf{x})$ are isomorphic. More specifically, there is a natural one-to-one correspondence between the equivalence classes in $D(\mathbf{x})$ and the equivalence classes in $F_D(\mathbf{x})$. The only difference between the two fields is that each equivalence class has many more representatives in $F_D(\mathbf{x})$ than in $D(\mathbf{x})$.

Power Series Domains

Example 2.27. In the polynomial domain $\mathbf{Z}[x]$ the only units are 1 and -1. In the power series domain $\mathbf{Z}[[x]]$, any power series with constant term 1 or -1 is a unit in $\mathbf{Z}[[x]]$. For example, the power series $1-x$ is a unit in $\mathbf{Z}[[x]]$ 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.

●

Example 2.29. In the power series domain $\mathbf{Z}[[x]]$, 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. ●

Example 2.30. In the domain $\mathbf{Q}((x))$ of power series rational functions over the field $\mathbf{Q}$, 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

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

•

1-37

Example 2.31. In the field $\mathbf{Q}\langle x\rangle$ 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

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

and

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

Thus,

$$[a(x)]^{-1} = x^{-2}\,(1 - \frac{1}{2}x) = x^{-2} - \frac{1}{2}x^{-1}.$$