THE DIVISION ALGORITHM IN Z AND $F[T]$

KEITH CONRAD

1. Introduction

In the integers we can carry out a process of division with remainder, as follows.

Theorem 1.1. *For any integers a and b, with $b \neq 0$ there are unique integers q and r such that*

$$a = bq + r, \qquad 0 \leq r < |b|.$$

Division with remainder is also possible for certain systems of polynomials. We only work with polynomials in one variable, T. Set

$$\begin{aligned}
\mathbf{Z}[T] &= \{c_0 + c_1T + \cdots + c_dT^d : d \geq 0, c_i \in \mathbf{Z}\},\\
\mathbf{Q}[T] &= \{c_0 + c_1T + \cdots + c_dT^d : d \geq 0, c_i \in \mathbf{Q}\},\\
\mathbf{R}[T] &= \{c_0 + c_1T + \cdots + c_dT^d : d \geq 0, c_i \in \mathbf{R}\},\\
\mathbf{C}[T] &= \{c_0 + c_1T + \cdots + c_dT^d : d \geq 0, c_i \in \mathbf{C}\}.
\end{aligned}$$

For example, $\mathbf{Z}[T]$ is the collection of *all* polynomials in T with coefficients in $\mathbf{Z}$ and $\mathbf{Q}[T]$ is the collection of *all* polynomials in T with coefficients in $\mathbf{Q}$. One polynomial in $\mathbf{Z}[T]$ is $4T^3 - 7T + 8$, and one polynomial in $\mathbf{Q}[T]$ are $T^3 - (5/4)T^2 + (9/7)$. From $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ we have $\mathbf{Z}[T] \subset \mathbf{Q}[T] \subset \mathbf{R}[T] \subset \mathbf{C}[T]$.

The desired form of division with remainder for polynomials is this: for polynomials $f(T)$ and $g(T)$, where $g(T) \neq 0$, we want there to be unique polynomials $q(T)$ and $r(T)$ such that $f(T) = g(T)q(T) + r(T)$ and $r(T) = 0$ or $\deg r(T) < \deg g(T)$. We want this to take place in some system of polynomials, such as $\mathbf{Z}[T]$ or $\mathbf{Q}[T]$.

However, there is a serious problem in $\mathbf{Z}[T]$: division with remainder is not always possible! For example, we can't divide T^2 by $2T + 1$ in $\mathbf{Z}[T]$. In $\mathbf{Q}[T]$ we can say $T^2 = (2T+1)(T/2-1/4)+1/4$, with quotient $q(T) = T/2 - 1/4$ and remainder $r(T) = 1/4$ in $\mathbf{Q}[T]$, but we can't have $T^2 = (2T + 1)q(T) + r(T)$ in $\mathbf{Z}[T]$: the leading coefficient of T^2 is 1 while the leading coefficient of $(2T + 1)q(T) + r(T)$ in $\mathbf{Z}[T]$ is 2 times the leading coefficient of $q(T)$, and that's even but 1 is not even.

It turns out that we get a nice result for division of polynomials if the coefficients of the polynomials are in $\mathbf{Q}, \mathbf{R}$, or $\mathbf{C}$. More generally, we're okay with division for polynomials whose coefficients are in a *field*, where a field is the name for any system of numbers where the usual algebraic rules of addition, subtraction, and multiplication hold, and we can divide by every nonzero number. For example, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are each fields (*e.g.*, $(2/3)/(4/5) = 5/6$), but $\mathbf{Z}$ is *not* a field since 2 and 3 are in $\mathbf{Z}$ but $2/3$ is not. Here is the statement of division with remainder for polynomials with coefficients in a field, and note how similar it is to Theorem 1.1.

Theorem 1.2. *Let F be a field. For any $f(T)$ and $g(T)$ in $F[T]$, with $g(T) \neq 0$, there are unique $q(T)$ and $r(T)$ in $F[T]$ such that*

$$f(T) = g(T)q(T) + r(T), \quad r(T) = 0 \text{ or } \deg r(T) < \deg g(T).$$

When we speak about a "field F", think of F as something like $\mathbf{Q}$, $\mathbf{R}$, or $\mathbf{C}$, but not $\mathbf{Z}$.

In both Theorem 1.1 and 1.2, there are two things to be proved: for each a and nonzero b in $\mathbf{Z}$, or $f(T)$ and nonzero $g(T)$ in $F[T]$, a quotient and remainder exist satisfying the conclusions of the theorem *and* there is only one such quotient and remainder. Often when proving such "existence and uniqueness" theorems, it is convenient to split up the proof into an existence part and a uniqueness part.

