Integers and Polynomials

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

The aim of this article is to bring to the attention of undergraduate students of mathematics the striking similarity between the set of integers and the set of polynomials, say, over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. As the student learns higher mathematics, especially modern algebra (theory of rings), he will come to know about this in a better perspective. However, it is my opinion that an attempt of this kind will show the students how mathematicians develop a theory by looking at patterns and examples. Also, proceeding along similar lines with a lot many examples and exercises, this can be given as a one-semester course on very concrete mathematics. Another aim of this article is to gently introduce the young students to one of the most powerful and exciting aspects of modern number theory which exploits this similarity between the study of numbers and that of rational functions (function fields) by employing algebraic geometric techniques.

To explain my ideas, I am going to assume some basic facts on integers and proceed to establish the above mentioned similarity.

In the rest of this article, we shall let $\mathcal{F}$ denote any one of the fields $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Most of what I say below will be true for any field, if the reader understands what a field is. By a polynomial over the field $\mathcal{F}$ with the indeterminate X, we mean an expression of the form $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ where $a_k \in \mathcal{F}$ for $0 \le k \le n$ and $n \in \mathbb{N}$. The element a_k is called the coefficient of X^k. We shall let $\mathcal{F}[X]$ denote the set of polynomials over $\mathcal{F}$. Given a polynomial $f \in \mathcal{F}[X]$, we can consider it as a function on $\mathcal{F}$: If $f(X) = \sum_{k=0}^n a_kX^k$, then the associated function is

$$\lambda \mapsto f(\lambda) := \sum_{k=0}^n a_k\lambda^k.$$

Two polynomials $f(X) := \sum_{k=0}^m a_kX^k$ and $g(X) := \sum_{r=0}^n b_rX^r$ are said to be *equal* if $m = n$ and $a_k = b_k$ for $1 \le k \le n$. It is possible that f and g may be equal as functions on $\mathcal{F}$ but are not equal as polynomials. (However, see Cor. 11.)

The first fact one learns about the integers is the division algorithm.

Theorem 1 (Division Algorithm.). *(a) Let $a > 0$ and b be two integers. Then there exist two integers q and r such that $b = qa + r$ where $0 \le r < a$.*
(b) Let f and g be polynomials in $\mathcal{F}[X]$ with $f \neq 0$. Then there exist polynomials q and r such that either $r = 0$ or $\deg r < \deg f$ such that $g = qf + r$.

Moreover the objects whose existence is assured are unique.

Proof. Let $S := \{b - ax : x \in \mathbb{Z} \ \& \ b - ax \geq 0\}$. If $b \geq 0$, we may take $x = 0$ and hence $b = ax \geq 0 \in S$. If $b < 0$, then we take $x = -b$ so that $b - ab = b(1-b) > 0$ and lies in S. In any case, we conclude that $S \neq \emptyset$. By well-ordering, S has a least element, say, r. By definition, r is of the form $r = b - aq$ for some $q \in \mathbb{Z}$. Note that $r \geq 0$. We claim that $r < a$. If not, then , $r - a \geq 0$ so that

$$r - a = b - aq - a = b - a(q+1) \geq 0,$$

and hence $r - a \in S$, a contradiction. This proves a).

To prove b), we fix $f \neq 0$. We prove that for any $g \in \mathcal{F}[X]$, there exist q and r as stated in b), using induction on the degree of g. If $\deg g < \deg f$, then we may take $q = 0$ and $r = g$. So we may assume that $\deg g \geq \deg f$. Let $g(X) = b_n X^n + \cdots + b_0$, $f(X) = a_m X^m + \cdots + a_0$ with $a_m \neq 0 \neq b_n$ and $m \leq n$. Let $n = m + k$. Let $g_1(X) := g(X) - (\frac{b_n}{a_m})X^k f(X)$. Then $\deg g_1 < \deg g$. By induction, we can write $g_1 = fq_1 + r_1$. We then have

$$\begin{aligned} g &= g_1 + \frac{b_n}{a_m} X^k f \\ &= fq_1 + r_1 + \frac{b_n}{a_m} X^k f \\ &= f(q_1 + (\frac{b_n}{a_m})X^k) + r_1. \end{aligned}$$

This completes the proof of b).

