International Mathematical Forum, Vol. 7, 2012, no. 31, 1517 - 1535

Two Proofs of the Existence and Uniqueness of the Partial Fraction Decomposition

William T. Bradley and William J. Cook[1]

Appalachian State University
Mathematical Sciences – Walker Hall
121 Bodenheimer Dr. Boone, NC 28608, USA

Abstract

Two proofs of the existence and uniqueness of the partial fraction decomposition of a (real) rational function are presented. The first proof of existence and uniqueness uses only elementary facts from linear algebra. The second existence proof uses the Euclidean algorithm and applies to all Euclidean domains. While existence can be proven for any Euclidean domain, additional hypotheses are required to establish uniqueness. The second uniqueness proof applies to polynomials with arbitrary field coefficients as well as the ring of integers. A partial fraction decompostion contains a whole and a fractional part. We show that the whole part will vanish for proper fractions of polynomials with field coefficients. In the final section we present a method which uses the partial fraction decomposition to solve linear differential equations with constant coefficients. Then we show how the partial fraction decomposition gives a refinement of Chinese remaindering which in turn proves the existence of Hermite interpolation polynomials.

Mathematics Subject Classification: 13F07

Keywords: partial fraction decomposition, euclidean domain

1 Introduction

The partial fraction decomposition is the main tool which allows one to integrate any rational function. This is why it is usually introduced when learning elementary integral calculus. The decomposition's next appearance is usually in an introductory course on solving differential equations when it is again used to integrate rational functions. In particular, one uses it to solve the logistic

[1] cookwj@appstate.edu

equation after separating variables. When Laplace transforms are covered, the decomposition will reappear during calculations of inverse transforms. After these instances, the partial fraction decomposition often fades into distant memory.

If one looks at any number of standard calculus texts or even many non-standard texts, techniques for computing the partial fraction decomposition of real rational functions is often presented. However, such texts never discuss or prove why such a decomposition exists. We suggest this happens because such textbooks are typically focused on teaching how to use techniques. Proofs of many facts are pushed off to a future course in analysis. This is where the partial fraction decomposition slips into the cracks. Analysts view this as pure algebra (which it is) so it should not be addressed in a course on analysis. Algebraists typically view partial fractions as a technique only good for integrating and thus a problem for analysts. So, outside of the realm of symbolic computation, the partial fraction decomposition tends to never be fully discussed.

In this paper we provide a simple accessible proof of the existence and uniqueness of the partial fraction decomposition which requires only a few facts from elementary linear algebra (see section 2). The second proof found in sections 3 (existence) and 4 (uniqueness) relies on the Euclidean algorithm. The existence proof works in any Euclidean domain while the uniqueness only holds for certain Euclidean domains. These proofs would fit in any course covering basic ring theory. In the final section we discuss some (less often seen) applications of the partial fraction decomposition including solutions of nonhomogeneous linear differential equations with constant coefficients, the Chinese remainder theorem, and Hermite interpolation.

Both authors would like to thank the National Science Foundation (NSF) for partial support (NSF grant STEP 0756928). We would also like to thank the members of our research cluster: Hadi Marrow, Hannah Gilmore, and Kyle Kelley for many helpful discussions.

2 A Linear Algebraic Proof

As noted in the introduction, partial fraction decompositions are primarily useful when dealing with rational functions. In this section we present a proof of the existence and uniqueness of the partial fraction decomposition for real polynomials using only elementary facts from linear algebra.

Suppose we are given two real polynomials $f(x), g(x) \in \mathbb{R}[x]$ where $g(x) \neq 0$. If the degree of $f(x)$ is bigger than the degree of $g(x)$, we should start by performing polynomial long division. From long division we obtain (unique) real polynomials $q(x), r(x) \in \mathbb{R}[x]$ such that $f(x) = q(x)g(x) + r(x)$ where

$\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$ and so $\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$. Therefore, we may assume that our rational function is a *proper fraction*. Also, for convenience assume that $g(x)$ is monic (its leading coefficient is 1).

We will begin our proof by noting that the existence of a partial fraction decomposition for $f(x)/g(x)$ is equivalent to $f(x)$ belonging to the span of a certain set of polynomials.

Any real non-constant real polynomial can be factored into linear and quadratic factors. In particular, suppose that $g(x)$ is factored as follows:

$$g(x) = \ell_1(x)^{k_1}\ell_2(x)^{k_2}\cdots\ell_m(x)^{k_m}\cdot q_1(x)^{s_1}q_2(x)^{s_2}\cdots q_n(x)^{s_n} \tag{2.1}$$

where $\ell_i(x) = x - r_i$ are distinct linear factors, $q_j(x) = x^2 + a_jx + b_j$ are distinct irreducible quadratic factors (which have complex roots), and the exponents k_i and s_j are positive integers.

A *partial fraction decomposition* of $f(x)/g(x)$ is

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{m}\sum_{j=1}^{k_i}\frac{A_{ij}}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i}\frac{B_{ij}x + C_{ij}}{q_i(x)^j} \tag{2.2}$$

where all A_{ij}, B_{ij}, and C_{ij} are real numbers. Multiplying both sides by $g(x)$ clears the denominators.

$$f(x) = \sum_{i=1}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} \tag{2.3}$$

Notice that since $g(x)$ is divisible by these linear and quadratic factors, we have $\frac{g(x)}{(x-r_i)^j} \in \mathbb{R}[x]$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, k_i$ and $\frac{g(x)}{q_i(x)^j} \in \mathbb{R}[x]$ for all $i = 1, \ldots, n$ and $j = 1, \ldots s_i$. Therefore, finding a partial fraction decomposition for $f(x)/g(x)$ is equivalent to writing $f(x)$ as a linear combination of the members of the set $\mathcal{S}$ where

$$\mathcal{S} = \left\{ \frac{g(x)}{(x-r_i)^j} \,\middle|\, 1 \le i \le m, 1 \le j \le k_i \right\} \cup \left\{ \frac{g(x)}{q_i(x)^j}, x\frac{g(x)}{q_i(x)^j} \,\middle|\, 1 \le i \le n, 1 \le j \le s_i \right\} \tag{2.4}$$

First, note that the cardinality of $\mathcal{S}$ is $N = k_1 + \cdots + k_n + 2s_1 + \cdots + 2s_n = \deg(g(x))$. Consider $P_N = \{h(x) \in \mathbb{R}[x] \,|\, \deg(h(x)) < N \text{ or } h(x) = 0\}$, the vector space of all real polynomials of degree less than $N = \deg(g(x))$ and recall that $\dim(P_N) = N = \deg(g(x))$. Also, $\mathcal{S} \subseteq P_N$ since all of the polynoimials in S are constructed by knocking out factors from $g(x)$ or knocking out at least a degree 2 polynomial from $g(x)$ and then multiplying by x (which still results in a polynomial of degree than less $g(x)$).

Therefore, showing that all polynomials $f(x)$ (of degree less than $g(x)$) have a partial fraction decomposition is equivalent to showing $P_N = \text{Span}(\mathcal{S})$. But since $|\mathcal{S}| = N = \dim(P_N)$, this is equivalent to showing $\mathcal{S}$ is a basis for P_N. Now since $\mathcal{S}$ has N elements (it is the *correct* size), we know $\mathcal{S}$ is a basis if and only if it is linearly independent. To prove this we need a few lemmas.