Not only do Theorems 1.1 and 1.2 look the same, but they can be proved in similar (although not exactly identical) ways. First we will prove Theorem 1.1, and then we will adapt the ideas there for a proof of Theorem 1.2. We will then describe one application of the division theorem in $\mathbf{Z}$ and $F[T]$ that is widely used: base expansions.

2. Proof of Theorem 1.1

Proof. Uniqueness: For a choice of integers a and b with $b \neq 0$, assume there are q_1, r_1 and q_2, r_2 in $\mathbf{Z}$ that both satisfy the conclusion of the theorem for that a and b. That is,

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b| \tag{2.1}$$

and

$$a = bq_2 + r_2, \quad 0 \leq r_2 < |b|. \tag{2.2}$$

Comparing the equations in (2.1) and (2.2), we have $bq_1 + r_1 = bq_2 + r_2$. Subtracting,

$$b(q_1 - q_2) = r_2 - r_1. \tag{2.3}$$

This implies the difference $r_2 - r_1$ is a multiple of b.

Because r_1 and r_2 range from 0 to $|b| - 1$, the difference $r_2 - r_1$ is smaller in absolute value than $|b|$. (Why?) Feeding this into (2.3) implies

$$|b(q_1 - q_2)| = |r_2 - r_1| < |b|.$$

The only integer multiple of b that is smaller in absolute value than $|b|$ is 0, so $b(q_1 - q_2) = 0$. Because $b \neq 0$ (aha...), we must have $q_1 - q_2 = 0$, so $q_1 = q_2$. Then, returning to (2.3), $r_2 - r_1 = b \cdot 0 = 0$ and we get $r_1 = r_2$.

Existence: For a choice of integers a and b with $b \neq 0$, we want to prove there are q and r in $\mathbf{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$. We will give *two* proofs. The first one will be very short, while the second may look more fussy and formal. It is the second proof, not the first, whose ideas can generalize to the polynomial setting of Theorem 1.2.

The most interesting case is $b > 0$, so we treat this first. Consider all the integer multiples of b: $\{0, \pm b, \pm 2b, \dots\}$. Since $b \neq 0$, these multiples are equally spaced all along the real line. The integer a lies in the interval between consecutive multiples of b:

$$bq \leq a < b(q+1) \tag{2.4}$$

for some $q \in \mathbf{Z}$. (Why is $b > 0$ necessary here?) Now subtract bq from all terms in (2.4) to get $0 \leq a - bq < b$. Set $r = a - bq$, so $0 \leq r < b = |b|$. We are done.

For a second proof of existence of q and r when $b > 0$, we treat the cases $a \geq 0$ and $a < 0$ separately. We **fix** $b > 0$ and will show for each $a \geq 0$ there are appropriate q and r, and then we will show for each $a < 0$ there are appropriate q and r.

When $a \geq 0$, we argue by (strong) induction on a. If $0 \leq a < b$ then we can use $q = 0$ and $r = a$. Suppose now that $a \geq b$ and for *all* integers a_0 with $0 \leq a_0 < a$ we have the existence of a q_0 and r_0 for a_0 and b in Theorem 1.1 (namely $a_0 = bq_0 + r_0$ where $0 \leq r_0 < b$). To get q and r for a and b, we will replace a with $a_0 := a - b$. Since $a \geq b > 0$, we have $0 \leq a_0 < a$. Therefore by induction there are integers q_0 and r_0 such that $a_0 = bq_0 + r_0$ and $0 \leq r_0 < b$. Writing this as

$$a - b = bq_0 + r_0, \quad 0 \leq r_0 < b,$$

add b to both sides of the equation: $a = b(q_0 + 1) + r_0$. Use $q = q_0 + 1$ and $r = r_0$. This completes the second proof of existence for $b > 0$ and $a \geq 0$.

If $a < 0$ and $b > 0$, then consider $-a$ and b. Both are positive, so by the previous case we can write

$$-a = bQ + R, \quad 0 \leq R < b.$$

Negating, we have $a = b(-Q) - R$ with $-b < -R \leq 0$. If $R = 0$ then $a = b(-Q)$ so we can use $q = -Q$ and $r = 0$. If $R > 0$, so $-b < -R < 0$, we want to add b to $-R$ to make it positive (and still small), so write $a = b(-Q - 1) + (b - R)$ with $0 < b - R \leq b$. We can use $q = -Q - 1$ and $r = b - R$

Finally, if $b < 0$ and a is arbitrary, then consider a and $-b$. From what we already showed, we can write $a = -bQ + R$ where $0 \leq R < b$. Writing this as $a = b(-Q) + R$, we can use $q = -Q$ and $r = R$. □

Reread this proof until you see what's going on. Run through the proof with several choices for a and b, such as $a = 17$ and $b = 5$, or $a = -17$ and $b = 3$.

