Polynomials of a single variable.

A *monomial* in a single variable x is a function $P(x) = a_n x^n$, where a_n is a non-zero real number and $n \in \{0, 1, 2, 3, \ldots\}$.

Examples are $3x^2$, $-\pi x^8$ and $\sqrt{2}$.

A *polynomial* in a single variable x is either a finite sum of monomials in x or identically zero for all x.

So a polynomial is either always zero (written $P(x) \equiv 0$) or it may be written uniquely as

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $n \in \{0, 1, 2, 3, \ldots\}$, and $a_0, a_1, \ldots, a_n$ are real numbers and $a_n \neq 0$.

Each $a_i x^i$ is called a term of the polynomial. The number a_i is called the *coefficient* of x^i, for $i = 0, 1, 2, \ldots, n$.

The highest power of x in a polynomial (here n) is called the *degree* of the polynomial and is written $\deg P = n$.

The corresponding term $a_n x^n$ is called the *leading term* of the polynomial and a_n is called the *leading coefficient*.

A *monic polynomial* is a polynomial with $a_n = 1$.

The coefficient a_0 is called the *constant term* of the polynomial, even when it is zero.

Using summation notation, a polynomial is commonly written as $P(x) = \sum_{i=0}^{n} a_i x^i$.

The degree n and the coefficients $a_0, a_1, \ldots, a_n$ uniquely specify the polynomial.

We can have polynomials in two or more variables *e.g.* $2x^2y^3 - 3x^4 + xy^2 + y^3 - x - 3$ is a polynomial in x and y.

The degree of a term in a polynomial in several variables is the sum of the powers of the variables *e.g.* the degree of $14x^3yz^2$ is 6. A polynomial in several variables is called *homogeneous* if the degree of each term is the same, for example $x^3y^2 - 3z^5 + 4y^4z - x^2y^2z$ is a homogeneous polynomial of degree 5.

We will mainly consider polynomials in a single variable.

Algebra of Polynomials

Polynomials can be added subtracted and multiplied to give other polynomials. We can formally multiply $P(x) = \sum_{i=0}^{n} a_i x^i$ by $Q(x) = \sum_{j=0}^{m} b_j x^j$ to get

$$P(x)Q(x) = a_0b_0 + x(a_0b_1 + a_1b_0) + x^2(a_0b_2 + a_1b_1 + a_2b_0) + \cdots + x^{n+m-1}(a_{n-1}b_m + a_nb_{m-1}) + a_nb_mx^{n+m}.$$

More formally $\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m} x^k S_k,$

where $S_k = \sum_{\substack{i=1 \\ (i+j=k)}}^{n} \sum_{j=1}^{m} a_i b_j.$

The *Binomial Theorem* $(x+c)^n = \sum_{i=0}^{n} x^i c^{n-i} \binom{n}{i}$ is useful in expanding the power of a sum of two terms.

More generally, we can evaluate the product

$(x+c_1)(x+c_2)\cdots(x+c_n) =$

$x^n + x^{n-1}(\sum_{i_1=1}^{n} c_{i_1}) + x^{n-2}(\sum_{i_1<i_2} c_{i_1}c_{i_2}) + \cdots + c_1c_2\cdots c_n.$

We can write this more formally as

$\prod_{i=1}^{n}(x+c_i) = \sum_{k=0}^{n} x^{n-k} \sum_{i_1<\cdots<i_k} c_{i_1}\cdots c_{i_k}.$

For example, when $n=3$, $\sum_{i_1<i_2} c_{i_1}c_{i_2} = c_1c_2 + c_1c_3 + c_2c_3$.

Rational Functions

A *rational function* is the ratio of two polynomials $\frac{P(x)}{Q(x)}$, where $Q(x) \not\equiv 0$.

By long division, we can write $\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$, where S and R are polynomials and $\deg R < \deg Q$.

R is called the *remainder*.

For example, $\frac{x^3-x^2-3x-1}{x-2} = x^2+x-1+\frac{-3}{x-2}$.

We say x^3-x^2-3x-1 divided by $x-2$ equals x^2+x-1, with remainder -3.

If $R(x) \equiv 0$, we say that $Q(x)$ divides evenly into $P(x)$ (or just $P(x)$ is divisible by $Q(x)$).

Polynomials of low degree and their graphs

The zero polynomial $P(x) \equiv 0$ is often defined to have degree $-\infty$.

For degree $n=0$, we get a *constant polynomial* $P_0(x) = a_0$.

Its graph $y = a_0$ is a straight line parallel to the x-axis.

