Monday: Polynomials

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

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n$$

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. *The* degree *of the term $a_i x^i$ is i. The degree of the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ 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

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

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

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_m x^m) = c_0 + c_1 x + \cdots + c_N x^N,$$

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 $b_i = 0$.]

Exercise 1. *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 $a_0 + a_1 x$ and $b_0 + b_1 x + b_2 x^2$? If we multiply out the brackets and collect terms together we get

$$\begin{aligned}(a_0 + a_1 x)(b_0 + b_1 x + b_2 x^2) &= a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + a_1 b_0 x + a_1 b_1 x^2 + a_1 b_2 x^3 \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1)x^2 + a_1 b_2 x^3\end{aligned}$$

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 $i > n$, $j > m$.]

Exercise 2. *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 3 (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 4. *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:

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

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

Tuesday: 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 5. *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 6 (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. *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 $\mathbb{C}[x]$.

Exercise 7. *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).

Thursday: Groups

Definition. *Let* $*$ *be a binary operation on a set* A *with identity element* e*. Let* $a \in A$*. Then* b *is an* inverse *of* a *if* $a * b = b * a = e$*.*

Example 8. *The inverse of a real number x under the operation $+$ is the number $-x$: we have $x+(-x) = (-x)+x = 0$.*

Definition. *A* group *is a pair $(G, *)$ where $*$ is a binary operation on G such that*

- *for any $a, b, c \in G$, $a*(b*c) = (a*b)*c$;*
- *there is some $e \in G$ such that, for every $a \in G$, $a*e = e*a = a$; and*
- *for any $a \in G$ there is some $b \in G$ with $a*b = b*a = e$.*

We often abuse notation and refer to "the group G" instead of "the group $(G, *)$".

Example 9. *The integers form a group under addition, in other words $(\mathbb{Z}, +)$ is a group. The non-zero real numbers for a group under multiplication, in other words $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.*

Proposition 10. *The inverse of a is unique. In other words, if $a*b = b*a = e$ and $a*c = c*a = e$ then $b = c$.*

Because of this uniqueness, we can denote the inverse of an element a by a^{-1}.

Proposition 11. *If $(G, *)$ is a group and $a, b, c \in G$ with $a*b = a*c$ then $b = c$.*

This is sometimes called the *cancellation law*.

Cayley tables

If $*$ is a binary operation on a finite set, we can write down a "multiplication table" for $*$. For example, we can define an operation $*$ on the set $G = \{e, a, b, c\}$ by the following table:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We call this the *Cayley table* of the operation.

Exercise 12. *Show that if $*$ is defined by the above table then $(G, *)$ is a group.*

Proposition 13. *Each element of G occurs exactly once in each row and each column of the Cayley table of a group operation.*

Proposition 14. *Let $(G, *)$ be a group with identity element e.*

1. *If $x \in G$ satisfies $x*x = x$, then $x = e$.*
2. *If $x, y \in G$ satisfy $x*y = y$, then $x = e$. [Put another way, if $x*y = y$ for* some *$y \in G$ then $x*y = y$ for* every *$y \in G$.]*

Exercise 15. *Given that $\oplus$ is a group operation on the set $G = \{p, q, r, s\}$, complete the following Cayley table:*

$\oplus$	p	q	r	s
p	r			
q		q		
r				
s				

Symmetry Groups

In this section we will discuss a very important class of groups, the *symmetry groups* of solid objects.

Definition. *A* symmetry *of a solid object is a way of moving it so that it ends up in the space it originally occupied. We are only interested in the final position of the object, not how it got there, so for example a clockwise rotation of* 90° *is the same as an anticlockwise rotation of* 270°.

For example, consider the set of symmetries of a square. We can rotate it anticlockwise through 90°, 180° or 270°. We can also flip it over either horizontally or vertically, or along the main diagonal or the other diagonal. And, of course, we can simply put the square back where we found it. We denote these symmetries by R_{90}, R_{180}, R_{270}, H, V, D, D' and R_0 respectively. We can represent these in the figure below. We imagine that the square is transparent and has the letter R on it.