3. Proof of Theorem 1.2

As with the proof of Theorem 1.1, we first show uniqueness and then existence.

Proof. Uniqueness: Picking $f(T)$ and $g(T)$ in $F[T]$ with $g(T)$ being nonzero, suppose there are $q_1(T), r_1(T)$ and $q_2(T), r_2(T)$ in $F[T]$ that both satisfy the conclusion of Theorem 1.2:

$$f(T) = g(T)q_1(T) + r_1(T), \quad r_1(T) = 0 \text{ or } \deg r_1(T) < \deg g(T) \tag{3.1}$$

and

$$f(T) = g(T)q_2(T) + r_2(T), \quad r_2(T) = 0 \text{ or } \deg r_2(T) < \deg g(T). \tag{3.2}$$

Comparing the equations in (3.1) and (3.2), we have $g(T)q_1(T)+r_1(T) = g(T)q_2(T)+r_2(T)$. Subtracting,

$$g(T)(q_1(T) - q_2(T)) = r_2(T) - r_1(T). \tag{3.3}$$

This implies the difference $r_2(T) - r_1(T)$ is a polynomial multiple of $g(T)$.[1]

To prove $q_1(T) = q_2(T)$ and $r_1(T) = r_2(T)$, we will argue by contradiction. Assume $q_1(T) \neq q_2(T)$. Then $q_1(T) - q_2(T) \neq 0$, so the left side of (3.3) is not 0 and therefore the right side is not 0: $r_1(T) \neq r_2(T)$. We are going to look at the degrees of both sides of (3.3).[2] On the left side of (3.3), since the factors $g(T)$ and $q_1(T) - q_2(T)$ are not 0, we have

$$\deg(g(T)q_1(T) - q_2(T)) = \deg g(T) + \deg(q_1(T) - q_2(T)) \geq \deg g(T). \tag{3.4}$$

[1]The argument so far is just like the proof of uniqueness in $\mathbf{Z}$.

[2]Here we need a slightly different argument than in $\mathbf{Z}$, since polynomials don't have absolute values. We use the degree as a measure of size instead.

On the right side of (3.3), $r_1(T)$ and $r_2(T)$ are 0 or have degree less than $\deg g(T)$, so the highest power of T in either of them is *less than* $\deg g(T)$. Since a difference of polynomials can't lead to powers of T appearing above the highest power of T in either term, the highest power of T in $r_2(T) - r_1(T)$ is at most the highest power in $r_1(T)$ and $r_2(T)$, which is less than $\deg g(T)$. Therefore

$$\deg(r_2(T) - r_1(T)) < \deg g(T). \tag{3.5}$$

Equations (3.4) and (3.3) are inconsistent, since $g(T)(q_1(T) - q_2(T)) = r_2(T) - r_1(T)$. Therefore our assumption that $q_1(T) \neq q_2(T)$ is wrong: we must have $q_1(T) = q_2(T)$, so by (3.3) we get $r_1(T) - r_2(T) = 0$, so $r_1(T) = r_2(T)$.

Existence: Given $f(T)$ and $g(T)$ in $F[T]$ with nonzero $g(T)$, we want to find $q(T)$ and $r(T)$ in $F[T]$ such that

(1) $f(T) = g(T)q(T) + r(T)$,
(2) $r(T) = 0$ or $\deg r(T) < \deg g(T)$.

We will do this by modifying a proof for the analogous situation in $\mathbf{Z}$ (existence of q and r) that we have already discussed in Theorem 1.1.

The first proof of the existence of q and r in Theorem 1.1 does *not* generalize to polynomials: what would "equally spaced" polynomials mean? However, the second proof of the existence part of Theorem 1.1 will carry over to polynomials, using induction on the *degrees* of polynomials. Specifically, we fix $g(T)$ and will prove the existence of $q(T)$ and $r(T)$ for all $f(T)$ by using induction on the degree of $f(T)$.

The case when $g(T)$ is constant (that is, $\deg g(T) = 0$) is easy: if $g(T) = c$ is a nonzero constant then for each $f(T)$ we can use $q(T) = (1/c)f(T)$ and $r(T) = 0$.

Fix now a nonconstant $g(T) \in F[T]$. If $f(T) = 0$ use $q(T) = 0$ and $r(T) = 0$. To show for all nonzero $f(T)$ in $F[T]$ that there are polynomials $q(T)$ and $r(T)$ in $F[T]$ such that $f(T) = g(T)q(T) + r(T)$ such that $r(T) = 0$ or $\deg r(T) < \deg g(T)$, we will use strong induction on $\deg f(T)$. That is, for every integer $n \geq 0$ we will prove the existence of $q(T)$ and $r(T)$ for all $f(T)$ of degree n by strong induction on n.

