Definition 1. *A* polynomial in x over $\mathbb{R}$ *(or, more briefly, a* polynomial*) is an expression of the form*

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

where $a_0, a_1, \ldots, a_n \in \mathbb{R}$. We may change the order of the terms, and omit the terms where $a_i = 0$. The numbers $a_0, a_1, \ldots, a_n$ are called the coefficients*.*

The set of all such polynomials is denoted by $\mathbb{R}[x]$.

Definition 2. *The* degree *of the term a_ix^i is i. The degree of the polynomial $a_0 + a_1x + \cdots + a_nx^n$ is the greatest i such that $a_i \neq 0$. If there is no such i (i.e. $a(x) = 0$), then the degree is $-\infty$. We denote the degree of $a(x)$ by $\deg a(x)$.*

We can also consider polynomials over other sets of numbers, such as $\mathbb{Z}[x]$ (polynomials with integer coefficients), $\mathbb{Q}[x]$ (polynomials with rational coefficients) and so on.

We usually just think of a polynomial over $\mathbb{R}$ as being a function from $\mathbb{R}$ to $\mathbb{R}$. However, we must be careful when considering polynomials over $\mathbb{Z}_n$: there are infinitely many polynomials, and only finitely many functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, so sometimes different polynomials give the same function. For example, we have $\bar{a}^n - \bar{a} = 0$ for all $\bar{a} \in \mathbb{Z}_n$, but the polynomials $x^n - x$ and 0 are not equal.

Addition of polynomials

Now that we have our set $\mathbb{R}[x]$, we will define operations of addition and multiplication on $\mathbb{R}[x]$. First, we consider addition. To add together two polynomials, we just collect together the terms with the same degree. In other words, we have

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

If the two polynomials had different degrees, we have to "padd out" the one with the lower degree with terms $0x^i$. To put this another way, we have

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m) = c_0 + c_1x + \cdots + c_Nx^N,$$

where $N = \max(n, m)$, and for $0 \leq k \leq N$ we have $c_k = a_i + b_i$. [In this definition, if $i > n$ then $a_i = 0$ and if $i > m$ then $b_i = 0$.]

Problem 3. *Suppose $a(x)$ and $b(x)$ are polynomials of degree n and m respectively. What is the degree of $a(x) + b(x)$?*

Multiplication of polynomials

What happens when we multiply together the polynomials $a_0 + a_1x$ and $b_0 + b_1x + b_2x^2$? If we multiply out the brackets and collect terms together we get

$$\begin{aligned}(a_0 + a_1x)(b_0 + b_1x + b_2x^2) &= a_0b_0 + a_0b_1x + a_0b_2x^2 + a_1b_0x + a_1b_1x^2 + a_1b_2x^3 \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1)x^2 + a_1b_2x^3\end{aligned}$$

In general, we have

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m},$$

where for $0 \leq k \leq n+m$, $c_k = \sum_{i=0}^{k} a_ib_{k-i}$. [As before, we take $a_i = b_j = 0$ for any $i > n$, $j > m$.]

Problem 4. *Suppose $a(x)$ and $b(x)$ are polynomials of degree n and m respectively. What is the degree of $a(x)b(x)$?*

Multiplication in $\mathbb{R}[x]$ is rather like multiplication in $\mathbb{Z}$. As in $\mathbb{Z}$, we define a notion of "divisibility": we write $a(x) \mid b(x)$ if there is some $c(x)$ such that $b(x) = a(x)c(x)$. Like $\mathbb{Z}$, and unlike $\mathbb{N}$, this relation in **not** antisymmetric. In $\mathbb{Z}$ we have that if $a \mid b$ and $b \mid a$ then $a = \pm b$. In $\mathbb{R}[x]$, we have that if $a(x) \mid b(x)$ and $b(x) \mid a(x)$ then $a(x) = cb(x)$ for some $c \neq 0$.

The Division Algorithm in $\mathbb{R}[x]$

The structure $\mathbb{R}[x]$ is, in many ways, like $\mathbb{Z}$. Particularly interesting is that we have a result similar to the Division Algorithm in $\mathbb{Z}$. Roughly speaking, it says that we can divide a non-zero polynomial $b(x)$ into a polynomial $a(x)$, and get a smaller remainder. In the Divison Algorithm in $\mathbb{Z}$, we write $a = qb + r$, where $0 \leq r < b$. In $\mathbb{R}[x]$, the sensible meaning for "$r(x) < b(x)$" is that the degree of $r(x)$ is less than the degree of $b(x)$.

Theorem 5 (The Division Algorithm for $\mathbb{R}[x]$). *Let $a(x), b(x) \in \mathbb{R}[x]$ with $b(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ with $\deg r(x) < \deg b(x)$ such that*

$$a(x) = q(x)b(x) + r(x).$$

We won't actually prove this result here. If we were going to prove it, we would us induction on the degree of $a(x)$. Instead, we will illustrate how the result works with an example.

