Lecture notes of Algebra. Week 3

7. Writing numbers in a different base

7.1. Integers, and then real numbers, written in a base b. Fix an integer $b > 1$, called *base*. Then every non-negative integer n can be written in the form

$$n = d_{k-1}b^{k-1} + d_{k-2}b^{k-2} + \cdots + d_1 b + d_0,$$

and will be denoted by $(d_{k-1} \dots d_1 d_0)_b$, where each d_i is a digit in base b, that is, a symbol for one of the integers $0, 1, \dots, b-2, b-1$. For example, if $b \leq 10$ one one can use the ordinary (decimal) $0, 1, \dots, b-1$ digits to represent themselves in base b. However, if $b > 10$ it may be convenient to use extra symbols to denote the digits having values $10, 11, \dots, b-1$. For example, when $b = 16$ (the *hexadecimal* system) it is customary to use the letters from A to F as digits with values 10 to 15.

It is neither necessary nor convenient to assume $d_{k-1} \neq 0$. If that holds then we say that n has (exactly) k digits in base b. Not assuming that allows us to identify writings such as 010 or 0010 for the number 10 in decimal notation. Allowing for that we have that the above expression for n in base b is unique, that is, each digit d_j (including the leading zeroes) depends only on n. [3]

As for base 10, this generalises from positive integers to arbitrary positive real numbers. Every positive real number n can be written as $\sum_{i<k} d_i b^i$ (with i ranging over all integers less than k, hence possibly negative) and denoted by $(d_{k-1}d_{k-2} \dots d_1 d_0, d_{-1}d_{-2} \dots)_b$, where the digits may continue indefinitely to the right. This writing is also unique, but with exceptions, occurring when all d_i starting with a certain d_j equal $b-1$; in that case we may replace d_i for $i \geq j$ with 0 (and possibly omitting it in writing) and increase d_{j-1} by one.

Remark. The number of digits in base b of a non-negative integer n is given by the formula

$$k = \lfloor \log_b n \rfloor + 1 = \left\lfloor \frac{\log n}{\log b} \right\rfloor + 1.$$

This is because $b^{k-1} \leq n < b^k$.

[3] A proof of uniqueness essentially amounts to writing up formally and more generally the familiar way in which we tell which of two different integers in base 10 is larger, by scanning the digits from left to right until we find a different digit (assuming they have the same number of digits). A proof of existence of the expression, for any positive integer n, can be obtained by writing up formally the procedure for writing and integer in an arbitrary base b, which we explain later.

7.2. Converting integers from base b to base 10. For n an integer we conveniently write the conversion as

$$n = (\dots((d_{k-1}b + d_{k-2})b + d_{k-3})b + \cdots + d_1)b + d_0.$$

This method (the same as we conveniently use to evaluate a polynomial on some number, in thic case the base b) requires only $k-1$ multiplications by b, and $k-1$ additions. It is also easy to perform on a pocket calculator (as long as that is not too smart, meaning that it should execute operations in the order in which we type them in.) For example,

$$(61405)_7 = ((6 \cdot 7 + 1) \cdot 7 + 4) \cdot 7 \cdot 7 + 5 = 14950.$$

The calculations can be conveniently arranged as follows, a special case of Ruffini's rule for polynomials (or Horner scheme, see a later section on polynomials):

	6	1	4	0	5
7		42	301	2135	14945
	6	43	305	2135	14950

7.3. Converting integers from base 10 to base b. If n is an integer, its last digit in base b, which is d_0, can be obtained as the remainder of dividing n by b, then d_1 is obtained as the remainder of dividing the previous quotient by b, etc., until we get quotient zero. For example converting $(14950)_{10}$ to base 7 can be done as follows:

$$\begin{aligned}
14950 &= 7 \cdot 2135 + 5\\
2135 &= 7 \cdot 305 + 0\\
305 &= 7 \cdot 43 + 4\\
43 &= 7 \cdot 6 + 1\\
6 &= 7 \cdot 0 + 6
\end{aligned}$$

We conclude that $(14950)_{10} = (61405)_7$.