If $n < \deg g(T)$, then for each $f(T)$ of degree n we can use $q(T) = 0$ and $r(T) = f(T)$.[3] Now assume that $n \geq \deg g(T)$ and the existence of $q(T)$ and $r(T)$ has been proved for $g(T)$ and all polynomials $f(T)$ of degree *less than* n. We will use this to show there are $q(T)$ and $r(T)$ for the same $g(T)$ and every $f(T)$ of degree n. Write the leading terms of $f(T)$ and $g(T)$ as

$$\begin{aligned} f(T) &= a_n T^n + \text{lower order terms}, \\ g(T) &= c_d T^d + \text{lower order terms}. \end{aligned}$$

Here $n \geq d$ (why?). We now look to the proof of existence for $\mathbf{Z}$ for inspiration. In $\mathbf{Z}$, when $a \geq b$ we passed from the case of a and b to the previous case of $a - b$ and b, which was useful because $a - b < a$. In the polynomial case we want to do something similar, but the direct analogue of using $f(T) - g(T)$ in place of $f(T)$ will usually not work since $\deg(f(T) - g(T)) = n$ if $n > d$: the degree does not drop. What we will do to get around that is subtract from $f(T)$ a *multiple* of $g(T)$, not just $g(T)$ itself, in order to get a polynomial of degree less than n.

We'll use the simplest kind of multiple of $g(T)$: multiplication by a monomial cT^i. The leading term of $g(T)(cT^i)$ is $c_d c T^{d+i}$. We want this to *match* the leading term of $f(T)$ so

[3] This corresponds to the case $0 \leq a < b$ in the proof for $\mathbf{Z}$ when $b > 0$, where we can use $q = 0$ and $r = a$.

their difference has the leading term cancel and thus cause the degree to drop. Making the leading terms match means $c_d c = a_n$ and $d + i = n$. In other words, take $c = a_n/c_d$[4] and $i = n - d$:

$$g(T)\left(\frac{a_n}{c_d}T^{n-d}\right) = \Big(c_dT^d + \text{lower order terms}\Big)\left(\frac{a_n}{c_d}T^{n-d}\right) = a_nT^n + \text{lower order terms}.$$

Since $f(T)$ and $g(T)(a_n/c_d)T^{n-d}$ have the same leading term a_nT^n, the difference $f(T) - g(T)(a_n/c_d)T^{n-d}$ is either 0 or is a polynomial of degree less than n.

Case 1: If the difference is 0 then $f(T) = g(T)(a_n/c_d)T^{n-d}$, so $f(T) = g(T)q(T) + r(T)$ where $q(T) = (a_n/c_d)T^{n-d}$ and $r(T) = 0$.

Case 2: If the difference has degree less than n, then by the inductive hypothesis there are $q_0(T)$ and $r_0(T)$ in $F[T]$ such that

(1) $f(T) - g(T)(a_n/c_d)T^{n-d} = g(T)q_0(T) + r_0(T)$,
(2) $r_0(T) = 0$ or $\deg r_0(T) < \deg g(T)$.

Bring $g(T)(a_n/c_d)T^{n-d}$ to the other side in (1):

$$f(T) = g(T)(a_n/c_d)T^{n-d} + g(T)q_0(T) + r_0(T) = g(T)((a_n/c_d)T^{n-d} + q_0(T)) + r_0(T).$$

Therefore $f(T) = g(T)q(T)+r(T)$ where $q(T) = (a_n/c_d)T^{n-d}+q_0(T)$ and $r(T) = r_0(T)$. □

In the last part of the proof (the 'reduction' part), we multiplied $g(T)$ by a monomial $(a_n/c_d)T^{n-d}$ to make the top term match the top term of $f(T)$ (in both degree and coefficient), so their difference has lower degree (or is 0). This process can be repeated to drop the degree further, until we get a polynomial that has degree less than $\deg g(T)$ or is the polynomial 0. Putting everything back together, we got $q(T)$ and $r(T)$. This is essentially the algorithm that is taught in school to divide one polynomial by another, but presented in a less formal way.