Lemma 2.1. *Let $h(x), g(x) \in \mathbb{R}[x]$ (real polynomials), k a positive integer, and $r \in \mathbb{R}$ such that $g(r) \neq 0$. If $A_1, \ldots, A_k \in \mathbb{R}$ such that $h(x)(x-r)^k + A_1 g(x)(x-r)^{k-1} + A_2 g(x)(x-r)^{k-2} + \cdots + A_k g(x) = 0$, then $A_1 = A_2 = \cdots = A_k = 0$.*

Proof: If we evaluate $h(x)(x-r)^k + A_1 g(x)(x-r)^{k-1} + A_2 g(x)(x-r)^{k-2} + \cdots + A_k g(x) = 0$ at $x = r$, we get $h(r)(0)^k + A_1 g(r)(0)^{k-1} + \cdots + A_{k-1} g(r)(0) + A_k g(r) = 0$. So that $A_k g(r) = 0$. However, $g(r) \neq 0$ therefore, $A_k = 0$.

Now our equation reads $h(x)(x-r)^k + A_1 g(x)(x-r)^{k-1} + \cdots + A_{k-1} g(x)(x-r) = 0$. Factoring out and canceling $x-r$, gives us $h(x)(x-r)^{k-1} + A_1 g(x)(x-r)^{k-2} + \cdots + A_{k-1} g(x) = 0$.

Therefore, applying the same argument again we find that $A_{k-1} = 0$. Continuing in this fashion we find that $A_1 = A_2 = \cdots = A_k = 0$. ■

The next lemma (which is quite similar to Lemma 2.1) will deal with irreducible quadratic factors. Remember that irreducible quadratic polynomials have a conjugate pair of (complex) roots. Here we let i denote the imaginary root $\sqrt{-1}$.

Lemma 2.2. *Let $h(x), g(x) \in \mathbb{R}[x]$ (real polynomials), s be a positive integer, and $q(x) \in \mathbb{R}[x]$ an irreducible quadratic factor with roots $z = a+bi, \bar{z} = a-bi \in \mathbb{C}$. In addition suppose that $g(z) \neq 0$ and $g(\bar{z}) \neq 0$. If $B_1, \ldots, B_k, C_1, \ldots, C_k \in \mathbb{R}[x]$ such that $h(x)q(x)^s + (B_1 x + C_1)g(x)q(x)^{s-1} + (B_2 x + C_2)g(x)q(x)^{s-2} + \cdots + (B_k x + C_k)g(x) = 0$, then $B_1 = B_2 = \cdots = B_k = C_1 = C_2 = \cdots = C_k = 0$.*

Proof: If we evaluate $h(x)q(x)^s + (B_1 x + C_1)g(x)q(x)^{s-1} + (B_2 x + C_2)g(x)q(x)^{s-2} + \cdots + (B_s x + C_s)g(x) = 0$ at both $x = z$ and $x = \bar{z}$, we get $h(z)(0)^s + (B_1 z + C_1)g(z)(0)^{s-1} + \cdots + (B_{s-1} z + C_{s-1})g(z)(0) + (B_s z + C_s)g(z) = 0$ and $h(\bar{z})(0)^s + (B_1 \bar{z} + C_1)g(\bar{z})(0)^{s-1} + \cdots + (B_{s-1}\bar{z} + C_{s-1})g(\bar{z})(0) + (B_s \bar{z} + C_s)g(\bar{z}) = 0$ so that $(B_s z + C_s)g(z) = 0$ and $(B_s \bar{z} + C_s)g(\bar{z}) = 0$. Thus $B_s z + C_s = 0$ and $B_s \bar{z} + C_s = 0$ since $g(z) \neq 0$ and $g(\bar{z}) \neq 0$. Next, expand recall $z = a + bi$ and $\bar{z} = a - bi$ so we have $aB_s + bB_s i + C_s = 0$ and $aB_s - bB_s i + C_s = 0$. Subtracting equations yields, $2bB_s i = 0$ and so $B_s = 0$ since $b \neq 0$ (if $b = 0$ then our quadratic factor $q(x)$ has a real root $z = a + bi = a$ which contradicts the assumption that $q(x)$ is irreducible). Since $B_s = 0$ we get $C_s = B_s z + C_s = 0$. Therefore, we have that $B_s = C_s = 0$.

Now our equation reads $h(x)q(x)^s + (B_1 x + C_1)g(x)q(x)^{s-1} + (B_2 x + C_2)g(x)q(x)^{s-2} + \cdots + (B_{s-1} x + C_{s-1})q(x)g(x) = 0$. Factoring out and canceling the common factor $q(x)$, gives us $h(x)q(x)^{s-1} + (B_1x + C_1)g(x)q(x)^{s-2} + \cdots + (B_{s-1}x + C_{s-1})g(x) = 0$

We can now apply the same argument again and find that $B_{s-1} = C_{s-1} = 0$. Continuing in this fashion we have $B_1 = B_2 = \cdots = B_s = C_1 = C_2 = \cdots = C_s = 0$. ■

Proposition 2.3. *The set $\mathcal{S}$ is linearly independent.*

Proof: Suppose that $\sum_{i=1}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} = 0$. First, we focus on the factor $x - r_t$ (for some $1 \le t \le m$). Let $g_t(x) = \frac{g(x)}{(x-r_t)^{k_t}}$. Notice that all of the elements in $\mathcal{S}$ have the factor $(x-r_t)^{k_t}$ except $\frac{g(x)}{x-r_t}, \frac{g(x)}{(x-r_t)^2}, \ldots, \frac{g(x)}{(x-r_t)^{k_t}}$. Therefore,

$$\sum_{\substack{i=1\\ i\neq t}}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} = h(x)(x-r_t)^{k_t}$$

where $h(x) = \sum_{\substack{i=1\\ i\neq t}}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g_t(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g_t(x)}{q_i(x)^j} + C_{ij}\frac{g_t(x)}{q_i(x)^j}$.

Note that $\frac{g(x)}{(x-r_t)^j} = g_t(x)(x-r_t)^{k_t-j}$ and $g_t(r_t) \neq 0$. Therefore,

$$\begin{array}{rcccl} & & \sum_{i=1}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} & = & \\ \sum_{j=1}^{k_t} A_{tj}\frac{g(x)}{(x-r_t)^j} & + & \sum_{\substack{i=1\\ i\neq t}}^{m}\sum_{j=1}^{k_i} A_{ij}\frac{g(x)}{(x-r_i)^j} + \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} & = & \\ \sum_{j=1}^{k_t} A_{tj}g_t(x)(x-r_t)^{k_t-j} & + & h(x)(x-r_t)^k_t & = & 0 \end{array}$$

Applying Lemma 2.1, we have that $A_{t1} = A_{t2} = \cdots = A_{tk_t} = 0$. Therefore, $A_{ij} = 0$ for all i and j.