This algorithm can be efficiently executed on a pocket calculator (which does not do divisions with remainder) if we repeatedly divide by b starting with n (without subtracting the remainders), and comparing the fractional part of each quotient with a table which we will have prepared in advance, containing $0/b, 1/b, 2/b, \dots, (b-1)/b$. The correct digit d at each stage will be found according to the rule $d/b \le f < (d+1)/b$, where f is the fractional part of the quotient. In the previous example we will have

$$\begin{aligned}
1/7&=0.142\ldots\\
2/7&=0.285\ldots\\
3/7&=0.428\ldots\\
4/7&=0.571\ldots\\
5/7&=0.714\ldots\\
6/7&=0.857\ldots
\end{aligned}$$

We will find

$$\begin{array}{r}
14950\qquad\quad .\\
2135.714\ldots\\
305.102\ldots\\
43.586\ldots\\
6.226\ldots\\
0.889\ldots
\end{array}$$

and hence

0.714	5
0.102	0
0.586	4
0.226	1
0.889	6

Note that such a table will need to be sufficiently accurate, especially if there are sequences of consecutive digits 6 in the expansion of n in base b. Also, the divisions will need to be done with a sufficient accuracy, otherwise we may find an incorrect answer, as we exemplify now.

Example. Consider the integer 16806, in decimal notation. If we perform the divisions by 7 with a precision limited to three digits after the point, we find

$$\begin{array}{r}
16806\qquad\quad .\\
2400.857\ldots\\
342.980\ldots\\
48.997\ldots\\
7.000\ldots\\
1\ldots\\
0.142\ldots
\end{array}$$

and hence

0.857	6
0.980	6
0.997	6
0.0	0
0.0	0
0.142	1

It would appear that $(16806)_{10} = (100666)_7$, but that is wrong, and the correct conclusion is $(16806)_{10} = (66666)_7$. The problem is that

$$\frac{6}{7}+\frac{6}{7^2}+\frac{6}{7^3}+\frac{6}{7^4}=0.99958307\ldots,$$

which gets approximated to 1 if we only use three digits after the point (In other words, the 7.000 appearing in the penultimate row of the above calculation should really be a little less than 7. Unfortunately, this may produce a large error in the final result: in this case an error of $(1000)_7 = 7^3$.)

Remark. We have used two different methods to convert from base b to base 10, and from base 10 to base b (inverse to each other: *multiplying* in the former case, and *dividing* in the latter). By symmetry, each of those methods would also work for the other task, but it would involve doing the relevant calculations in base b rather than in base 10. Of course if $b = 2$ and the conversions are to be done by a computer working in base 2, rather than by a human, the two algorithms would be exchanged.

Remark. Converting from *binary* (base 2) to *hexadecimal* (base 16, where the customary symbols for the digits are $0, 1, \ldots, 9, A, B, C, D, E, F$), and from hexadecimal to binary, will be much simpler than described above. For example, to convert from binary to hexadecimal it will be sufficient to split the bits into blocks of four starting from the decimal points, and then convert each block into the corresponding hexadecimal digit.

7.4. Converting real numbers from base b to base 10. Consider a positive number written in base b with a finite number h of digits after the point. To convert it to decimal one may use the same procedure as for an integer, but continuing with the digits (in base b) after the point, up to the last digit d_{-h}, and then divide the result by b^h. (This is because ignoring the point amounts to multiplying our number by b^h.)

Example. To convert $(14.22)_5$ to decimal, remove the point (which means multiplying by 5^2), convert $(1422)_5 = 237$, and then divide by 5^2: $\quad (14.22)_5 = 237/25 = 9.48$.

Note that until just before this last step you work with integer numbers, thus avoiding approximation errors. In fact, because of the final division the decimal expansion of the number may have infinitely many digits, even though you started with finitely many digits in base b. This cannot occur if $b = 2$ or 5 or, more generally, if the base b has only 2 and 5 as prime factors. (See a later subsection about periodic numbers.)

Example. We have $(1.22)_3 = (122)_3/3^2 = 17/9 = 5.222\cdots = 5.\dot{2}$.