We shall prove the uniqueness part of (a). Let $b = aq + r$ and $b = ac + d$ with $0 \leq r, d < a$. Then $0 = b - b = a(q - c) + (r - d)$ so that $r - d = a(c - q)$. It follows that $|r - d| = a|c - q|$. If $c \neq q$, then $|c - q| \geq 1$ so that $a|c - q| \geq a$ whereas $|r - d| < a$, since we may assume without loss of generality $0 \leq r \leq d < a$. This contradictions forces us to conclude that $c = q$ and $r = d$.

Uniqueness part for b) is left to the reader. □

Remark 2. The q and r of the last theorem are called the *quotient* and *remainder* of b (respectively g) when divided by a (resp. f).

The quotient and the remainder are usually found by the so-called long division method of high school algebra.

The next result tells us about the Indian way of writing integers to the base 10 and much more.

Theorem 3 (Expansion w.r.t. a base)**.** *(a) Fix a natural number $b \geq 2$ in $\mathbb{N}$. We can represent any natural number a uniquely as*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0,$$

where $0 \leq r_i < b$ for all i.
(b) Let p be fixed in $\mathcal{F}[X]$. Assume that $\deg p \geq 1$.Then we can write any $f \in \mathcal{F}[X]$ uniquely as

$$f = r_n p^n + r_{n-1} p^{n-1} + \cdots + r_1 p + r_0,$$

where $0 \leq \deg r_i < \deg p$ for all i.

Proof. Let $S \subset \mathbb{N}$ be the set of integers which admit expansion as specified. Then $S \neq \emptyset$, since any natural number $a \leq b$ lies in S. Let $a \in \mathbb{N}$ be such that any integer less than a lies in S. Then, using division theorem, we can write $a = bq + r$, with $0 \leq r < b$. By hypothesis, $q \in S$ and hence we can write it uniquely as

$$q = r_n b^n + \cdots + r_1 b + r_0.$$

Then

$$\begin{aligned} a &= bq + r \\ &= b(r_n b^n + \cdots + r_1 b + r_0) + r \\ &= s_{n+1} b^{n+1} + \cdots + s_1 b + s_0, \end{aligned}$$

where $s_j = r_{j-1}$ for $1 \leq j \leq n+1$ and $s_0 = r$.

(b) is proved using the induction on the degree. □

Remark 4. Note that the division theorem gives us an algorithm to write these expansions. Suppose that we wish to write a in base b. By successive use of division theorem, we get

$$\begin{aligned} a &= bq + r_0 \\ q &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\vdots \\ q_{n-1} &= b + r_n. \end{aligned}$$

The process stops when 0 is obtained as the quotient. The desired expansion then is $a = r_n b^n + \cdots + r_1 b + r_0$.

Fix $p \in \mathcal{F}[X]$. We can write $f \in \mathcal{F}[X]$ in base p as follows:

$$\begin{aligned} f &= pq_0 + r_0 \\ q_0 &= pq_1 + r_1 \\ q_1 &= pq_2 + r_2 \\ &\vdots \\ q_{k-1} &= pq_k + r_k, \end{aligned}$$

with $\deg q_j < \deg p$ for all j. Then $f = r_k p^k + r_{k-1} p^{k-1} \cdots + r_1 p + r_0$, by back substitution. By the uniqueness of the division algorithm, this representation of f in powers of p is unique.

Ex. 5. (a) Write 123 in base 2. (b) Write $x^5 + x^3 + 1$ in base $x^2 + 1$.

We collect some standard results concerning polynomials.

Theorem 6 (Remainder Theorem)**.** *Let $f(X) \in \mathcal{F}[X]$ and $a \in \mathcal{F}$. Then $f(a)$ is the remainder when $f(X)$ is divided by $(X - a)$.*

Proof. Write $f(X) = (X-a)g(X)+r(X)$ by the division theorem. Then $\deg R < \deg(X-a) = 1$. Hence $r(X) = r \in \mathcal{F}$. Evaluating both sides at $X = a$, we get $f(a) = r$. □

Remark 7. We can give an alternate proof of the remainder theorem as follows: Consider $f(X) - f(a)$. It is divisible by $(X - a)$. For, we can write $f(X) - f(a)$ in terms of $(X^k - a^k)$ which are divisible by $(X - a)$. Hence $f(X) = g(X)(X - a) + f(a)$. By the uniqueness part of the remainder theorem, the result follows. □

Definition 8. An element $\lambda \in \mathcal{F}$ is said to a *zero* or a *root* of $f \in \mathcal{F}[X]$ if $f(\lambda) = 0$.