Example 6. *Find polynomials $q(x)$ and $r(x)$ with $\deg r(x) < 2$ such that*

$$x^4 + 5x^3 - 3x^2 + x + 2 = q(x)(x^2 + 3x + 5) + r(x)$$

Solution. We use "long division", just as we used to do division of integers before we had calculators:

$$
\begin{array}{rrrrrrr}
 & & x^2 & +2x & -14 & & \\
\cline{3-7}
x^2+3x+5 &) & x^4 & +5x^3 & -3x^2 & +x & +2 \\
 & & x^4 & +3x^3 & +5x^2 & & \\
\cline{2-5}
 & & & 2x^3 & -8x^2 & +x & \\
 & & & 2x^3 & +6x^2 & +10x & \\
\cline{4-6}
 & & & & -14x^2 & -9x & +2 \\
 & & & & -14x^2 & -42x & -70 \\
\cline{5-7}
 & & & & & 33x & +72
\end{array}
$$

From this we see that $x^4 + 5x^3 - 3x^2 + x + 2 = (x^2 + 2x - 14)(x^2 + 3x + 5) + (33x + 72)$. □

The Euclidean Algorithm in $\mathbb{R}[x]$

In $\mathbb{Z}$ we use the Euclidean Algorithm to find greatest common divisors. What makes this possible is the Division Algorithm.

Since we also have the Division Algorithm in $\mathbb{R}[x]$, we can use a similar process to find greatest common divisors in $\mathbb{R}[x]$.

Example 7. *Find the greatest common divisor of* $a(x) = 2x^3+x^2-2x-1$ *and* $b(x) = x^3-x^2+2x-2$.

Solution. We use the Euclidean Algorithm: first divide $b(x)$ into $a(x)$, then divide the remainder into $b(x)$, then divide this new remainder into the first one, and so on. The last non-zero remainder is the greatest common divisor.

We have

$$
\begin{aligned}
2x^3 + x^2 - 2x - 1 &= 2(x^3 - x^2 + 2x - 2) + (3x^2 - 6x + 3) \\
x^3 - x^2 + 2x - 2 &= (\tfrac{1}{3}x + \tfrac{1}{3})(3x^2 - 6x + 3) + (3x - 3) \\
3x^2 - 6x + 3 &= (x - 1)(3x - 3)
\end{aligned}
$$

So the last non-zero remainder is $d(x) = 3x - 3$. □

Theorem 8 (The Factor Theorem). *Let* $p(x) \in \mathbb{R}[x]$, *and let* $a \in \mathbb{R}$. *Then* $(x - a) \mid p(x)$ *if and only if* $p(a) = 0$.

Proof. Suppose first that $(x - a) \mid p(x)$. Then there is some $q(x)$ such that $p(x) = q(x)(x - a)$. But then $p(a) = q(a)(a - a) = 0$.

Conversely, suppose that $p(a) = 0$. By the Division Algorithm in $\mathbb{R}[x]$, we can find polynomials $q(x)$ and $r(x)$ with $\deg r(x) < 1$ such that $p(x) = q(x)(x - a) + r(x)$. Now, since $\deg r(x) < 1$, $r(x)$ is a constant. Also, we have $p(a) = q(a)(a - a) + r(a)$, in other words $0 = q(a) \cdot 0 + r(a)$, so $r(a) = 0$. Hence $r(x) = 0$, so we have $p(x) = q(x)(x - a)$, so $(x - a) \mid p(x)$. □

Irreducible polynomials in $\mathbb{R}[x]$

Definition 9. *A polynomial $p(x) \in \mathbb{R}[x]$ is* reducible *in $\mathbb{R}[x]$ if it can be factorised as $p(x) = a(x)b(x)$, where $a(x), b(x) \in \mathbb{R}[x]$ with $\deg a(x) < \deg p(x)$ and $\deg b(x) < \deg p(x)$. It is* irreducible *in $\mathbb{R}$ if it is not reducible in $\mathbb{R}[x]$.*

When we say that a polynomial is irreducible, we must specify over what field of coefficients. For example, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but it can be factorised as $(x - i)(x + i)$ in $\mathbb{C}[x]$.

Problem 10. *Show that every linear polynomial $ax + b$ (with $a \neq 0$) is irreducible.*

The irreducible polynomials in $\mathbb{R}[x]$ play the same rôle in $\mathbb{R}[x]$ that the primes play in $\mathbb{Z}$: every polynomial of degree greater than 0 can be written as a product of (one or more) irreducible polynomials. Moreover, as with uniqueness of prime factorisations in $\mathbb{Z}$, the factorisation of a polynomial as a product of irreducibles is unique (up to the order of the elements, and multiplication by constants).