If the number to be converted has infinitely many digits, one can do the same with an approximation (keeping a few digits after the point).

Example. To convert $(2.\dot{1})_3 = (2.11111\cdots)_3$ into decimal, we may convert the approximation $(2.111)_3 = (2111)_3/27 = 67/27$, which equals $2 + \frac{13}{27} = 2.\dot{4}8\dot{1}$, so roughly 2.48. In this case we can actually convert it exactly, namely $(2.\dot{1})_3 = 2.5$, because $(2.\dot{1})_3 \cdot 2 = (11.\dot{2})_3 = (12)_3 = 5$. More generally, if the number is periodic (written in any base) then it is rational and there is a rule to convert it into a fraction of integers, see a later subsection.

7.5. Converting real numbers from base 10 to base b. If n is not an integer we can deal separately with the integer part and the fractional part. In fact, multiplying the latter by b and taking the integer part of the result we get d_{-1}; then we may repeat this procedure with the fractional part of the result and find d_{-2}, etc.

EXAMPLE. To convert 2.481 to base 3, write it as $2 + 0.481$.

- $0.481 \cdot 3 = 1.443$, so first digit after the point will be 1;
- $0.443 \cdot 3 = 1.329$, so second digit after the point will be 1;
- $0.329 \cdot 3 = 0.987$, so third digit after the point will be 0;
- $0.987 \cdot 3 = 2.961$, so fourth digit after the point will be 2;
- $0.961 \cdot 3 = 2.883$, so fifth digit after the point will be 2; and so on.
- In conclusion, $2.481 = (2.11022\cdots)_3$.

This can be conveniently done on a simple pocket calculator, and we can also avoid subtracting the integral part at each step by using a trick which we have seen before, and requires a preliminary table with (at least approximate) decimal expansions of $1/b, 2/b, \ldots (b-1)/b$. In this case we have $1/3 = 0.\dot{3}$ and $2/3 = 0.\dot{6}$. We proceed as before, but reading each digit off the fractional part (rather than from the integral part) *before* multiplying by b, hence subtracting the integral part becomes unnecessary.

Hence to convert 2.481 to base 3, write it as $2 + 0.481$. Then

- because $\dot{3} \le 0.481 < \dot{6}$, the first digit after the point will be 1;
- $0.481 \cdot 3 = 1.443$, and as $\dot{3} \le 0.443 < \dot{6}$ the second digit after the point will be 1;
- $1.443 \cdot 3 = 4.329$, and as $0.329 < \dot{3}$ the third digit after the point will be 0;
- $4.329 \cdot 3 = 12.987$, and as $\dot{6} \le 0.987$ the fourth digit after the point will be 2;
- $12.987 \cdot 3 = 38.961$, and as $\dot{6} \le 0.961$ the fifth digit after the point will be 2;
- $38.961 \cdot 3 = 116.883$, and as $\dot{6} \le 0.883$ the sixth digit after the point will be 2; and so on.
- In conclusion, we find $2.481 = (2.110222\cdots)_3$.

EXAMPLE. Converting the number π to base 2 we will find:

$$(3,1415926\ldots)_{10} = (11,00100100001111110\ldots)_2.$$

Please check that yourself, starting with as many decimal digits of π as they fit on your calculator, and proceeding like in the previous example, comparing the fractional part with $1/2 = 0.5$ after each multiplication by 2.

8. Arithmetic and geometric progressions

A finite sequence $a_1, a_2, \ldots, a_n$ of (real or) complex numbers is called an *arithmetic progression* if the difference $d = a_{k+1} - a_k$ between each two consecutive terms is constant, meaning that it is independent of k. We could also write this condition as $a_{k+1} - a_k = a_k - a_{k-1}$ for all k (to which this applies, that is, $1 < k < n$), or, equivalently, $a_{k+1} + a_{k-1} = 2a_k$.