Next, consider a quadratic factor, $q_t(x)$ (where $1 \le t \le n$). As before, let $g_t(x) = \frac{g(x)}{q_t(x)^{s_t}}$. Everything in $\mathcal{S}$ has the factor $q_t(x)^{s_t}$ except $\frac{g(x)}{q_t(x)}, x\frac{g(x)}{q_t(x)}, \frac{g(x)}{q_t(x)^2}$, $x\frac{g(x)}{q_t(x)^2}, \ldots, \frac{g(x)}{q_t(x)^{s_t}}, x\frac{g(x)}{q_t(x)^{s_t}}$. Therefore, $\sum_{\substack{i=1\\ i\neq t}}^{n}\sum_{j=1}^{s_i} B_{ij}x\frac{g(x)}{q_i(x)^j} + C_{ij}\frac{g(x)}{q_i(x)^j} = h(x)q_t(x)^{s_t}$

where $h(x) = \sum_{\substack{i=1 \\ i\neq t}}^{n} \sum_{j=1}^{s_i} B_{ij}x\frac{g_t(x)}{q_i(x)^j} + C_{ij}\frac{g_t(x)}{q_i(x)^j}$

Note that $\frac{g(x)}{q_t(x)^j} = g_t(x)q_t(x)^{s_t-j}$, $g_t(z) \neq 0$, and $g_t(\bar{z}) \neq 0$. Therefore,

$$\begin{aligned} & & \sum_{i=1}^{n}\sum_{j=1}^{s_i} B_{ij}x\tfrac{g(x)}{q_i(x)^j} + C_{ij}\tfrac{g(x)}{q_i(x)^j} &= \\ \sum_{j=1}^{s_t} B_{tj}x\tfrac{g(x)}{q_t(x)^j} + C_{tj}\tfrac{g(x)}{q_t(x)^j} &+& \sum_{\substack{i=1 \\ i\neq t}}^{n}\sum_{j=1}^{s_i} B_{ij}x\tfrac{g(x)}{q_i(x)^j} + C_{ij}\tfrac{g(x)}{q_i(x)^j} &= \\ \sum_{j=1}^{s_t} B_{tj}xg_t(x)q_t(x)^{s_t-j} + C_{tj}g_t(x)q_t(x)^{s_t-j} &+& h(x)q_t(x)^{s_t} &= 0 \end{aligned}$$

Applying Lemma 2.2, we find that $B_t = C_t = 0$. Therefore, $B_{ij} = C_{ij} = 0$ for all i and j. Therefore, $\mathcal{S}$ is linearly independent. ■

The linear independence of $\mathcal{S} \subset P_N$ and the fact that $|\mathcal{S}| = \dim(P_N)$ implies $\mathcal{S}$ is a basis for (and thus spans) P_N. Therefore, the partial fraction decomposition exists for real polynomials.

Theorem 2.4. *Let $f(x), g(x) \in \mathbb{R}[x]$ with $g(x) \neq 0$. Then $f(x)/g(x)$ possesses a unique partial fraction decomposition (up to rearrangement of terms).*

Proof: We just need to show uniqueness. Suppose $g(x)$ factors as before and $h(x)+\sum_{i=1}^{m}\sum_{j=1}^{k_i}\frac{A_{ij}}{(x-r_i)^j}+\sum_{i=1}^{n}\sum_{j=1}^{s_i}\frac{B_{ij}x+C_{ij}}{q_i(x)^j} = \frac{f(x)}{g(x)} = \tilde{h}(x)+\sum_{i=1}^{m}\sum_{j=1}^{k_i}\frac{\tilde{A}_{ij}}{(x-r_i)^j}+\sum_{i=1}^{n}\sum_{j=1}^{s_i}\frac{\tilde{B}_{ij}x+\tilde{C}_{ij}}{q_i(x)^j}$ where $h(x), \tilde{h}(x) \in \mathbb{R}[x]$ and $A_{ij}, \tilde{A}_{ij}, B_{ij}, \tilde{B}_{ij}, C_{ij}, \tilde{C}_{ij} \in \mathbb{R}$ are two partial fraction decompositions for $\frac{f(x)}{g(x)}$. Then clearing the denominators and moving everything to the left hand side we have that $g(x)(h(x) - \tilde{h}(x))+\sum_{i=1}^{m}\sum_{j=1}^{k_i}(A_{ij}-\tilde{A}_{ij})\frac{g(x)}{(x-r_j)^i}+\sum_{i=1}^{n}\sum_{j=1}^{s_i}((B_{ij}-\tilde{B}_{ij})x+(C_{ij}-\tilde{C}_{ij}))\frac{g(x)}{q_i(x)^j} = 0$. In both of the summations, each term has a degree strictly less than $g(x)$. Therefore, if $h(x) - \tilde{h}(x) \neq 0$, the degree of the left hand side of the equation would be at least $N = \deg(g(x))$. But this is impossible since it is equal to 0. Therefore, $h(x) - \tilde{h}(x) = 0$ and so $h(x) = \tilde{h}(x)$. This means that

$$\sum_{i=1}^{m}\sum_{j=1}^{k_i}(A_{ij} - A'_{ij})\frac{g(x)}{(x-r_j)^i} + \sum_{i=1}^{n}\sum_{j=1}^{s_i}((B_{ij} - B'_{ij})x + (C_{ij} - C'_{ij}))\frac{g(x)}{q_i(x)^j} = 0$$

and so using the linear independence of $\mathcal{S}$, we have that $A_{ij} - \tilde{A}_{ij} = 0$, $B_{ij} - \tilde{B}_{ij} = 0$, and $C_{ij} = \tilde{C}_{ij} = 0$ for all i and j. Thus $A_{ij} = \tilde{A}_{ij}$, $B_{ij} = \tilde{B}_{ij}$, and $C_{ij} = \tilde{C}_{ij}$ for all i and j. Therefore, the decomposition of $f(x)/g(x)$ is unique. ■

Remark 2.5. *The proofs in this section apply equally well to polynomials whose coefficients lie in other fields. However, the appearance of irreducible factors of degree greater than 2 requires more complicated formulae and more tedious calculations. We will see how to avoid these unpleasantries in the next section.*

3 Existence in Euclidean Domains

While the proofs in the previous section used only results and concepts from elementary linear algebra, there is something unsatisfying about having to deal with linear and quadratic factors separately (as is often the case when working with polynomials over the field of real numbers). Here we present a second existence proof using the Euclidean algorithm. In fact, this proof works in the context of an arbitrary Euclidean domain. However, while a decomposition will always exist in a Euclidean domain, it is not necessarily unique. We will take a look at the uniqueness of such decompositions in section 4. Please note that a similar proof of the existence of partial fraction decompositions in Euclidean domains can be found in [PW]. We begin by reviewing a few definitions.

Definition 3.1. *An integral domain R equipped with a norm $\delta : R - \{0\} \to \mathbb{Z}_{\geq 0}$ ($\delta(r)$ is a non-negative integer for each $r \neq 0$ in R) is called a* Euclidean Domain *if and only if*

E1 *For each $a, b \in R$ such that $b \neq 0$ there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.*

E2 *$\delta(a) \leq \delta(ab)$ for all $a, b \in R - \{0\}$.*

Remark 3.2. *The definition of a Euclidean domain varies from text to text. However, these differences are (for the most part) superficial. In particular, the requirement E2 is often omitted. However, Roger in [Ro] proved that E2 is unnecessary. Specifically, if an integral domain R posseses a norm N and satisfies E1, then when R's norm is replaced by $\delta(a) = \min\{N(ax) \mid x \in R - \{0\}\}$, it becomes a Euclidean domain (in the sense of definition 3.1).*

For what follows we will assume R is a Euclidean domain with norm $\delta : R - \{0\} \to \mathbb{Z}_{\geq 0}$. Recall that every integral domain can be imbedded in its field of fractions. Let $\mathbb{F}$ be R's field of fractions. Suppose that $f/g \in \mathbb{F}$ (where $f, g \in R$) we say that f/g is a *proper fraction* if either $f = 0$ or $\delta(f) < \delta(g)$.

Recall that all Euclidean domains are principal ideal domains – that is – given any ideal $I \triangleleft R$, there exists some $a \in R$ such that $I = (a) = \{ra \,|\, r \in R\}$.