For degree $n=1$, we get a *linear polynomial* $P_1(x) = a_1x + a_0$.

Its graph $y = a_1x + a_0$ is a line not parallel to either axis.

For degree $n=2$, we get a *quadratic polynomial* $P_2(x) = a_2x^2 + a_1x + a_0$.

The graph of a quadratic $y = P_2(x)$ is $\bigcup$-shaped if $a_2 > 0$ and is $\bigcap$-shaped if $a_2 < 0$. These curves are sometimes called *parabolas*.

For $n=3$, we get a *cubic polynomial* $P_3(x) = a_3x^3 + a_2x^2 + a_1x + a_0$.

So forth, we get *quartics* $P_4(x)$, *quintics* $P_5(x)$ *etc.*

Note that for very large positive and negative values of x, $P_n(x) \sim a_nx^n$ -we say $P_n(x)$ behaves like (or is asymptotically like) a_nx^n.

If $a_n > 0$, then, for even $n \geq 2$, $P_n(x) \to \infty$ as $x \to \infty$ and $P_n(x) \to \infty$ as $x \to -\infty$; for odd $n \geq 1$, $P_n(x) \to \infty$ as $x \to \infty$ and $P_n(x) \to -\infty$ as $x \to -\infty$.

Analogous statements are made when $a_n < 0$ (all signs are reversed).

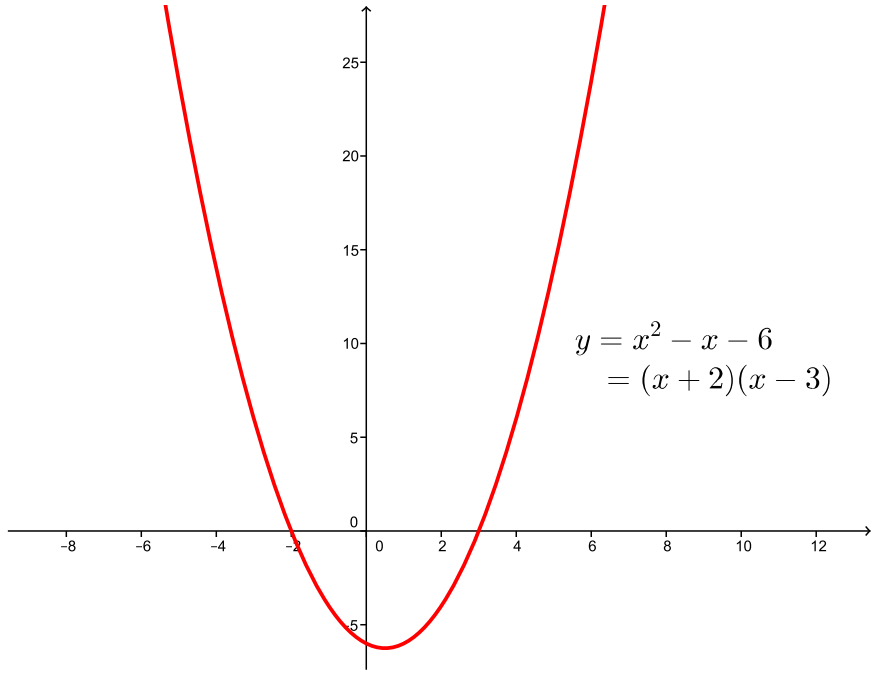
Polynomials are *continuous* functions of x (no breaks or jumps).

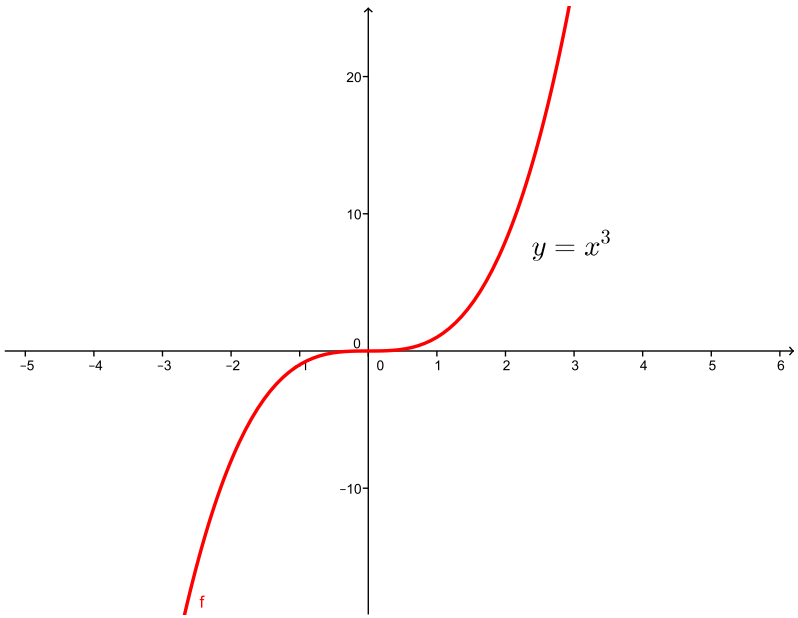
Polynomials with terms containing only even powers are called *even*. An *even polynomial* satisfies $P(x) = P(-x)$.