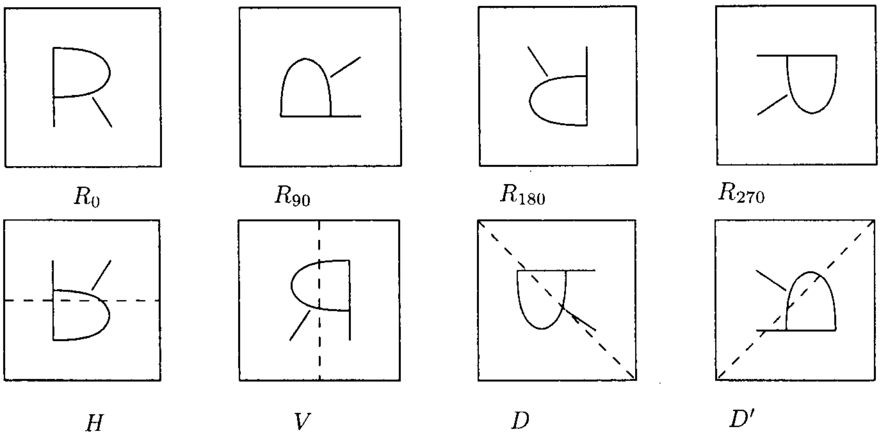

Figure 1: Symmetries of the square

To form a group, we need an operation. For symmetries A and B, we define $A*B$ to be the symmetry which has the same effect as B followed by A. For example, $R_{90} * R_{180} = R_{270}$. Less obviously, $R_{90} * H = D'$. And we obviously have $R_0 * A = A = A * R_0$ for any A.

Exercise 16. *Complete the Cayley table of* $*$.

$*$	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}				D'			
R_{180}	R_{180}							
R_{270}	R_{270}							
H	H							
V	V							
D	D							
D'	D'							

Proposition 17. *The set of symmetries of the square forms a group under the operation* $*$.

The hardest part of proving this would be to check associativity: there are $8^3 = 512$ ways of choosing A, B and C to check that $A * (B * C) = (A * B) * C$. But the symmetries are functions, and the operation we have is function composition, and we know that composition of functions is an associative operation.

The symmetry group of the square is usually denoted D_4. More generally, the symmetries of a regular n-gon form a group with $2n$ elements, usually denoted D_n and called the *dihedral group of order* $2n$.

Friday: The full symmetric group S_n

Related to the symmetry groups we discussed last week are the *full symmetric groups*. The group S_n is defined to be the set of all bijections (one-to-one and onto functions) from $\{1, 2, \ldots, n\}$ to itself. Again, the group operation is "composed with", in other words $f * g = f \circ g$.

Exercise 18. *How many elements does S_n have?*

We can represent the elements of S_n in matrix form, as follows. For our example, we will fix $n = 4$. We represent the element f by the 2×4 matrix which has $\begin{bmatrix} 1 & 2 & 3 & 4 \end{bmatrix}$ as its first row and $\begin{bmatrix} f(1) & f(2) & f(3) & f(4) \end{bmatrix}$ as its second row. For example the bijection which has $f(1) = 3$, $f(2) = 4$, $f(3) = 2$, $f(4) = 1$ is represented by the matrix $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$. We can then work out the composition of two elements. For example, we have

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}.$$

To answer the previous exercise, we can see that there are n ways to fill in the first entry in row 2, $n-1$ ways to fill in the next, $n-2$ for the next and so on, giving a total of $n!$ ways to write such a matrix. Thus $|S_n| = n!$.

Commutativity and abelian groups

For any real numbers x and y we have $x + y = y + x$. Thus the group operation in $(\mathbb{R}, +)$ is a commutative operation. However, there is no need for every group operation to be commutative. For example, looking back at the group D_4 of symmetries of the square, we have that $R_{90} * H = D'$, whereas $H * R_{90} = D$.

Definition. *A group $(G, *)$ is* abelian *if $*$ is a commutative operation, and* non-abelian *otherwise.*

So $(\mathbb{R}, +)$ is an abelian group whereas D_4 is a non-abelian group.

Notice that even if G is a non-abelian group, there will still be *some* elements x and y satisfying $x * y = y * x$. For example, this will be true if $x = y$, or if $x = e$ or $y = e$ (where e is the identity element).

Exercise 19. *The elements of S_3 are $e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$, $\varphi = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ and $\psi = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$, $\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\gamma = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Complete the Cayley table for S_3.*

$*$	e	φ	ψ	α	β	γ
e						
φ						
ψ						
α						
β						
γ						

Find elements x and y such that $x * y \neq y * x$.

Proposition 20. *Let n be an integer with $n \geq 3$. Then S_n is non-abelian.*

Cycles in S_n

Definition. *A* cycle *in S_n is an element of S_n such that there exist distinct $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ with $f(i_j) = i_{j+1}$ for $1 \leq j < k$, $f(i_k) = i_1$ and $f(j) = j$ for $j \notin \{i_1, i_2, \ldots, i_k\}$. We denote this cycle by $(i_1\ i_2\ \ldots\ i_k)$.*

For example, in S_8 we have

$$(1\ 3\ 4\ 6) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 1 & 7 & 8 \end{bmatrix}.$$

Exercise 21. *Write the elements φ, ψ, α, β and γ of S_3 in cycle form.*