Definition 3.3. *Let $f/g \in \mathbb{F}$ where $f, g \in R$ and $g \neq 0$. Also, suppose that $g = a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell}$ where $k_i \in \mathbb{Z}_{>0}$ (each k_i is a positive integer) and every pair a_i and a_j is relatively prime (when $i \neq j$).*

Then $\dfrac{f}{g} = q + \displaystyle\sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$ *where $q, r_{ij} \in R$ is a* partial fraction decomposition *of f/g relative to $g = a_1^{k_1} \cdots a_\ell^{k_\ell}$ if for each $1 \leq i \leq \ell$ and $1 \leq j \leq k_i$ either $r_{ij} = 0$ or $\delta(r_{ij}) < \delta(a_i)$.*

If $g = a_1^{k_1} \cdots a_\ell^{k_\ell}$ is a prime factorization of g (a factorization of g into irreducibles), then we simply call this a partial fraction decomposition *of f/g.*

Remark 3.4. *Consider the special case $R = \mathbb{R}[x]$ (real polynomials) and so $\mathbb{F} = \mathbb{R}(x)$ is the field of real rational polynomials. In $\mathbb{R}[x]$ we have $\delta = \deg$ (the degree of the polynomial). Consider a partial fraction decomposition of f/g (so g is factored into irreducibles $a_1(x), a_2(x), \ldots, a_\ell(x)$).*

If $a_i(x)$ is a linear factor, then for each $1 \leq j \leq k_i$, $r_{i,j}(x) = 0$ or r_{ij} has degree 0 so in either case, it is a constant. If $a_i(x)$ is an irreducible quadratic factor, then for each $1 \leq j \leq k_i$ either $r_{i,j}(x) = 0$ or r_{ij} has degree 0 or 1, so $r_{ij}(x)$ is a constant or a linear polynomial. Thus defintion 3.3 includes our old definition as a special case.

Proposition 3.5. *Let $f, g \in R$ where $g \neq 0$. In addition suppose that $g = ab$ where a and b are relatively prime. Then $\dfrac{f}{g} = \dfrac{A}{a} + \dfrac{B}{b}$ for some $A, B \in R$.*

Proof: Since a and b are relatively prime elements of a Euclidean domain, there exist $c, d \in R$ such that $bd + ac = 1$. Therefore, $f = b(fd) + a(fc)$ and thus

$$\frac{f}{g} = \frac{b(fd) + a(fc)}{ab} = \frac{b(fd)}{ab} + \frac{a(fc)}{ab} = \frac{fd}{a} + \frac{fc}{b}$$

So $A = fd$ and $B = fc$ are the desired elements of R. ■

Proposition 3.6. *Let $f, g \in R$ where $g \neq 0$ and $g = a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell}$ where $a_1, a_2, \ldots, a_\ell$ are pairwise relatively prime and $k_i \in \mathbb{Z}_{>0}$. Then $\dfrac{f}{g} = \dfrac{A_1}{a_1^{k_1}} + \dfrac{A_2}{a_2^{k_2}} + \cdots + \dfrac{A_\ell}{a_\ell^{k_\ell}}$ for some $A_1, A_2, \ldots, A_\ell \in R$.*

Proof: Since a_1 is relatively prime with each of a_i $(2 \le i \le \ell)$, we have that $a_1^{k_1}$ and $a_2^{k_2} \cdots a_\ell^{k_\ell}$ are relatively prime (if not they would share a prime factor, so a_1 would share a prime factor with some a_i contradicting our assumption that a_1 and a_i are relatively prime.)

Applying Proposition 3.5, we obtain $\frac{f}{g} = \frac{A_1}{a_1^{k_1}} + \frac{B_1}{a_2^{k_2} a_3^{k_3} \cdots a_\ell^{k_\ell}}$ where $A_1, B_1 \in R$. Applying Proposition 3.5 again to the pair $a_2^{k_2}$ and $a_3^{k_3} \cdots a_\ell^{k_\ell}$, we obtain $A_2, B_2 \in R$ such that $\frac{B_1}{a_2^{k_2} \cdots a_\ell^{k_\ell}} = \frac{A_2}{a_2^{k_2}} + \frac{B_2}{a_3^{k_3} \cdots a_\ell^{k_\ell}}$ and so $\frac{f}{g} = \frac{A_1}{a_1^{k_1}} + \frac{A_2}{a_2^{k_2}} + \frac{B_2}{a_3^{k_3} \cdots a_\ell^{k_\ell}}$. Continuing in this fashion, we obtain $A_1, A_2, \ldots, A_\ell \in R$ such that $\frac{f}{g} = \frac{A_1}{a_1^{k_1}} + \frac{A_2}{a_2^{k_2}} + \cdots + \frac{A_\ell}{a_\ell^{k_\ell}}$. ■

Remark 3.7. *At this point we should note that both of these propositions (and their proofs) work equally well for principal ideal domains (PIDs). If R is a PID and $a, b \in R$, then $(a, b) = \{as + bt \mid s, t \in R\}$ is an ideal. Thus $(a, b) = (d)$ for some $d \in R$. It is easy to show that d is a greatest common divisor of a and b. Thus if a and b are relatively prime, we would have $s, t \in R$ such that $as + bt = 1$. However, in a PID we are just guaranteed existence whereas in a Euclidean domain, we have an algorithm for computing s and t.*

Also, note that these propositions do not follow for unique factorization domains (UFDs). In a UFD if a and b are relatively prime, one cannot always find c and d such that $ac + bd = 1$.

Proposition 3.8. *Let $A, a \in R$, $a \neq 0$, and $k \in \mathbb{Z}_{>0}$. Then there exists $q_1, r_1, \ldots, r_k \in R$ such that for each $i = 1, \ldots, k$, either $r_i = 0$ or $\delta(r_i) < \delta(a)$ and $\frac{A}{a^k} = q_1 + \frac{r_1}{a} + \frac{r_2}{a^2} + \cdots + \frac{r_k}{a^k}$.*

Proof: Since R is a Euclidean domain, we can apply the division algorithm for R to A and a. Thus, there exists $q_k, r_k \in R$ such that $A = aq_k + r_k$ where $r_k = 0$ or $\delta(r_k) < \delta(a)$. Now apply the division algorithm to q_k and a and get $q_{k-1}, r_{k-1} \in R$ such that $q_k = aq_{k-1} + r_{k-1}$ and either $r_{k-1} = 0$ or $\delta(r_{k-1}) < \delta(a)$. Continuing in this fashion, we obtain $q_1, q_2, \ldots, q_k, r_1, r_2, \ldots, r_k \in R$ where for each $i = 1, \ldots, k$ either $r_i = 0$ or $\delta(r_i) < \delta(a)$ and $A = aq_k + r_k$, $q_{i+1} = aq_i + r_i$ for $i = 1, \ldots, k-1$. Therefore,

$$\begin{aligned} \frac{A}{p^k} &= \frac{aq_k + r_k}{a^k} = \frac{q_k}{a^{k-1}} + \frac{r_k}{a^k} = \frac{aq_{k-1} + r_{k-1}}{a^{k-1}} + \frac{r_k}{a^k} = \frac{q_{k-1}}{a^{k-2}} + \frac{r_{k-1}}{a^{k-1}} + \frac{r_k}{a^k} = \ldots \\ &= q_1 + \frac{r_1}{a} + \frac{r_2}{a^2} + \cdots + \frac{r_k}{a^k} \end{aligned}$$

■

Theorem 3.9. *Given $f, g \in R$ where $0 \neq g = a_1^{k_1} \cdots a_\ell^{k_\ell}$ and $a_1, \ldots, a_\ell \in R$ are pairwise relatively prime, then f/g has a partial fraction decomposition relative to $a_1, \ldots, a_\ell$. In particular, f/g has a partial fraction decomposition.*

Proof: First, we apply Proposition 3.6 to decompose f/g into fractions whose denominators are $a_1^{k_1}, \ldots, a_\ell^{k_\ell}$. Then we apply Proposition 3.8 to each term. Finally, adding the q_1's together, we obtain the desired decomposition. ■

If we put the proofs of Propositions 3.6 and 3.8 together, we get an algorithm for computing partial fraction decompositions. In particular a decomposition can be computed by running the Euclidean algorithm ℓ times and then performing $k_1 + \cdots + k_\ell$ divisions with remainder.