Hence a sequence is an arithmetic progression precisely when each term is the average, or arithmetic mean, of the preceding and the following term. [4]

For an arithmetic progression we have

$$a_n = a_1 + d(n-1).$$

The sum of an arithmetic progression, also called an *arithmetic series* $a_1 + a_2 + \cdots + a_n$, can be computed as follows:

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n = \frac{(a_1 + a_n) \cdot n}{2}.$$

This can be shown by noting that any two terms which have the same distance from both ends have the same sum $a_k + a_{n-k+1} = \big(a_1 + d(k-1)\big) + \big(a_1 + d(n-k)\big) = 2a_1 + d(n-1) = a_1 + a_n$, and hence

$$\begin{aligned} 2(a_1 + a_2 + \cdots + a_n) = &\quad (a_1 + a_2 + \cdots \qquad + a_n) \\ &+ (a_n + a_{n-1} + \cdots \quad + a_1) \\ = &\ (a_1 + a_n) \cdot n. \end{aligned}$$

Because the indices of an arithmetic progression may cover a different range, for example $a_3, a_4, \ldots, a_9$, the formula for the sum is best remembered as *the sum of the first and last term, times the total number of terms, divided by two.* (Or, equivalently, *the arithmetic mean (or average) of the first and last term, times the total number of terms.*) More generally, an arithmetic progression may have infinite terms. In fact, any finite arithmetic progression with at least two terms can be extended, on either side, to form an infinite arithmetic progression, in a unique way.

Geometric progressions are analogous to arithmetic progressions, except that sums and differences are replaced by products and quotients (ratios). Hence a finite sequence $a_1, a_2, \ldots, a_n$, made of nonzero numbers, is called a *geometric progression* if the ratio $r = a_{k+1}/a_k$ between each two consecutive terms is constant. Note that the ratio r is nonzero, but may possibly be negative, in which case the terms of the progression have alternating signs. Similarly as for arithmetic progressions, a sequence is a geometric progression precisely when $a_{k+1} \cdot a_{k-1} = a_k^2$ for all k which make sense, that is to say, when each term is the geometric mean of the preceding and the following term.

For a geometric progression we have

$$a_n = a_1 \cdot r^{n-1}.$$

[4] A sequence satisfying $a_{k+1} + a_{k-1} \geq 2a_k$ for all k is usually called *convex,* and *strictly convex* if $a_{k+1} + a_{k-1} > 2a_k$ for all k. Similarly, a sequence satisfying $a_{k+1} + a_{k-1} \leq 2a_k$ for all k is usually called *concave.* You may relate this to Calculus notions if you note that $a_{k+1} - 2a_k + a_{k-1}$ is a discrete analogue of the ‘second derivative’ of a function (and here a_k is a function of the discrete variable k).

In a finite geometric progressions, any two terms which have the same distance from both ends have the same product. Hence, arguing in a similar way as for the sum of an arithmetic progression we see that the product of all terms of a geometric progression, say made of positive real numbers for simplicity, is given by

$$\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdots a_n = \sqrt{(a_1 a_n)^n}.$$

This can also be thought of as *the n-th power* of the *geometric mean* $\sqrt{a_1 a_n}$ of the first and last terms.

One may also consider the sum of a geometric progression, also called a *geometric series*. If $a_1, a_2, \ldots, a_n$ is a geometric progression with (common) ratio r, then

$$a_1 + a_2 + a_3 + \cdots + a_n = a_1(1 + r + r^2 + \cdots + r^{n-1}) = a_1 \frac{r^n - 1}{r - 1} = a_1 \frac{1 - r^n}{1 - r}.$$

This can also be used to compute the sum of an infinite geometric progression $a_1, a_2, \ldots$ (continuing indefinitely to the right). The corresponding geometric series converges (see the Calculus module for the meaning of this) exactly when r^n tends to zero as n tends to $+\infty$, which occurs exactly when $|r| < 1$. In that case the sum of the series is given by

$$a_1 + a_2 + a_3 + \cdots = a_1(1 + r + r^2 + r^3 + \cdots) = \frac{a_1}{1 - r}.$$