Corollary 9 (Root Theorem)**.** *Let the notation be as in the remainder theorem. Then a is a zero of f iff $X - a$ divides $f(X)$.* □

Corollary 10 (D'Alembert)**.** *A nonzero polynomial of degree n in $\mathcal{F}[X]$ has at most n distinct zeros in $\mathcal{F}$.* □

Corollary 11. *If $\mathcal{F}$ is an infinite field and if $f = g$ as* **functions** *on $\mathcal{F}$, then $f = g$ as polynomial.* □

Definition 12. Let $a, b \in \mathbb{Z}$. An integer $d \in \mathbb{N}$ is called a *a greatest common divisor* of a and b if (1) d divides both a and b and (2) any common divisor of a and b is smaller than or equal to d.

Let $f, g \in \mathcal{F}[X]$, $\mathcal{F}$ a field. A polynomial $p \in \mathcal{F}[X]$ is a greatest common divisor of f and g if (1) p divides both f and g and (2) if $q \in \mathcal{F}[X]$ divides them, then $\deg q \leq \deg p$.

Definition 13. Given integers a and b, we let

$$(a, b) := \{n \in \mathbb{Z} : n = xa + yb \text{ for some } x, y \in \mathbb{Z}\}.$$

Similarly define, for $f, g \in \mathcal{F}[X]$,

$$(f, g) := \{h \in \mathcal{F}[X] : h = fu + gv, \text{ for some } u, v \in \mathcal{F}[X]\}.$$

Ex. 14. If $m, n \in (a, b)$, then $m + n, mn \in (a, b)$. In fact, $ks \in (a, b)$ for any $k \in \mathbb{Z}$ and $s \in (a, b)$. Formulate and prove its analogue for the case of $\mathcal{F}[X]$.

Theorem 15. *(a) Given $a, b \in \mathbb{Z}$, there exists an integer $d \in \mathbb{Z}$ such that $(a, b) = \{nd : n \in \mathbb{Z}\}$.*
(b) Given $f, g \in \mathcal{F}[X]$, there exists $d \in \mathcal{F}[X]$ such that $(f, g) := \{h \cdot d : h \in \mathcal{F}[X]\}$.

Proof. Note that if one of a or b is zero, say, $b = 0$, then $(a, b) = (a) = \{k \cdot a : k \in \mathbb{Z}\}$. Hence, we may assume that neither of them is zero. Hence there exists positive elements in (a, b). By well-ordering principle, let d be the smallest positive integer. Let d be in (a, b). Let $d = xa + yb$. Then $kd \in (a, b)$ for any $k \in \mathbb{Z}$. Let $m \in (a, b)$. Then, by division theorem, we can write $m = qd + r$ with $0 \leq r < d$. Since $r = m - qd \in (a, b)$ and since d is the smallest positive integer in (a, b) , we infer that $r = 0$. That is, $m = kd$. Thus (a) is proved.

(b) is proved similarly. Choose $d \in (f, g)$ of least possible degree. Argue as in (a) using the division theorem. □

Ex. 16. There exists a unique greatest common divisor for a given pair of nonzero integers. There is no such uniqueness in the case of polynomials in $\mathcal{F}[X]$. For example, consider $(x^2 - 1)$ and $2x^3 + 4x^2 + 3x = x(x + 1)(x + 3) \in \mathbb{Q}[X]$. Then all polynomials of the form $\alpha(X + 1)$ are gcd's of the given polynomials.

Ex. 17. We say $f \in \mathcal{F}[X]$ is *monic* if the coefficient of the highest degree term in f is 1. Show that there exists a unique monic polynomial among the gcd's of f and g.

Ex. 18. Show that if p_j, $j = 1, 2$ are gcd's of $f, g \in \mathcal{F}[X]$, then p_j are constant multiples of each other.

Recall the Euclidean algorithm for a pair of natural numbers a and b. We apply division theorem successively as follows:

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned} \tag{1}$$

If n is such that r_n divides r_{n-1}, then r_n is the gcd of a and b.