Remark 3.10. *Although propositions 3.5 and 3.6 work over an PID, Proposition 3.8 requires a division algorithm (thus a Euclidean domain). Notice that the very concept of a partial fraction decomposition becomes unclear over a PID since we have no well defined way of deciding if numerators are "smaller" than denominators.*

4 Uniqueness in Euclidean Domains

We have shown that a partial fraction decomposition exists for any element of the fraction field of a Euclidean domain. Naturally we now turn to the question of uniqueness.

Recall that we already proved uniqueness in the context of real polynomials (see section 2). It turns out that uniqueness of the decomposition does not follow for all Euclidean domains. It even fails for integers. An easy example is $0 + \frac{1}{2} = 1 + \frac{-1}{2}$. We only have unique decompositions in certain Euclidean domains.

After dealing with uniqueness, we turn to the related question of when $q = 0$ in a partial fraction decomposition $\frac{f}{g} = q + \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$. For real polynomials we already know that $q = 0$ in the partial fraction decomposition of $f(x)/g(x)$ exactly when $f(x)/g(x)$ is a proper fraction (i.e. $\deg(f(x)) < \deg(g(x))$). Considering the example above, we see that an analogous statement does not hold for integers.

Throughout the remainder of this section R is a Euclidean domain with norm $\delta : R - \{0\} \to \mathbb{Z}_{\geq 0}$. Also, $f, g \in R$ and $g = a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell}$ where $a_1, \ldots, a_\ell \in R$ are pairwise relatively prime. In this section all partial fraction decompositions are relative to $g = a_1^{k_1} a_2^{k_2} \cdots a_\ell^{k_\ell}$.

If the division algorithm in R does not produce unique quotients and remainders, one should not expect partial fraction decompositions to be unique.

However, if one requires uniqueness for quotients and remainders, we will essentially be reduced to dealing with the case of polynomials.

Proposition 4.1. *Let R be a Euclidean domain.*

1. *Quotients and remainders are unique in R if and only if $\delta(a+b) \leq \max\{\delta(a), \delta(b)\}$ for all $a, b \in R - \{0\}$ such that $a + b \neq 0$.*
2. *If quotients and remainders are unique, then the units of R along with zero form a field, say $\mathbb{K}$. Moreover, either $R = \mathbb{K}$ or R is isomorphic to $\mathbb{K}[x]$.*

Proof: [Ra] and [J] ■

As a first step towards proving the uniqueness of the partial fraction decomposition when R has unique quotients and remainders, we will show that the sum of two partial fraction decomposition (with common denominators) is again a partial fraction decomposition.

Lemma 4.2. *Suppose that we have unique quotients and remainders in R and $f, h \in R$.*
If $\frac{f}{g} = q + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$ and $\frac{h}{g} = \tilde{q} + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{\tilde{r}_{ij}}{a_i^j}$ are partial fraction decompositions, then $\frac{f+h}{g} = (q+\tilde{q}) + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{r_{ij}+\tilde{r}_{ij}}{a_i^j}$ is a partial fraction decomposition.

Proof: For each i and j either $r_{ij} + \tilde{r}_{ij} = 0$ or we have one the following cases:

$r_{ij} \neq 0$ **and** $\tilde{r}_{ij} = 0$ Thus we have $\delta(r_{ij} + \tilde{r}_{ij}) = \delta(r_{ij}) < \delta(a_i)$.

$r_{ij} = 0$ **and** $\tilde{r}_{ij} \neq 0$ Thus we have $\delta(r_{ij} + \tilde{r}_{ij}) = \delta(\tilde{r}_{ij}) < \delta(a_i)$.

$r_{ij} \neq 0$ and $\tilde{r}_{ij} \neq 0$] Thus we have $\delta(r_{ij} + \tilde{r}_{ij}) \leq \max\{\delta(r_{ij}), \delta(\tilde{r}_{ij})\} < \delta(a_i)$.

■

Theorem 4.3. *When R has unique quotients and remainders, partial fraction decompositions are unique.*

Proof: Suppose $q + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j} = \frac{f}{g} = \tilde{q} + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{\tilde{r}_{ij}}{a_i^j}$ are partial fraction decompositions of f/g. Now, $q - \tilde{q} + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{r_{ij}-\tilde{r}_{ij}}{a_i^j} = \frac{f-f}{g} = \frac{0}{g} = 0$. By Lemma 4.2 the expression on the left hand side of the equation is a partial fraction decomposition of $0/g$.

Let us relabel ℓ, $k_1, \ldots, k_\ell$, and $a_1, \ldots, a_\ell$ (reordering terms if necessary) so that the sum over i no longer includes sums over j which are identically zero and each sum over j stops at the last $r_{ij} - \tilde{r}_{ij} \neq 0$. The equation $q - \tilde{q} = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{\tilde{r}_{ij}-r_{ij}}{a_i^j}$ is equivalent to $g \cdot (q - \tilde{q}) = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i}(\tilde{r}_{ij} - r_{ij}) \cdot \hat{a}_{ij}$, where $\hat{a}_{ij} = \frac{g}{a_i^j} = a_1^{k_1} \ldots a_{i-1}^{k_{i-1}} a_i^{k_i-j} a_{i+1}^{k_{i+1}} \ldots a_\ell^{k_\ell}$. Thus, we have

$$g \cdot (q - \tilde{q}) + \sum_{\substack{i=1 \\ i \neq m}}^{\ell} \sum_{j=1}^{k_i} (r_{ij} - \tilde{r}_{ij}) \cdot \hat{a}_{ij} + \sum_{j=1}^{k_m-1} (r_{mj} - \tilde{r}_{mj}) \cdot \hat{a}_{mj} = (\tilde{r}_{mk_m} - r_{mk_m}) \cdot \hat{a}_{mk_m}.$$

Notice that a_m divides the left hand side since a_m divides g and a_m divides each $\hat{a}_{ij}$ except $\hat{a}_{mk_m}$. Thus a_m divides the right hand side as well. Since a_m is relatively prime to all a_i for $i \neq m$, it cannot divide $\hat{a}_{mk_m}$ so it must divide $\tilde{r}_{mk_m} - r_{mk_m}$. So there exists some $u \in R$ such that $a_m u = \tilde{r}_{mk_m} - r_{mk_m}$. Now $\tilde{r}_{mk_m} - r_{mk_m} \neq 0$ since our summation stopped at the last nonzero term and so $\delta(\tilde{r}_{mk_m} - r_{mk_m}) < \delta(a_m)$ by the definition of a partial fraction decomposition. Therefore, $\delta(a_m) \leq \delta(a_m u) = \delta(\tilde{r}_{mk_m} - r_{mk_m}) < \delta(a_m)$ which is impossible.