Remark (Optional: Arithmetic, geometric, and harmonic mean). We mentioned above the *arithmetic mean* $(a+b)/2$ of two numbers, and the *geometric mean* $\sqrt{ab}$ of two *positive real* numbers. Note that the geometric mean never exceeds the arithmetic mean, that is, $\sqrt{ab} \leq (a+b)/2$ for all positive real numbers a, b. In fact, because both sides are positive this inequality is equivalent to $ab \leq (a+b)^2/4$. In turn, this is equivalent to $0 \leq (a+b)^2 - 4ab$, that is, $0 \leq (a-b)^2$, which is certainly true for all positive real numbers a, b. A third type of mean occurs in some applications, the *harmonic mean* $\frac{1}{\frac{1}{2}(\frac{1}{a}+\frac{1}{b})} = \frac{2ab}{a+b}$. The harmonic mean of two positive real numbers a, b never exceeds their geometric mean (similar proof), and so we have

$$\frac{2ab}{a+b} \leq \sqrt{ab} \leq \frac{a+b}{2},$$

that is, [harmonic mean]$\leq$[geometric mean]$\leq$[arithmetic mean]. Note that the product of the arithmetic mean and the harmonic mean equals the square of the geometric mean; this is another (but equivalent) explanation of why the geometric mean takes an intermediate value between the other two means.

9. Periodic numbers (in decimal notation or any other base)

Example. Converting a real number with periodic decimal expansion into a fraction:

$$0.171717\cdots = 0.\overline{17} = 0.17 \cdot 1.\overline{01} = 0.17 \cdot \big(1 + (0.01) + (0.01)^2 + \cdots\big) = \frac{0.17}{1 - 0.01} = \frac{17}{99}.$$

It is easy to discover how to extend this to the most general situation of a *periodic decimal expansion* (also called a *repeated* or *recurring decimal,* for which various notations are in use) with both an *integer part* and a *pre-period*:

$$1234.56789789789\cdots = 1234.56\overline{789} = 1234.56\dot{7}8\dot{9} = \frac{123456789 - 123456}{99900}.$$

The numerator of the fraction equals

$$\text{[integer part|pre-period|period]} \quad \text{minus} \quad \text{[integer part|pre-period]},$$

ignoring the decimal dot; the denominator has as many 9s as the number of digits of the period, followed by as many 0s as the digits of the pre-period.

The procedure explained in the example shows that a real number whose decimal expansion is periodic, is actually a rational number (a fraction of integers). Obviously, a real number whose decimal expansion is finite is also a rational number. (This may actually be viewed as a special case of a periodic expansion where the period is $\dot{0}$, and the procedure for converting it to a fraction still works...) More is true: *a real number has finite or periodic decimal expansion if and only if it is rational.* We have just seen the 'only if' implication, that is, the '$\Rightarrow$' implication. To prove the opposite implication, note that when computing the decimal expansion of a rational number m/n (hence with m and n integers), that is, when performing the ordinary school division algorithm (similar to long division for polynomials), at each step at most n remainders r are possible (as $0 \leq r < n$). Once we have finished 'carrying down' all the digits from m (so the following ones would all be zeroes, which we usually do not write), sooner or later one of the remainders will have to repeat, and from that point on a whole bunch of steps of the division algorithm will have to repeat periodically. It is easier to see what happens by working out an example than explaining it in words, but it follows that the resulting decimal expansion must be periodic.

The same procedure would work in any base b, just replace the digits 9 used in the rule with the digit $b-1$. However, beware that those numbers you are writing as numerator and denominator of the fraction will be in base b, so you may then need to convert them to decimal in order to write the fraction in the ordinary way. For example,

$$(3.\dot{2}\dot{1})_7 = \frac{(321)_7 - (3)_7}{(66)_7} = \frac{(315)_7}{(66)_7} = \frac{159}{48}.$$

Note that some fractions of integers may have a finite expansion when written in some base, and a periodic infinite expansion when written in some other base:

$$\frac{1}{2} = 0.5 = (0.1)_2 = (0.\dot{1})_3 = (0.2)_4 = (0.\dot{2})_5 = (0.3)_6 = (0.\dot{3})_7 = \cdots$$

$$\frac{1}{3} = 0.\dot{3} = (0.\dot{0}\dot{1})_2 = (0.1)_3 = (0.\dot{1})_4 = (0.\dot{1}\dot{3})_5 = (0.2)_6 = \cdots$$