We have an analogous Euclidean algorithm in $\mathcal{F}[X]$. Given $f, g \in \mathcal{F}[X]$, with $f \neq 0$, we apply the division theorem of $\mathcal{F}[X]$ successively:

$$\begin{aligned} g &= fq_1 + r_1, \\ f &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned} \tag{2}$$

(Since $\deg r_1 < \deg r_2 \cdots < \deg r_{k-1} < \deg r_k$, there are atmost $\deg f$ steps.) Then r_n is a $\gcd(f, g)$.

We prove both these results in

Theorem 19 (Euclidean Algorithm & Bezout's Identity). *(a) Let r_N be the last nonzero remainder in the Euclidean algorithm for $a, b \in \mathbb{N}$. Then r_N is the $\gcd(a, b)$ and we have Bezout's identity.*

$$r_N = ax + by \text{ for some integers } x, y \in \mathbb{Z}. \tag{3}$$

(b) An analogous result holds in $\mathcal{F}[X]$.

Proof. Under the hypothesis of the theorem, the number of steps in the algorithm is $N + 1$. We prove the result by induction on N.

If $N = 0$, then a divides b and hence the result follows. If $N = 1$, let

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + 0. \end{aligned}$$

It is easy to see that $r_1 = \gcd(a, b)$. Also, $r_1 = b - aq_1 = b \cdot 1 + a(-q_1)$. Hence Bezout's identity is true.

Assume that the result is true for $N = n - 1$, i.e., the theorem is true for any two natural numbers whose Euclidean algorithm takes n steps. Let $a, b \in \mathbb{N}$ be such that the algorithm takes $n + 1$ steps. Using the notation as in (1) above for the steps in the algorithm, if we ignore the first equation, the remaining n equations constitute the Euclidean algorithm for the pair (a, r_1). By induction, we conclude $r_n = \gcd(a, r_1)$, and $r_n = au + r_1 v$ for some integers u and v. Now, $b = aq_1 + r_1$. One easily shows that $\gcd(b, a) = \gcd(a, r_1)$ (Exercise). Hence we conclude that $\gcd(b, a) = \gcd(a, r_1) = r_n$. From $r_1 = b - aq_1$ and $r_n = au + r_1 v$, we see that $r_n = bv + a(u - q_1 v)$. Hence, Bezout's identity is true. Thus (a) is proved.

Proof of (b) is left to the reader. □

Definition 20. We say that an integer $n \in \mathbb{Z}$ is a *unit* if there exists an integer $m \in \mathbb{Z}$ such that $mn = 1$. It is easily shown that the only units in $\mathbb{Z}$ are ± 1.

We say that a polynomial$f(X) \in \mathcal{F}[X]$ is a *unit* if there exists $g(X) \in \mathcal{F}[X]$ such that $f(X)g(X) = 1$, the constant polynomial. It is an easy exercise to show that the only units in $\mathcal{F}[X]$ are the nonzero constant polynomials.

We say that an integer $p \in \mathbb{Z}$ is a *prime* if p is not a unit and if $p = rs$, $r, s \in \mathbb{Z}$, then either r or s is a unit. Note that if $n \in \mathbb{N}$ is a positive integer, then n is a prime iff $n > 1$ and the only positive divisors of n are n and 1.

A polynomial $p(X) \in \mathcal{F}[X]$ is said to be *irreducible* **in** $\mathcal{F}[X]$ if p is not a unit and if $p = fg$, then either f or g is a unit.

Example 21. (a) For any field $\mathcal{F}$ and $a \in \mathcal{F}$, the polynomial $X - a$ is irreducible.
(b) The polynomial $X^2 + 1 \in \mathbb{R}[X]$ is irreducible in $\mathbb{R}[X]$ but not in $\mathbb{C}[X]$.
(c) The polynomial $(X^3 - 2)$ is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{R}[X]$.

Example 22. Let $f(X) = X^2 + bX + c \in \mathbb{R}[X]$ be quadratic. We claim that f is irreducible iff f has no real roots. This follows from the root theorem. Geometrically, this happens iff the graph of f, considered as a function on $\mathbb{R}$ crosses the x-axis. We may proceed algebraically as follows:

$$\begin{aligned} f(X) &= X^2 + bX + b^2/4 + (c - \frac{b^2}{4}) \\ &= a[X + \frac{b}{2}]^2 + (c - \frac{b^2}{4}). \end{aligned}$$

Thus, at $X = -b/2$, the function f takes the minimum value $y = f(-b/2) = -\frac{b^2 - 4ac}{4}$. For large values of $|X|$, $y > 0$. Hence f crosses the x-axis iff $b^2 - 4c > 0$. (Do you understand this?)