Therefore, all $\tilde{r}_{ij} - r_{ij} = 0$ and so $\tilde{r}_{ij} = r_{ij}$ for all i, j. Thus $q - \tilde{q} = 0$ and so $q = \tilde{q}$ as well. ■

Corollary 4.4. *Partial fraction decompositions are unique for polynomials with field coefficients.*

Proposition 4.5. *In $\mathbb{Z}$, if we only allow non-negative remainders for division and thus only allow nonnegative integers in the numerators of the fractional part of partial fraction decompositions, then decompositions are unique.*

Proof: If we force non-negative remainders, then $0 \leq r < |a|$ and $0 \leq \tilde{r} < |a|$ implies that $|r - \tilde{r}| \leq \max\{|r|, |\tilde{r}|\} < |a|$ and the proof above applies. ■

Example 4.6. $5 + \dfrac{1}{2} + \dfrac{1}{2^2} + \dfrac{2}{3}$ *is the unique decomposition of* $\dfrac{77}{12}$ *(if we only allow nonnegative integers in numerators).*

Beyond having unique quotients and remainders we need an additional assumption to guarantee that proper fractions have $q = 0$ in their partial fraction decompositions.

Theorem 4.7. *Suppose R has unique quotients and remainders and for all $x, y, z \in R - \{0\}$ with $\delta(y) < \delta(z)$ we have $\delta(xy) < \delta(xz)$.*

If f/g is a proper fraction (i.e. $\delta(f) < \delta(g)$) and $\frac{f}{g} = q + \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$ is a partial fraction decomposition, then $q = 0$.

Proof:

Clearing denominators, $f = q \cdot g + \sum\limits_{i=1}^{\ell} \sum\limits_{j=1}^{k_i} r_{ij}\hat{a}_{ij}$ where $\hat{a}_{ij} = \frac{g}{a_i^j}$ $= a_1^{k_1} \ldots a_{i-1}^{k_{i-1}} a_i^{k_i - j} a_{i+1}^{k_{i+1}} \ldots a_\ell^{k_\ell}$. Suppose $q \neq 0$ so $q \cdot g \neq 0$, then $f - \sum\limits_{i=1}^{\ell} \sum_{j=1}^{k_i} r_{ij}\hat{a}_{ij} = q \cdot g$ and so $\delta\left(f - \sum\limits_{i=1}^{\ell} \sum_{j=1}^{k_i} r_{ij}\hat{a}_{ij}\right) = \delta(q \cdot g)$.

Notice that $g = \hat{a}_{ij}a_i^j$ and $\delta(r_{ij}) < \delta(a_i) \leq \delta(a_i^j)$. Thus by assumption $\delta(r_{ij}\hat{a}_{ij}) < \delta(\hat{a}_{ij}a_i^j) = \delta(g)$. Next, recall that units do not effect the norm's value and that we have assumed R has unique quotients and remainders. Therefore, $\delta\left(f - \sum\limits_{i=1}^{\ell} \sum\limits_{j=1}^{k_i} r_{ij}\hat{a}_{ij}\right) \leq \max\left\{\delta(f), \delta\left(-\sum\limits_{i=1}^{\ell} \sum\limits_{j=1}^{k_i} r_{ij}\hat{a}_{ij}\right)\right\} = \max\left\{\delta(f), \delta\left(\sum\limits_{i=1}^{\ell} \sum\limits_{j=1}^{k_i} r_{ij}\hat{a}_{ij}\right)\right\} \leq \max\limits_{ij}\{\delta(f), \delta(r_{ij}\hat{a}_{ij})\} < \delta(g)$ since $\delta(f) < \delta(g)$ and $\delta(r_{ij}\hat{g}_{ij}) < \delta(g)$ for all ij.

However, $\delta\left(f - \sum\limits_{i=1}^{\ell} \sum_{j=1}^{k_i} r_{ij}\hat{a}_{ij}\right) = \delta(q \cdot g) \geq \delta(g)$ and so $\delta(g) < \delta(g)$ which is impossible. Therefore, q must be 0. ■

Corollary 4.8. *If R has unique quotients and remainders and either $\delta(xy) = \delta(x)\delta(y)$ and $\delta(x) > 0$ for all $x, y \in R - \{0\}$ or $\delta(xy) \leq \delta(x) + \delta(y)$ for all $x, y \in R - \{0\}$, then $q = 0$ in partial fraction decompositions of proper fractions.*

Corollary 4.9. *For polynomials with field coefficients, $deg(f) < deg(g)$ implies $q = 0$.*

Remark 4.10. *In light of proposition 4.1, we have $q = 0$ for proper fractions whenever R has unique quotients and remainders.*

Corollary 4.11. *Let $R = \mathbb{Z}$ and suppose $a_1, \ldots, a_\ell \in \mathbb{Z}_{>0}$. Also, suppose $\frac{f}{g} = q + \sum\limits_{i=1}^{\ell} \sum\limits_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$ is a partial fraction decomposition with $r_{ij} \geq 0$ for all ij.*

Then $q = 0$ if and only if f/g is nonnegative proper fraction.

Proof: We know by Proposition 4.5 that partial fraction decompositions are unique under the assumption that $r_{ij} \geq 0$.

Since $|xy| = |x||y|$ for all $x, y \in \mathbb{Z} - \{0\}$, notice that the proof of Theorem 4.7 applies *for nonnegative integers*. Thus if f/g is a nonnegative proper fraction, then $q = 0$. [Note that if negative integers are allowed, $|x - y| \leq \max\{|x|, |y|\}$ may fail to hold. Thus the proof of Theorem 4.7 does not work for negative integers.]

If f/g is nonnegative and $f \geq g$ (non-proper), then there exists (unique) $q, r \in \mathbb{Z}$ such that $f = q \cdot g + r$ and $0 \leq r < g$. Thus $\dfrac{f}{g} = \dfrac{q \cdot g + r}{g} = q + \dfrac{r}{g}$. Now as we have just shown, the partial fraction decomposition of r/g (which is nonnegative and proper) has the property that "$q = 0$". Thus the non-fractional part of the decomposition of f/g is q. Since f/g is not proper, $q \neq 0$.

Finally if f/g is negative and $r_{ij} \geq 0$, then $q = \frac{f}{g} - \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j} < 0$. Therefore, $q \neq 0$. ■

Example 4.12. $-\dfrac{1}{6} = -1 + \dfrac{1}{2} + \dfrac{1}{3}$ *is a partial fraction decomposition of* $-1/6$.

Notice that $q = -1 \neq 0$ *since* $-1/6 < 0$. *It is interesting to note that* $-\frac{1}{6} = \frac{-1}{2} + \frac{1}{3}$ *is also a partial fraction decomposition. This time* $q = 0$. *However, we needed a negative numerator to get this.*

5 A Few Applications

As mentioned in the introduction, the partial fraction decomposition of a real rational function is usually discussed in one's introduction to integral calculus and ordinary differential equations. This decomposition is primarily used to facilitate the integration of rational functions or compute inverse Laplace transforms. For example,

$$\int \frac{2x^3 + 3x^2 + 2x - 1}{(x^2+1)(x+1)^2}\, dx = \int \frac{2x}{x^2+1} + \frac{-1}{(x+1)^2}\, dx = \ln(x^2+1) + \frac{1}{x+1} + C$$

In differential equations, one solves the logistic equation by first separating variables and then uses the partial fraction decomposition to help integrate a certain rational function.