10. Polynomials

In this and the following sections we will consider polynomials with coefficients in a *field* F. Some examples of fields are $\mathbb{Q}$ (the field of rational numbers), $\mathbb{R}$ (the field of real numbers), $\mathbb{C}$ (the field of complex numbers). These fields satisfy $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, but later we will discover some other interesting and unrelated fields. Most of what we do with polynomials in the following section does not really depend on which field we use (unless we state that explicitly), and so you may take F to be some field which is familiar to you, say $\mathbb{Q}$ or $\mathbb{R}$, and worry only later about the proper definition of an arbitrary field. Very roughly, a field is a set of 'numbers' which you can add, subtract, and multiply arbitrarily, and also divide except for dividing by zero, and where those operations satisfy the familiar calculation 'rules,' such as $a - (b - c) = a - b + c$, $ab = ba$, $a(b + c) = ab + ac$, etc.

Example. The set of integers $\mathbb{Z}$ is not a field, because division cannot be done arbitrarily: $2/3$ is not an integer. One can of course consider polynomials with integer coefficients (being special rational numbers), but the theorems which we will see may not be true, and the algorithms may not work, unless we accept to use rational numbers, which are a field.

Example. There are many different fields, and even some with a finite number of elements. The simplest example is the field with two elements, usually denoted by $\mathbb{F}_2$. (Later in the module we will learn about the field $\mathbb{F}_p$ of p elements, where p is any prime.) Its elements are two symbols $\bar{0}$ and $\bar{1}$, which add and multiply exactly as the integers 0 and 1 do, except that $\bar{1} + \bar{1} = \bar{0}$. Here are the full addition and multiplication tables in $\mathbb{F}_2$:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

One can verify that $\mathbb{F}_2$ satisfies the definition of a field (which we have not explicitly given but roughly amounts to saying that the usual properties of addition, subtraction, multiplication and division hold).

For the moment, we may think of a polynomial (in the single *indeterminate* x) as an expression of the form $f(x) = a_n x^n + \cdots + a_1 x + a_0$. (Arranging them in the opposite order is just another convention in use.) The notation $f(x)$ is borrowed from Calculus to stress that one may think of the polynomial as a special type of function of the "variable" x, while $a_0, a_1, \ldots, a_n$ are to be thought of as "constants" (even though in some applications they may themselves be expressions depending on parameters, other than x). Strictly speaking, a function of this type should be called *a polynomial function,* rather than *a* *polynomial.* Thinking of polynomials as functions is OK as long as one works with real coefficients, but is not quite the best in view of generalizations.

Thus, a polynomial with coefficients in the field F is an expression of the form $f(x) = a_nx^n + \cdots + a_1x + a_0$ with $a_0, \ldots, a_n \in F$, for some n. If β is any element of F, we may *evaluate* $f(x)$ *on* β*, or for* $x = \beta$*,* and compute the value $f(\beta) = a_n\beta^n + \cdots + a_1\beta + a_0$.

Definition 19. The degree of a non-zero polynomial $f(x)$ is the largest integer n such that $a_n \neq 0$, and is denoted by $n = \deg(f)$.

The coefficient a_n in the definition is called *the leading coefficient*, and if $a_n = 1$ then $f(x)$ is said to be *monic*. We also call a_nx^n *the leading term* of the polynomial, and a_0 *the constant term*. We do not assign a degree to the zero polynomial. (In our notation $f(x) = a_nx^n + \cdots + a_1x + a_0$ we have not assumed that $a_n \neq 0$. This is actually convenient, and all that notation tells us is that $\deg(f(x)) \leq n$, or $f(x)$ might possibly be the zero polynomial.)

The sum of two polynomials is given by

$$(a_nx^n + \cdots + a_1x + a_0) + (b_nx^n + \cdots + b_1x + b_0) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

Note that the two polynomials need not have the same degree, and to make this formula simpler we have taken advantage of the possibility of adding zero coefficients in front of one of them to make both polynomials formally start with the same x^n.