For a long time, mathematicians believed that any polynomial $f(X) \in \mathbb{R}[X]$ of degree ≥ 3 is not irreducible. A proof was found after the fundamental theorem of algebra was proved.

Theorem 23 (Fundamental Theorem of Algebra)**.** *Let $f(X) \in \mathbb{C}[X]$ be any nonconstant polynomial. Then there exists a root $\alpha \in \mathbb{C}$.* □

We shall assume this result without proof.

Proposition 24. *There exists no irreducible polynomials in $\mathbb{R}[X]$ of degree ≥ 3.*

Proof. Let $f(X) \in \mathbb{R}[X]$ be of degree > 2. By root theorem, we may assume that $f(X)$ has no real roots. Since $f(X) \in \mathbb{C}[X]$, by the fundamental theorem of algebra, there exists a complex root, say $\lambda = a + ib$. One easily shows that $\overline{\lambda} = a - ib$ is also a root of $f(X)$. Then $p(X) = (X - \lambda)(X - \overline{\lambda}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$ and is irreducible over there. (Why? For, its roots are not real or still better, by the "$b^2 - 4c$" condition in the above example.) Using the division theorem in $\mathbb{R}[X]$, we can write

$$f(X) = p(X)q(X) + r(X), \tag{4}$$

with $\deg r \leq 1$. Let $r(X) = s + tX$, $s, t \in \mathbb{R}$. Evaluate (4), at $X = \lambda$. Sine $f(\lambda) = 0$, we deduce that $r(\lambda) = 0$, i.e., $s + t\lambda = 0$. That is, $\lambda \in \mathbb{R}$, unless $s = 0 = t$. Thus p divides f. Since $\deg p = 2 < \deg f$, f is not irreducible. □

Proposition 25. *(a) Let $p \in \mathbb{N}$ divide ab in $\mathbb{N}$. Assume that* $\gcd(p, a) = 1$. *Then p divides b.*
(b) Let $p(X) \in \mathcal{F}[X]$ divide ab in $\mathcal{F}[X]$. Assume that $\gcd(p, a)$ *are units. Then p divides b.*

Proof. By Bezout's identity, we can write $1 = pu + av$. Multiplying both sides by b, we get $b = pub + abv$. Clearly, p divides RHS and hence p divides b. □

Irreducible polynomials are like prime numbers, as the nest two results show.

Corollary 26. *(a) Let $p \in \mathbb{N}$ be a prime. If p divides ab, then p divides one of a and b.*
(b) Let $p \in \mathcal{F}[X]$ be irreducible. If p divides ab in $\mathcal{F}[X]$ then p divides one of a and b.

Proof. The only point here is that if $p \in \mathcal{F}[X]$ does not divide a, then $\gcd(p, a)$ are units. □

Theorem 27 (Fundamental Theorem of Arithmetic and its Analogue)**.** *(a) Any natural number $n \geq 2$ is a product of primes. This decomposition is unique in the sense that if $n = p_1 \cdots p_m = q_1 \cdots q_s$, then $m = s$ and there is a one-to-one correspondence between $\{p_i\}$ and $\{q_j\}$ such that p_i and q_j occur the same number of times in the above decomposition.*

(b) Any polynomial of degree ≥ 1 in $\mathcal{F}[X]$, $\mathcal{F}$ a field, is irreducible or is a product of irreducible polynomials in $\mathcal{F}[X]$. Furthermore such a factorization is unique in the following sense: If $f = p_1 \cdots p_m = q_1 \cdots q_n$, then $m = n$ and there is a one-to-one correspondence between $\{p_i\}$ and $\{q_j\}$ such that if p_i corresponds to q_j, then they differ by units in $\mathcal{F}[X]$.

Proof. If $n > 1$ is a prime, then it is a product of primes. If n is not a prime, say, $n = ab$, then by induction, a and b are products of primes and hence so is n. Thus the existence of factorization into prime factors is proved.