Sometimes the partial fraction decomposition is used as an algebraic "trick" for dealing with certain expressions. For example, it lets us see that the following series telescopes (and thus lets us find its sum):

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = \sum_{n=1}^{\infty} \frac{1}{n} - \frac{1}{n+1} = \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots = 1$$

We now turn to a few lesser known applications of the partial fraction decomposition.

5.1 Linear Differential Equations with Constant Coefficients

Another interesting application to the field of differential equations is that of inverting certain linear differential operators. The following technique will allow us to solve any (homogeneous or nonhomogeneous) linear differential equation with constant coefficients. In a typical differential equations course one is taught to solve such equations using variation of parameters (or in certain special cases using the method of undetermined coefficients). We offer this alternative (see for example [I] section 6.2).

Suppose we have a linear differential equation with constant coefficients $y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_2y'' + a_1y' + a_0y = g(t)$. Then letting $L = D^n + a_{n-1}D^{n-1} + \cdots + a_2D^2 + a_1D + a_0$ where $D = d/dt$, we can rewrite the equation as $L[y] = g(t)$. If L^{-1} existed we could write $y = L^{-1}[g(t)]$ and "solve" the equation. However, L has a nontrivial kernel (there are homogeneous solutions), so technically L^{-1} does not exist. Let us try to attach some meaning to L^{-1} anyway.

First, factor L. This can be done since we are dealing with constant coefficients and all operators commute. We will factor over the field of complex number to simplify notation. $L = (D-r_1)^{k_1}(D-r_2)^{k_2}\cdots(D-r_\ell)^{k_\ell}$. Next, treat D as a formal variable and perform the partial fraction decomposition on $1/L$. So that $L^{-1} = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}(D-r_i)^{-j}$ for some complex numbers s_{ij}. This implies the following formal relation:

$$1 = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}(D-r_1)^{k_1}\cdots(D-r_{i-1})^{k_{i-1}}(D-r_i)^{k_i-j}(D-r_{i+1})^{k_{i+1}}\cdots(D-r_\ell)^{k_\ell} \tag{5.1}$$

Since the relation holds among formal variables, it also holds among operators. Note that in terms of operators, the left hand side is the identity operator.

Consider the special case $(D-r)^k[y] = g(t)$. If $k = 1$, then we have $(D-r)[y] = y' - ry = g(t)$. This is a first order linear differential equation which is easily solved using an integrating factor. In this case $y = e^{rt}\int e^{-rt}g(t)\,dt$. If $k = 2$, we have $(D-r)^2[y] = (D-r)[(D-r)[y]] = g(t)$. So $(D-r)[y] = e^{rt}\int e^{-rt}g(t)\,dt$ and applying this formula again yields $y = e^{rt}\int e^{-rt}e^{rt}\int e^{-rt}g(t)\,dt\,dt = e^{rt}\int\int e^{-rt}g(t)\,dt$. In general, the solution of $(D-r)^k[y] = g(t)$ is

$$y = e^{rt}\underbrace{\int\int\cdots\int}_{k-\text{fold}} e^{-rt}g(t)\,dt\cdots dt\,dt. \tag{5.2}$$

Let $y_{ij} = e^{r_i t} \underbrace{\int\int\cdots\int}_{j-\text{fold}} e^{-r_i t} g(t)\,dt\cdots dt\,dt$ and $y = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}y_{ij}$. Then

$$L[y] = (D-r_1)^{k_1}\cdots(D-r_\ell)^{k_\ell}\left[\sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}y_{ij}\right]$$

$$= \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}(D-r_1)^{k_1}\cdots(D-r_{i-1})^{k_{i-1}}(D-r_i)^{k_i-j}(D-r_{i+1})^{k_{i+1}}\cdots(D-r_\ell)^{k_\ell}\left[(D-r_i)^j[y_{ij}]\right] = \sum_{i=1}^{\ell}\sum_{j=1}^{k_i} s_{ij}(D-r_1)^{k_1}\cdots(D-r_{i-1})^{k_{i-1}}(D-r_i)^{k_i-j}(D-r_{i+1})^{k_{i+1}}\cdots(D-r_\ell)^{k_\ell}[g(t)] = g(t)$$

The second equality follows from linearity and the fact that these operators commute, the third equality follows from 5.2, and the fourth equality follows from 5.1.

We should note that each j-fold indefinite integral will add j arbitrary constants to the solution. Also, integrals coming from the same repeated factor of the linear operator can introduce redundant constants. With a little more care this can be avoided.

Example 5.1. *Consider $y''' + y'' - 5y' + 3y = g(t)$. Then $L = D^3 + D^2 - 5D + 3 = (D-1)^2(D+3)$. The partial fraction decomposition of $1/L$ is*

$$\frac{1}{L} = \frac{1}{(D-1)^2(D+3)} = \frac{(-1/16)}{D-1} + \frac{(1/4)}{(D-1)^2} + \frac{(1/16)}{D+3}$$

So our solution looks like $y = L^{-1}[y] = -\frac{1}{16}(D-1)^{-1}[g(t)] + \frac{1}{4}(D-1)^{-2}[g(t)] + \frac{1}{16}(D+3)^{-1}[g(t)]$. Thus the general solution is

$$y = -\frac{1}{16}e^t\int e^{-t}g(t)\,dt + \frac{1}{4}e^t\int\int e^{-t}g(t)\,dt\,dt + \frac{1}{16}e^{-3t}\int e^{3t}g(t)\,dt$$

Remark 5.2. *If we want to avoid complex functions appearing in our solution, we will also need to know how to invert second order differential operators related to irreducible quadratic factors.*

Consider $(D-z)(D-\bar{z})$ where $z = a+bi$ and $\bar{z} = a-bi$ and $i = \sqrt{-1}$. It can be shown by performing the partial fraction decomposition on $1/[(D-z)(D-\bar{z})]$, applying the previous formula for a single factor, and some algebra that the solution of $(D-z)(D-\bar{z})[y] = g(t)$ is

$$y = \frac{1}{b}e^{at}\sin(bt)\int e^{-at}\cos(bt)g(t)\,dt - \frac{1}{b}e^{at}\cos(bt)\int e^{-at}\sin(bt)g(t)\,dt$$

To deal with irreducible quadratic factors with multiplicity two or greater, one just iterates.

5.2 Chinese Remaindering and Hermite Interpolation

Once the partial fraction decomposition is established, it is easy to prove the Chinese remainder theorem. In fact this gives a method for computing the solution which the theorem claims exists.

Note that in a principal ideal domain R the congruence $x \equiv y \pmod{z}$ means that there exists some $k \in R$ such that $x = y + zk$ (x and y are off by a multiple of z).

Theorem 5.3 (Chinese Remainder Theorem). *Let R be a principal ideal domain with $a_1, \ldots, a_\ell \in R$ pairwise relatively prime elements. In addition suppose that $b_1, \ldots, b_\ell \in R$. Then the system of congruences $x \equiv b_i \pmod{a_i}$ for $i = 1, \ldots, \ell$ has a simultaneous solution in R.*

Proof: By Proposition 3.6 there exists $A_1, \ldots, A_\ell \in R$ such that

$$\frac{1}{a_1 \cdots a_\ell} = \frac{A_1}{a_1} + \cdots + \frac{A_\ell}{a_\ell}$$

where this equality holds in the field of fractions of R. *Note:* By Remark 3.7 proposition 3.6 holds over all PIDs not just Euclidean domains.