The product of two polynomials can be computed by removing the parentheses using the distributive law, and then collecting like powers of x. Hence

$$\begin{aligned}(a_nx^n + &\cdots + a_1x + a_0) \cdot (b_mx^m + \cdots + b_1x + b_0) \\ &= a_nb_mx^{n+m} + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} + \cdots \\ &\qquad \cdots + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_1 + a_1b_0)x + a_0b_0.\end{aligned}$$

Those two formulas show that the degrees of a sum and of a product of polynomial satisfy

$$\deg\bigl(f(x) + g(x)\bigr) \leq \max\bigl(\deg(f(x)), \deg(g(x))\bigr),$$

and

$$\deg\bigl(f(x) \cdot g(x)\bigr) = \deg\bigl(f(x)\bigr) + \deg\bigl(g(x)\bigr),$$

provided that all degrees make sense, that is, unless one of the polynomials involved is the zero polynomial.

11. Polynomial division with remainder

Theorem 20 (Division Algorithm for $F[x]$). *Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

where

$$\textit{either} \quad r(x) = 0 \quad \textit{or} \quad \deg\bigl(r(x)\bigr) < \deg\bigl(g(x)\bigr).$$

The polynomials $q(x)$ and $r(x)$ are called the *quotient* and the *remainder* of the division of $f(x)$ by $g(x)$.

Remark (The degree of the zero polynomial). An alternate convention is to assign a degree to the zero polynomial as well. To make things work properly, however, the zero polynomial should be assigned some negative number, say -1. Doing so, the condition

$$\text{either} \quad r(x) = 0 \quad \text{or} \quad \deg\bigl(r(x)\bigr) < \deg\bigl(g(x)\bigr)$$

in Theorem 20 can be rephrased, more simply, as

$$\deg\bigl(r(x)\bigr) < \deg\bigl(g(x)\bigr).$$

An even better convention is assigning the symbol $-\infty$ to the zero polynomial, which makes the properties given above on the degrees of a sum and a product remain true even if one of the polynomials involved is the zero polynomial (with some natural interpretations such as $(-\infty) + 3 = -\infty$, or $(-\infty) + (-\infty) = -\infty$).

We omit the proof of Theorem 20, which is just a bit tedious to write down formally. However, a proof of the *existence* of $q(x)$ and $r(x)$ is just a formal transcription of what the actual algorithm does, as illustrated in the following example.

Example. In $\mathbb{Q}[x]$, divide $f(x) = 2x^4 + x^2 - x + 1$ by $g(x) = 2x - 1$ with remainder.

$$\begin{array}{r|rrrrrrrrr}
 & x^3 & + & \frac{1}{2}x^2 & + & \frac{3}{4}x & - & \frac{1}{8} & & \\ \cline{2-10}
2x-1 & 2x^4 & + & 0x^3 & + & x^2 & - & x & + & 1 \\
 & 2x^4 & - & x^3 & & & & & & \\ \cline{2-4}
 & & & x^3 & + & x^2 & & & & \\
 & & & x^3 & - & \frac{1}{2}x^2 & & & & \\ \cline{4-6}
 & & & & & \frac{3}{2}x^2 & - & x & & \\
 & & & & & \frac{3}{2}x^2 & - & \frac{3}{4}x & & \\ \cline{6-8}
 & & & & & & - & \frac{1}{4}x & + & 1 \\
 & & & & & & - & \frac{1}{4}x & + & \frac{1}{8} \\ \cline{7-10}
 & & & & & & & & & \frac{7}{8}
\end{array}$$

Therefore, we have $q(x) = x^3 + \frac{1}{2}x^2 + \frac{3}{4}x - \frac{1}{8}$ and $r(x) = \frac{7}{8}$. Another perfectly acceptable (and perhaps even preferable) answer is

$$2x^4 + x^2 - x + 1 = (2x - 1) \cdot \left(x^3 + \frac{1}{2}x^2 + \frac{3}{4}x - \frac{1}{8}\right) + \frac{7}{8}.$$