To prove uniqueness, assume that the result is true for all numbers $< n$. Let $n = p_1 \cdots p_r = q_1 \cdots q_s$. If n is a prime, then $n = p_1 = q_1$ and hence the result follows. If n is not a prime, then p_1 divides $n = q_1 \cdots q_s$ and hence p_1 divides some q_j. Then, $P - 1 = q_j$. Now, n/p_1 is a natural number less than n and has two factorizations $n/p_1 = p_2 \cdots p_r = q_2 \cdots q_s$. Hence, by induction, $r = s$ etc.

The proof in the case of polynomials is similar. □

The next item is to prove the existence of partial fractions in $\mathbb{Q}$, the set of rational numbers and also in $\mathcal{F}(X)$, the set of rational functions.

Definition 28. We say an expression of the form $\frac{f(X)}{g(X)}$ is a *rational function* on $\mathcal{F}$. Even though we call it a function, it is not considered, in general, as a function from $\mathcal{F}$ to $\mathcal{F}$. The set of all rational functions on $\mathcal{F}$ is denoted by $\mathcal{F}(X)$. Imitating the arithmetic operations in $\mathbb{Q}$, we can define the sum and product of two rational functions. Also, we can define a scalar multiplication in an obvious way:

$$(\alpha, r(X)) \mapsto \frac{\alpha f(X)}{g(X)} \text{ if } r(X) = \frac{f(X)}{g(X)}.$$

One can also show that if $r \in \mathcal{F}(X)$ is nonzero, it has a multiplicative inverse in the sense that there exists $s \in \mathcal{F}(X)$ such that $r(X)s(X) = 1$, the constant rational function.

The following may be noted. In the case of rational numbers, given a rational number $r = \frac{p}{q}$, then $r = \frac{ap}{aq}$ for any nonzero $a \in \mathcal{F}$. Similarly, if $r = \frac{f(X)}{g(X)} \in \mathcal{F}(X)$ is rational, then $r(X) = \frac{h(X)f(X)}{h(X)g(X)}$ for any nonzero polynomial $h \in \mathcal{F}[X]$.

We need a couple of lemmas.

Lemma 29. *Let $f, g \in \mathcal{F}[X]$. Assume that $\gcd(f,g) = d$. Then $d = rf + sg$ with $\deg r < \deg g$ and $\deg s < \deg f$.*

Proof. By Bezout's identity, we can always find r and s such that $d = rf + sg$. Using the division theorem, we write $r = gq_1 + r_1$ and $s = fq_2 + s_1$. Then

$$\begin{aligned} d &= rf + sg = (gq_1 + r_1)f + (fq_2 + s_1)g \\ &= fg(q_1 + q_2) + r_1 f + s_1 g. \end{aligned}$$

If $q_1 + q_2 \neq 0$, then the degree of the RHS is strictly greater than that of f and g so that d cannot be a divisor of f and g. Thus, $d = r_1 f + s_1 g$, and r_1 and s_1 are as required. □

Lemma 30. *Let $g = ab$, a and b being relatively prime in $\mathcal{F}[X]$. Assume that $\deg f < \deg g$. Then there exist unique polynomials r and s with $\deg r < \deg a$ and $\deg s < \deg b$ such that*

$$\frac{f}{g} = \frac{r}{a} + \frac{s}{b}.$$

Proof. By hypothesis, $\gcd(a,b) = 1$ and hence there exists r and s such that $ar + bs = f$ with $\deg r < \deg b$ and $\deg s < \deg a$. Dividing both sides of the equation by $g = ab$, we get the result. □

Theorem 31. *Let $g = p_1^{e_1} \cdots p_k^{e_k}$ be a factorization of g into a product of powers of relatively prime irreducible polynomials p_j in $\mathcal{F}[X]$. Assume that $\deg f < \deg g$. Then there exist unique polynomials h_i, $1 \leq i \leq k$, with $\deg h_i < \deg p_i^{e_i}$ such that*

$$\frac{f}{g} = \frac{h_1}{p_1^{e_1}} + \cdots + \frac{h_k}{p_k^{e_k}}.$$

Proof. By induction on k. For $k = 1$, the result is clear. To pass from k to $k-1$, we let

$$a = p_1^{e_1} \cdots p_{k-1}^{e_{k-1}} \qquad \text{and } b = p_k^{e_k}.$$

The result follows from the last lemma and induction. □

Given f/p^n, we can write f in base p:

$$\frac{f}{p^n} = \frac{r_0 + r_1 p + \cdots + r_k p^k}{p^n} = \frac{r_0}{p^n} + \frac{r_1}{p^{n-1}} + \cdots + \frac{r_k}{p^{n-k}},$$

with $\deg r_i < \deg p$ for all i.