Example 3.1. Let $f(T) = 7T^4 - 1$ and $g(T) = T^2 + 5T$. What are $q(T)$ and $r(T)$ making $f(T) = g(T)q(T) + r(T)$ with $r(T) = 0$ or $\deg r(T) < 2$? Since $f(T)$ has the same leading term as $7T^2g(T)$, we compute

$$f(T) - 7T^2g(T) = -35T^3 - 1.$$

Since $-35T^3 - 1$ has the same leading term as $-35Tg(T)$, we compute

$$(-35T^3 - 1) - (-35Tg(T)) = 175T^2 - 1.$$

Since $175T^2 - 1$ has the same leading term as $175g(T)$, we compute

$$(175T^2 - 1) - 175g(T) = -875T - 1,$$

whose degree is less than $2 = \deg g(T)$, so we stop. Feeding each equation into the previous ones gives

$$\begin{aligned} f(T) &= 7T^2g(T) - 35T^3 - 1 \\ &= 7T^2g(T) - 35Tg(T) + (175T^2 - 1) \\ &= 7T^2g(T) - 35Tg(T) + 175g(T) - 875T - 1 \\ &= g(T)(7T^2 - 35T + 175) - 875T - 1. \end{aligned}$$

Thus $q(T) = 7T^2 - 35T + 175$ and $r(T) = -875T - 1$.

[4]Here we use the fact that the coefficients of the polynomial are in a field, because that is how we know that we can solve $c_dc = a_n$ for c by using division by c_d.

Example 3.2. Let $f(T) = 2T^4 + T^2 + 6$ and $g(T) = 3T^2 + 1$. Since $f(T)$ has the same leading term as $\frac{2}{3}T^2 g(T)$, we compute

$$f(T) - \frac{2}{3}T^2 g(T) = \frac{1}{3}T^2 + 6.$$

The right side has the same leading term as $\frac{1}{9}g(T)$, so we compute

$$\left(\frac{1}{3}T^2 + 6\right) - \frac{1}{9}g(T) = \frac{53}{9},$$

whose degree is less than $2 = \deg g(T)$, so we stop. Feeding the equations into each other gives

$$\begin{aligned} f(T) &= \frac{2}{3}T^2 g(T) + \frac{1}{3}T^2 + 6 \\ &= \frac{2}{3}T^2 g(T) + \frac{1}{9}g(T) + \frac{53}{9} \\ &= g(T)\left(\frac{2}{3}T^2 + \frac{1}{9}\right) + \frac{53}{9}, \end{aligned}$$

so $q(T) = \frac{2}{3}T^2 + \frac{1}{9}$ and $r(T) = \frac{53}{9}$.

4. Division algorithm in $\mathbf{Z}[T]$

Theorem 1.2 is *not* true if we work in $\mathbf{Z}[T]$ instead of $F[T]$. More precisely, the existence part breaks down: if $f(T)$ and $g(T)$ are in $\mathbf{Z}[T]$, the proof of Theorem 1.2 does not generally lead to $q(T)$ and $r(T)$ in $\mathbf{Z}[T]$ such that $f(T) = g(T)q(T) + r(T)$ where $r(T) = 0$ or $\deg r(T) < \deg g(T)$. (The uniqueness part goes through in $\mathbf{Z}[T]$ without a problem.) Look at Example 3.2. The initial data $f(T)$ and $g(T)$ are in $\mathbf{Z}[T]$ while $q(T)$ and $r(T)$ are not in $\mathbf{Z}[T]$. Why is that? Where does the proof break down?

The proof of the existence of $q(T)$ and $r(T)$ has a problem in $\mathbf{Z}[T]$ in exactly one step: when we want to multiply $g(T) = c_d T^d + \cdots$ by a suitable monomial to get the top term to match that of $f(T) = a_n T^n + \cdots$, we want to multiply $g(T)$ by some cT^{n-d} where $c_d c = a_n$. When the coefficients of polynomials are in a field we can take $c = a_n/c_d$. But when a_n and c_d are in $\mathbf{Z}$, the equation $c_d c = a_n$ may not have a solution for c in $\mathbf{Z}$. For example, if c_d is even and a_n is odd there is no solution in $\mathbf{Z}$ for c. (If we were working in $\mathbf{Q}[T]$ then at this step denominators get introduced in $q(T)$ and $r(T)$ from the leading coefficient c_d of $g(T)$. For instance, in the second example after the proof of Theorem 1.2, $g(T)$ has leading coefficient 3 and $q(T)$ and $r(T)$ have coefficients with denominators 3 and 9.)

A special (and important!) case where division in $\mathbf{Z}[T]$ is valid is when the leading coefficient of $g(T)$ is 1 and $f(T)$ is arbitrary. In this case the difficulty in the proof of Theorem 1.2 for $\mathbf{Z}[T]$ does not arise. Let's record this result.

Theorem 4.1. *For $f(T)$ and $g(T)$ in $\mathbf{Z}[T]$ where $g(T)$ has leading coefficient 1, there are unique $q(T)$ and $r(T)$ in $\mathbf{Z}[T]$ such that*

$$f(T) = g(T)q(T) + r(T), \quad r(T) = 0 \text{ or } \deg r(T) < \deg g(T).$$

The reader should check carefully that the proof of Theorem 1.2 carries over to the setting of Theorem 4.1.