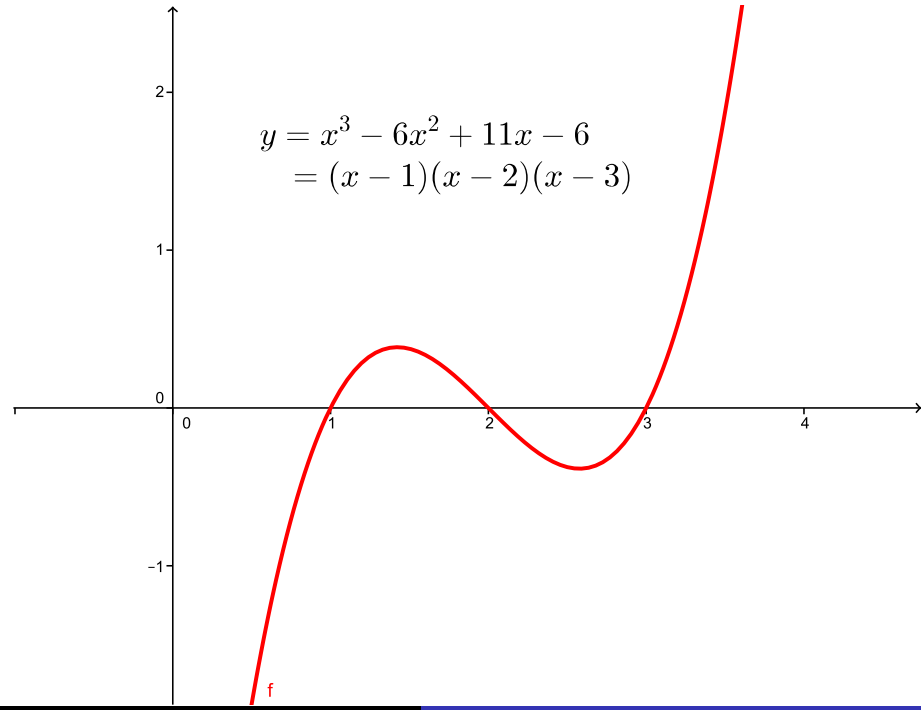
Polynomials with terms containing only odd powers are called *odd*. An *odd polynomial* satisfies $P(x) = -P(-x)$.

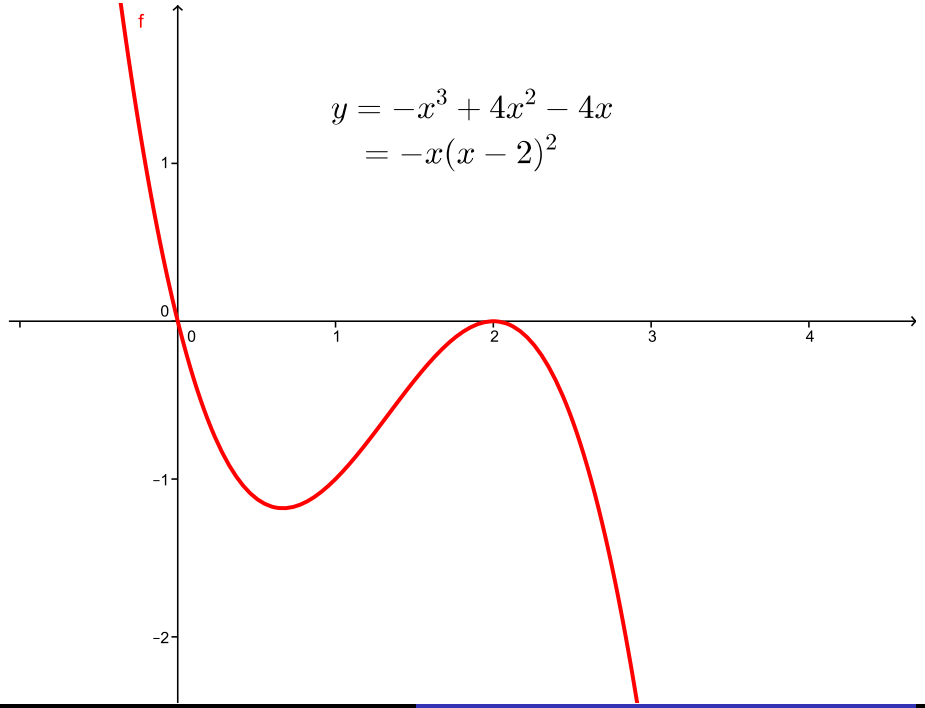
For example, $x^2 + 2$ is even and $x^3 - 3x$ is odd.