Putting all these facts together, we get the existence of partial fractions for rational functions in $\mathcal{F}(X)$.

Theorem 32 (Partial Fractions)**.** *(a) Let $f, g \in \mathcal{F}[X]$ and $\deg f \geq 1$. Then we can write*

$$f/g = h + \sum_{p \in P} \sum_{n \in \mathbb{N}} \frac{h_{p,n}}{p^n},$$

where P is the set of monic irreducible polynomials in $\mathcal{F}[X]$, and $\deg h_{p,n} \leq \deg p^n$ and is zero except for finitely many $p \in P$.

(b) Any rational number $r \in \mathbb{Q}$ has a unique partial fraction decomposition:

$$r = m + \sum_{p \in P} \sum_{k \in \mathbb{N}} \frac{r_{p,k}}{p^k},$$

where $m \in \mathbb{Z}$., $r_{p,k} \in \{0, 1, \ldots, p-1\}$ and P is the set of primes. Also $r_{p,k} = 0$ except for finitely many $p \in P$. □

Example 33. We shall work out an example for each case. First let us look at the integers where the result is not all that well-known. Let us write the partial fraction expansions for $7/20$. Since $20 = 4 \cdot 5$, a product of integers which are coprime, we can write $1 = 4x + 5y = -4 + 5$. Multiply both sides by 7 to get $7 = 7 \cdot 5 - 7 \cdot 4$. Divide both sides by 20 to get

$$\begin{aligned} \frac{7}{20} &= \frac{7}{4} - \frac{7}{5} \\ &= (1 + \frac{3}{4}) - (1 + \frac{2}{5}) \\ &= \frac{3}{4} - \frac{2}{5} \\ &= -1 + \frac{3}{4} + \frac{3}{5}. \end{aligned}$$

To decompose a rational function into partial fractions, it is better to adopt the method learnt in calculus. Consider $\frac{X^3+X^2+X+2}{X^4+3X^2+2}$. Note that

$$(X^4 + 3X^2 + 2) = (X^2 + 1)(X^2 + 2).$$

We write

$$\frac{X^3+X^2+X+2}{X^4+3X^2+2} = \frac{aX+b}{X^2+1} + \frac{cX+d}{X^2+2}.$$

Then we have

$$X^3+X^2+X+2 = (aX+b)(X^2+2) + (cX+d)(X^2+1).$$

Equating the coefficients of equal powers, we get $a+c=1$, $b+d=1$, $2a+c=1$ and $2b+d=2$. Solving these simultaneous equations leads to the desired result.

Ex. 34. Find the partial fraction expansion of (a) $\frac{5}{12}$ and (b) $\frac{3X+5}{X^3-X^2-X+1}$ in $\mathbb{R}(X)$.

Ex. 35. Consider $\mathbb{C}(X)$, the set of rational functions on $\mathbb{C}$ as vector space over $\mathbb{C}$. Then $\{X^n : n \in \mathbb{Z}_+\} \cup \{\frac{1}{(X-\alpha)^m} : \alpha \in \mathbb{C}, m \in \mathbb{N}\}$ is a basis for this vector space. Can you find a basis for $\mathcal{F}[X]$ for any field $\mathcal{F}$?

A Final Remark. We draw the attention of the reader to the following fact. What made things work in the cases of integers and polynomials is the fact that they both have a division algorithm and an integer valued function d (modulus function in the case of integers and degree function in the case of polynomials) which are related as follows: Given f, g with $f \neq 0$, there exist q, r such that $g = fq + r$ such that either $r = 0$ or $d(r) < d(f)$. Division algorithm and the function d allowed us to use induction in all the proofs. For more details, the reader may consult any of the books on algebra found in the references below.

Acknowledgement. I thank my friend Professor S.D. Adhikari for a critical reading of this article and suggestions for improving the exposition.

References

[1] S.D. Adhikari, *Introduction to Commutative Algebra and Number Theory*, Narosa.

[2] Artin, *Algebra*, Prentice-Hall of India.

[3] Bhattacharya et al, *Basic Abstract Algebra*, Cambridge, India.

[4] Fraleigh, *A First Course in Abstract Algebra*, Narosa.