We already saw an example of Theorem 4.1 in Example 3.1. There $g(T)$ has leading coefficient 1 and the resulting $q(T)$ and $r(T)$ are in $\mathbf{Z}[T]$.

5. Base expansions

Writing positive integers in base 10 is closely related to division by 10. For example,

$$36137 = 36130+7 = 3613\cdot 10+7 = (361\cdot 10+3)\cdot 10+7 = (((\mathbf{3}\cdot 10+\mathbf{6})\cdot 10+\mathbf{1})\cdot 10+\mathbf{3})\cdot 10+\mathbf{7}.$$

The digits of 36137 are in boldface in the last expression. This calculation can be written in terms of successive division by 10:

$$\begin{aligned} 36137 &= 10\cdot 3613 + \mathbf{7} \\ 3613 &= 10\cdot 361 + \mathbf{3}, \\ 361 &= 10\cdot 36 + \mathbf{1}, \\ 36 &= 10\cdot 3 + \mathbf{6}, \\ 3 &= 10\cdot 0 + \mathbf{3}. \end{aligned}$$

The base 10 digits are remainders on the right in reverse order. To write 36137 in base 6,

$$\begin{aligned} 36137 &= 6\cdot 6022 + 5, \\ 6022 &= 6\cdot 1003 + 4, \\ 1003 &= 6\cdot 167 + 1, \\ 167 &= 6\cdot 27 + 5, \\ 27 &= 6\cdot 4 + 3, \\ 4 &= 6\cdot 0 + 4. \end{aligned}$$

Using the remainders in reverse order, we'd write $36137 = 435145_6$. That means $36137 = 4\cdot 6^5 + 3\cdot 6^4 + 5\cdot 6^3 + 1\cdot 6^2 + 4\cdot 6 + 5$ (check!).

Theorem 5.1. *Fix an integer $b > 1$. Each $n \in \mathbf{Z}^+$ can be written in exactly one way as*

$$n = c_k b^k + c_{k-1}b^{k-1} + \cdots + c_1 b + c_0 \tag{5.1}$$

where $k \geq 0$ and $0 \leq c_i \leq b-1$, with $c_k \neq 0$.

The expression on the right side of (5.1) is called the *base b representation* of n.

Proof. We break up the proof into two parts: existence of a base b representation for each positive integer n and then uniqueness of the base b representation for each positive integer n.

Existence: We use (strong) induction on n. If $1 \leq n \leq b-1$ then we can use $k = 0$ and $c_0 = n$. Suppose $n \geq b$ and we can write all positive integers *less than* n in base b. As in the example of 36137 above, we will construct the base representation of n by starting with what will turn out to be its "units" digit c_0. Using division of n by b,

$$n = bq + r \tag{5.2}$$

where $0 \leq r \leq b-1$ and $q \geq 0$ (we don't have $q < 0$, since then $q \leq -1$ and $bq + r \leq -b + r = r - b < 0$, a contradiction). The integer q is "obviously" smaller than n. Let's check: since $n \geq b$ we don't have $q = 0$ in(5.2), so $q \geq 1$. Then $n = bq + r \geq bq > q$, so $0 < q < n$.

We can now apply the (strong) inductive hypothesis to q: the number q has a base b representation, say

$$q = a_\ell b^\ell + a_{\ell-1}b^{\ell-1} + \cdots + a_1 b + a_0$$

where $\ell \geq 0$ and $0 \leq a_i \leq b-1$ with $a_\ell \neq 0$. Feeding this into (5.2),

$$\begin{aligned} n &= bq + r \\ &= b(a_\ell b^\ell + a_{\ell-1}b^{\ell-1} + \cdots + a_1 b + a_0) + r \\ &= a_\ell b^{\ell+1} + a_{\ell-1}b^\ell + \cdots + a_1 b^2 + a_0 b + r, \end{aligned}$$

which is a base b representation for n as in (5.1): set $k = \ell + 1$, $c_0 = r$, and $c_i = a_{i-1}$ for $i = 1, \ldots, k$.

Uniqueness: In (5.1), $n \geq c_k b^k \geq b^k$, so if $0 \leq n < b$ then necessarily $k = 0$ and $c_0 = n$. This takes care of the uniqueness when n is less than b. From now on suppose $n \geq b$, so a base b representation must have $k \geq 1$

Write two base b representations for n as

$$n = c_k b^k + c_{k-1}b^{k-1} + \cdots + c_1 b + c_0, \quad n = c'_\ell b^\ell + c'_{\ell-1}b^{\ell-1} + \cdots + c'_1 b + c'_0,$$

where $k, \ell \geq 1$ and the "digits" c_i and c'_j are in $\{0, \ldots, b-1\}$. The uniqueness of the base b representation for n means $k = \ell$ and $c'_i = c_i$ for $i = 0, \ldots, k$. That is what we want to show.