Note that the algorithm stops as soon as we obtain a *remainder* which is zero or has degree less than the degree of $g(x)$, as stated in Theorem 20. For example, if we stopped two steps too early (omitting the last four lines) we would obtain that $f(x) = g(x)q_1(x) + r_1(x)$ with $q_1(x) = x^3 + \frac{1}{2}x^2$ and $r_1(x) = \frac{3}{2}x^2 - x + 1$, which is a true equality, but those are not the correct quotient and remainder because $\deg\big(r_1(x)\big) = 2$ is not less than $\deg(2x-1) = 1$, and $r_1(x)$ is not zero either.

Note that, although the two original polynomials in the above example had integer coefficients, we had to use rational numbers in the course of the calculation, and also to express the final result. That example shows that division with remainder of polynomials in $\mathbb{Z}[x]$ would simply not work, and the reason is that $\mathbb{Z}$ is not a field (as we cannot divide arbitrarily by non-zero integers). Division of polynomials with integer coefficients does work in a restricted situation, namely when the polynomial we are dividing by is monic (that is, it has leading coefficient 1), as in the next example.

Example. In $\mathbb{Q}[x]$, divide $f(x) = 2x^4 - x^3 + 3x^2 + x - 2$ by $g(x) = x^2 - 2x + 2$ with remainder.

$$\begin{array}{r|ccccccccc}
\multicolumn{1}{r}{} & 2x^2 & + & 3x & + & 5 & & & & \\ \cline{2-10}
x^2 - 2x + 2 & 2x^4 & - & x^3 & + & 3x^2 & + & x & - & 2 \\
\multicolumn{1}{r}{} & 2x^4 & - & 4x^3 & + & 4x^2 & & & & \\ \cline{2-6}
\multicolumn{1}{r}{} & & & 3x^3 & - & x^2 & + & x & & \\
\multicolumn{1}{r}{} & & & 3x^3 & - & 6x^2 & + & 6x & & \\ \cline{4-8}
\multicolumn{1}{r}{} & & & & & 5x^2 & - & 5x & - & 2 \\
\multicolumn{1}{r}{} & & & & & 5x^2 & - & 10x & + & 10 \\ \cline{6-10}
\multicolumn{1}{r}{} & & & & & & & 5x & - & 12
\end{array}$$

Therefore $q(x) = 2x^2 + 3x + 5$ and $r(x) = 5x - 12$. Or, more explicitly,

$$2x^4 + -x^3 + 3x^2 + x - 2 = (x^2 - 2x + 2) \cdot (2x^2 + 3x + 5) + (5x - 12).$$

A proof of the *uniqueness* of $q(x)$ and $r(x)$ in Theorem 20 is easier to write down formally than a proof of their existence.

Proof of uniqueness of $q(x)$ and $r(x)$ in Theorem 20. Suppose that the division can be done in two ways,

$$f(x) = g(x)q(x) + r(x) \qquad \text{and} \qquad f(x) = g(x)q_1(x) + r_1(x),$$

with both $r(x)$ and $r_1(x)$ satisfying the required condition. Then we claim that $q_1(x) = q(x)$ and $r_1(x) = r(x)$. In fact, putting together the two equalities we obtain

$$g(x)q(x) + r(x) = f(x) = g(x)q_1(x) + r_1(x),$$

and hence

$$g(x)[q_1(x) - q(x)] = r(x) - r_1(x).$$

If the right-hand side were different from zero, then its degree would be less than the degree of $g(x)$. However, the left-hand side, if nonzero, would have degree $\deg(g(x)) + \deg[q_1(x) - q(x)] \geq \deg(g(x))$. This is impossible, and so we have to conclude that each side of the equality is zero. This implies that $r_1(x) = r(x)$, and $q_1(x) = q(x)$ (because $g(x)$ is not the zero polynomial), as we wanted to prove. □

Remark 21. Although division with remainder for polynomials is conceptually very similar to division with remainder for integers, with polynomials we have no analogue of the variant of division with $-b/2 < r \leq b/2$: there is only one way to do division with remainder for polynomials.