Clearing denominators we have $1 = A_1 a_2 \cdots a_\ell + A_2 a_1 a_3 \cdots a_\ell + \cdots + A_\ell a_1 \cdots a_{\ell-1}$. Let $c_i = A_i a_1 \cdots a_{i-1} a_{i+1} \cdots a_\ell$ and so $1 = c_1 + c_2 + \cdots + c_\ell$. Notice that $c_j \equiv 0 \pmod{a_i}$ when $i \neq j$ since c_j contains a_i as a factor for $i \neq j$. Likewise, $b_j c_j \equiv 0 \pmod{a_i}$. Therefore, $1 = c_1 + \cdots + c_\ell \equiv c_i \pmod{a_i}$ for each i and so $x = b_1 c_1 + \cdots + b_\ell c_\ell \equiv b_i c_i \equiv b_i \cdot 1 \pmod{a_i}$. Therefore, $x = b_1 c_1 + \cdots + b_\ell c_\ell \in R$ is a simultaneous solution of the congruences $x \equiv b_i \pmod{a_i}$ where $i = 1, \ldots, \ell$. ■

This result can be somewhat refined over a Euclidean domain. Let $a_1, \ldots, a_\ell$ be pairwise relatively prime elements of the Euclidean domain R and $k_i \in \mathbb{Z}_{>0}$ (positive integers). Let $b_{ij} \in R$ where $i = 1, \ldots, \ell$ and $j = 1, \ldots, k_i$. Then there exists $r_{ij} \in R$ such that

$$\frac{1}{a_1^{k_1} \cdots a_\ell^{k_\ell}} = \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \frac{r_{ij}}{a_i^j}$$

where each $r_{ij} = 0$ or $\delta(r_{ij}) < \delta(a_i)$. Clearing denominators this gives us $1 = \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} r_{ij} \hat{a}_{ij}$ where $\hat{a}_{ij} = a_1^{k_1} \cdots a_{i-1}^{k_{i-1}} a_i^{k_i - j} a_{i+1}^{k_{i+1}} \cdots a_\ell^{k_\ell}$.

Consider the following element of R:

$$x = \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \left(b_{ij} a_i^{j-1} \sum_{m=j}^{k_i} r_{im} \hat{a}_{im} \right) \tag{5.3}$$

Fix $1 \le s \le \ell$ and $1 \le t \le k_s$. Then since $a_s^{k_s}$ divides $\hat{a}_{ij}$ for all $j = 1, \ldots, k_i$ when $i \neq s$ and also $t \le k_s$, we have $\hat{a}_{ij} \equiv 0 \pmod{a_s^t}$ for $i \neq s$. Therefore, $x \equiv \sum_{j=1}^{k_s} \left(b_{sj} a_s^{j-1} \sum_{m=j}^{k_s} r_{sm} \hat{a}_{sm} \right) \pmod{a_s^t}$.

In addition notice that $a_s^{j-1}\hat{a}_{sm}$ is divisible by $a_s^{k_s-m+j-1}$ and so $a_s^{j-1}\hat{a}_{sm} \equiv 0 \pmod{a_s^{k_s}}$ when $k_s - m + j - 1 \ge k_s$. This is equivalent to $m \le j-1$. Therefore, we can change the lower limit in the sum over m from $m = j$ to $m = 1$ without changing the value of x modulo a_s^t (for all $t \le k_s$). Thus $x \equiv \sum_{j=1}^{k_s} \left(b_{sj} a_i^{j-1} \sum_{m=1}^{k_s} r_{sm} \hat{a}_{sm} \right) \pmod{a_s^t}$.

Finally note that $1 = \sum_{i=1}^{\ell} \sum_{m=1}^{k_i} r_{im} \hat{a}_{im} \equiv \sum_{m=1}^{k_s} r_{sm} \hat{a}_{sm} \pmod{a_s^t}$. Therefore, $x \equiv \sum_{j=1}^{k_s} \left(b_{sj} a_i^{j-1} \cdot 1 \right) \pmod{a_s^t}$. In summary, $x = \displaystyle\sum_{i=1}^{\ell} \sum_{j=1}^{k_i} \left(b_{ij} a_i^{j-1} \sum_{m=j}^{k_i} r_{im} \hat{a}_{im} \right)$ simultaneously solves $x \equiv \displaystyle\sum_{m=1}^{t} b_{sm} a_s^m \pmod{a_s^t}$ for all $s = 1, \ldots, \ell$ and $t = 1, \ldots, k_s$.

This refinement of Chinese remaindering gives us the following theorem.

Theorem 5.4 (Hermite Interpolation). *Given real numbers $x_i, f_{ij} \in \mathbb{R}$ where $i = 1, \ldots, \ell$, $j = 0, \ldots, k_i - 1$, and $x_i \neq x_j$ for $i \neq j$, there exists a polynomial $f(x) \in \mathbb{R}[x]$ such that $f(x) = 0$ or $\deg(f(x)) \le k_1 + k_2 + \cdots + k_\ell - 1$ and $f^{(j)}(x_i) = f_{ij}$ for all $i = 1, \ldots, \ell$ and $j = 0, \ldots, k_i - 1$.*

Proof: Let $g(x) = (x - x_1)^{k_1} \cdots (x - x_\ell)^{k_\ell}$ and $\hat{g}_{ij}(x) = g(x)/(x - x_i)^j$. We can compute the partial fraction decomposition of $1/g(x)$, clear denominators, and get $1 = \sum_{i=1}^{\ell} \sum_{j=1}^{k_i} r_{ij} \hat{g}_{ij}(x)$ where $r_{ij} \in \mathbb{R}$ (since either $r_{ij} = 0$ or $\deg(r_i j) < \deg(x - x_i) = 1$).

By the above discussion, $f(x) = \sum_{i=1}^{\ell} \sum_{j=0}^{k_i-1} \left(\frac{f_{ij}}{j!} (x - x_i)^j \sum_{m=j+1}^{k_i} r_{im} \hat{g}_{im}(x) \right)$ simultaneously solves the congruences $f(x) \equiv \sum_{m=0}^{t-1} \frac{f_{sm}}{m!} (x - x_s)^m \pmod{(x - x_s)^t}$

In particular $f(x) = f_{s0} + f_{s1}(x - x_s) + \frac{f_{s2}}{2}(x - x_s)^2 + \cdots + \frac{f_{s(k_s-1)}}{(k_s-1)!}(x - x_s)^{k_s-1} + O\left((x - x_s)^{k_s}\right)$ is the Taylor expansion of $f(x)$ about $x = x_s$ (thus $f(x)$ has the requisite derivatives).

In addition note that the degree of $(x - x_i)^j \hat{g}_{im}(x)$ is $k_1 + \cdots + k_{i-1} + (k_i - m + j) + k_{i+1} + \cdots + k_\ell$ which never exceeds $k_1 + \cdots + k_\ell - 1$ since $j < m$. ■

References

[DF] D.S. Dummit and R.M. Foote, Abstract Algebra, 3rd ed., John Wiley & Sons, Hoboken, 2004.

[I] E.L. Ince, Ordinary Differential Equations, Dover, 1956.

[J] M.A. Jodeit Jr., "Uniqueness in the Division Algorithm", American Mathematical Monthly, Vol. 74, 1967, No. 7, 835–836.

[PW] R.W. Packard and E. Stephen, "Partial fractions in Euclidean domains", Math. Mag. **62** (1989), no. 2, 115–118.

[Ra] T.-S. Rhai, "A Characterization of Polynomial Domains Over a Field", American Mathematical Monthly, Vol. 69, 1962, No. 10, 981–986.

[Ro] K. Rogers, "The Axioms for Euclidean Domains", American Mathematical Monthly, Vol. 78, 1971, No. 10, 1127–1128.

Received: October, 2011