Rewrite the two base b representations for n as

$$n = b(c_k b^{k-1} + c_{k-1}b^{k-2} + \cdots + c_1) + c_0 = bq + r, \;\; n = b(c'_\ell b^{\ell-1} + c'_{\ell-1}b^{\ell-2} + \cdots + c'_1) + c'_0 = bq' + r',$$

where $q = c_k b^{k-1} + c_{k-1}b^{k-2} + \cdots + c_1$, $r = c_0$, $q' = c'_\ell b^{\ell-1} + c'_{\ell-1}b^{\ell-2} + \cdots + c'_1$, and $r' = c'_0$. Therefore $n = bq + r = bq' + r'$ where q and q' are in $\mathbf{Z}$ and $0 \leq r, r' < b$. From the *uniqueness* of the quotient and remainder in the division algorithm in $\mathbf{Z}$, $q = q'$ and $r = r'$. From the remainders being equal, $c_0 = c'_0$. From the quotients being equal, q has two base b representations:

$$q = c_k b^{k-1} + c_{k-1}b^{k-2} + \cdots + c_1 = c'_\ell b^{\ell-1} + c'_{\ell-1}b^{\ell-2} + \cdots + c'_1.$$

The quotient q is positive and less than n (as in the proof of the existence part), so by (strong) induction its base b representation is unique. Therefore $k-1 = \ell-1$, so $k = \ell$, and digits for corresponding powers of b match: $c_1 = c'_1, c_2 = c'_2, \ldots, c_k = c'_k$. Therefore k, the highest power of b in the base b representation of n is unique and the digits $c_0, c_1, \ldots, c_k$ in the base b representation of n are unique. □

In $F[T]$, elements automatically appear in "base T", but we can get a base representation using other nonconstant polynomials by adapting the proof from $\mathbf{Z}^+$ to the setting of $F[T]$.

Theorem 5.2. *Fix a nonconstant polynomial $b(T)$ in $F[T]$. For each nonzero $f(T)$ in $F[T]$, there is a unique way to write*

$$f(T) = c_k(T)b(T)^k + c_{k-1}(T)b(T)^{k-1} + \cdots + c_1(T)b(T) + c_0(T)$$

where $k \geq 0$ and $c_i(T)$ is 0 or $0 \leq \deg c_i \leq \deg b(T)$, with $c_k(T) \neq 0$.

Proof. First establish existence, then uniqueness. Existence is proved by strong induction on the degree of nonzero polynomials, as in the existence part of the proof of Theorem 5.1 but using division in $F[T]$ instead of in $\mathbf{Z}$. Uniqueness is proved from uniqueness of the remainder for division by $b(T)$ together with strong induction on the degree of the polynomial, as in the uniqueness part of the proof of Theorem 5.1. Details are left to the reader. □

Example 5.3. In $\mathbf{R}[T]$, let's write T^5+T^2-2 in base T^2+1. Since the base has degree 2, each "digit" is a polynomial of degree less than 2 (or the digit is 0). Dividing by T^2+1 repeatedly in the same way that we wrote 36137 in base 6 using repeated division by 6,

$$\begin{aligned} T^5+T^2-2 &= (T^2+1)(T^3-T+1)+(T-3), \\ T^3-T+1 &= (T^2+1)(T)-2T+1, \\ T &= (T^2+1)(0)+T. \end{aligned}$$

Using the remainders in reverse order, check that the "digits" of T^5+T^2-2 in base T^2+1 are T, $-2T+1$, and $T-3$:

$$T(T^2+1)^2+(-2T+1)(T^2+1)+(T-3) = T^5+T^2-2.$$

An application of polynomial base expansions in integral calculus is given in the appendix, concerning the integration of rational functions. The full scope of integration of rational functions is usually avoided in a calculus course, since the general case involves "too much algebra". One aspect of that algebra is base expansions for a polynomial base of degree 2.

Appendix A. Polynomial base expansions and integration

Polynomial base expansions appear in integral calculus to integrate rational functions with a repeated denominator. For example, if we want to determine

$$\int \frac{x^5+x^2-2}{(x^2+1)^3}\,dx,$$

where the denominator is the third power of x^2+1, then write the numerator in base x^2+1, separate terms, and simplify: from Example 5.3,

$$\frac{x^5+x^2-2}{(x^2+1)^3} = \frac{x(x^2+1)^2+(-2x+1)(x^2+1)+(x-3)}{(x^2+1)^3} = \frac{x}{x^2+1}+\frac{-2x+1}{(x^2+1)^2}+\frac{x-3}{(x^2+1)^3}.$$

On the right side each denominator is a power of x^2+1 and the numerators are the "digits" in base x^2+1: they are polynomials of degree at most 1. Split the integrand on the right side into two sums of rational functions, one having numerators equal to x and one having numerators equal to 1:

$$\int \left(\frac{x}{x^2+1}-2\frac{x}{(x^2+1)^2}+\frac{x}{(x^2+1)^3}\right)dx + \int \left(\frac{1}{(x^2+1)^2}-3\frac{1}{(x^2+1)^3}\right)dx. \tag{A.1}$$

Expansions with base x^2+1 have reduced us to evaluate the special integrals

$$I_n := \int \frac{x}{(x^2+1)^n}\,dx, \quad J_n := \int \frac{1}{(x^2+1)^n}\,dx.$$

for $n \leq 3$. The integrals I_1 and J_1 can both be found from elementary calculus: using the substitution $u = x^2+1$, so $du = 2x\,dx$,

$$I_1 = \int \frac{x}{x^2+1}\,dx = \frac{1}{2}\int \frac{du}{u} = \frac{1}{2}\log u = \frac{1}{2}\log(x^2+1)+C,$$

while

$$J_1 = \int \frac{1}{x^2+1}\,dx = \arctan x + C.$$

For $n \geq 2$, I_n can be computed with the same substitution $u = x^2 + 1$ as above:

$$I_n = \int \frac{x}{(x^2+1)^n}\,dx = \frac{1}{2}\int \frac{du}{u^n} = \frac{-1}{2(n-1)u^{n-1}} + C = \frac{-1}{2(n-1)(x^2+1)^{n-1}} + C.$$

For example,

$$I_2 = \frac{-1}{2(x^2+1)} + C, \quad I_3 = \frac{-1}{4(x^2+1)^2} + C.$$

The integrals J_n for $n \geq 2$ don't have a simple direct formula, but can be computed recursively using integration by parts. Taking $u = 1/(x^2+1)^n$ and $dv = dx$, so $du = -2nx/(x^2+1)^{n+1}$ and $v = x$,

$$J_n = \int \frac{1}{(x^2+1)^n}\,dx = \int u\,dv = uv - \int v\,du = \frac{x}{(x^2+1)^n} + 2n\int \frac{x^2}{(x^2+1)^{n+1}}\,dx.$$

In the integral on the right, write x^2 as $x^2 + 1 - 1$:

$$\int \frac{x^2}{(x^2+1)^{n+1}}\,dx = \int \frac{(x^2+1)-1}{(x^2+1)^{n+1}}\,dx = \int \frac{1}{(x^2+1)^n}\,dx - \int \frac{1}{(x^2+1)^{n+1}}\,dx = J_n - J_{n+1},$$

so

$$J_n = \frac{x}{(x^2+1)^n} + 2n(J_n - J_{n+1}) \Longrightarrow \boxed{J_{n+1} = \frac{x}{2n(x^2+1)^n} + \frac{2n-1}{2n}J_n.}$$

Armed with this recursion for J_n and the initial value $J_1 = \arctan x + C$, we get

$$\begin{aligned} J_2 &= \frac{x}{2(x^2+1)} + \frac{1}{2}\arctan x + C, \\ J_3 &= \frac{x}{4(x^2+1)^2} + \frac{3x}{8(x^2+1)} + \frac{3}{8}\arctan x + C. \end{aligned}$$

Plugging the computed values of I_1, I_2, I_3, J_1, and J_2 into (A.1),

$$\begin{aligned} \int \frac{x^5+x^2-2}{(x^2+1)^3}\,dx &= (I_1 - 2I_2 + I_3) + (J_2 - 3J_3) \\ &= \left(\frac{1}{2}\log(x^2+1) + \frac{1}{x^2+1} - \frac{1}{4(x^2+1)^2}\right) + \\ &\quad \left(\frac{x}{2(x^2+1)} + \frac{1}{2}\arctan x - \frac{3x}{4(x^2+1)^2} - \frac{9x}{8(x^2+1)} - \frac{9}{8}\arctan x\right) + C. \end{aligned}$$

Combining like terms together,

$$\begin{aligned} \int \frac{x^5+x^2-2}{(x^2+1)^3}\,dx &= \frac{1}{2}\log(x^2+1) - \frac{5}{8}\arctan x + \frac{-(5/8)x+1}{x^2+1} + \frac{-(3/4)x - 1/4}{(x^2+1)^2} + C \\ &= \frac{1}{2}\log(x^2+1) - \frac{5}{8}\arctan x - \frac{5x-8}{8(x^2+1)} - \frac{3x+1}{4(x^2+1)^2} + C. \end{aligned}$$