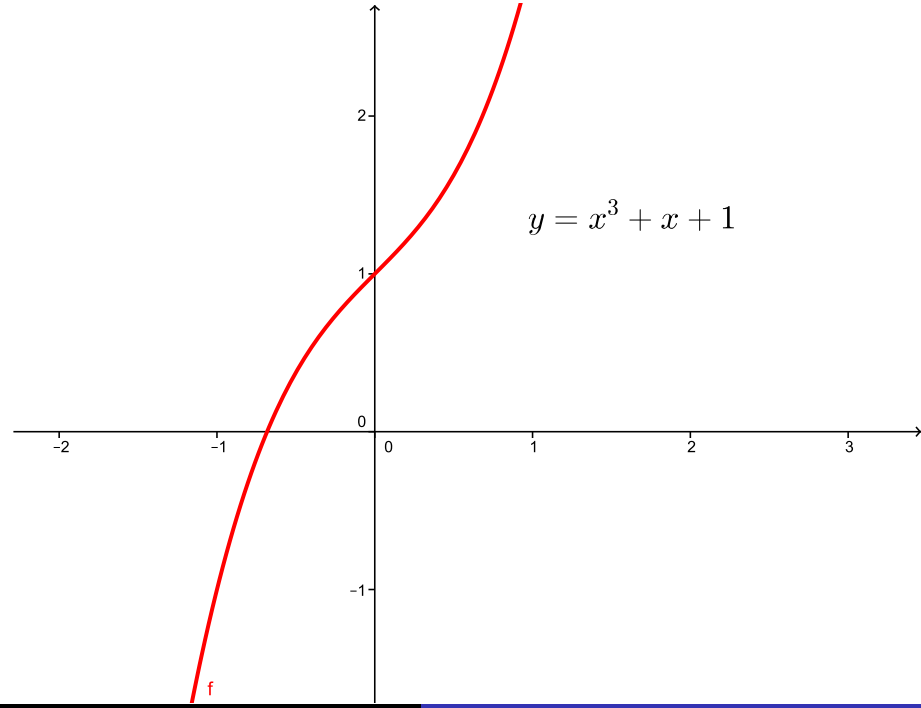
Polynomials of even degree $n \geq 2$ will always have a *global minimum* value if $a_n > 0$ (or analogously a *global maximum* if $a_n < 0$).

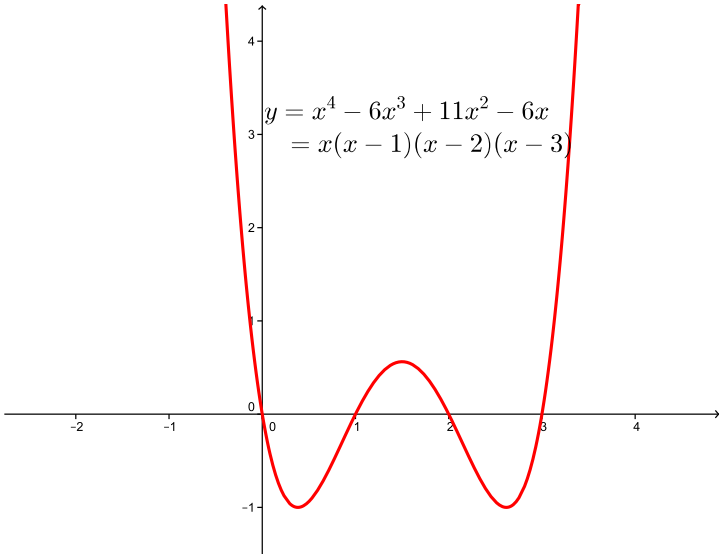


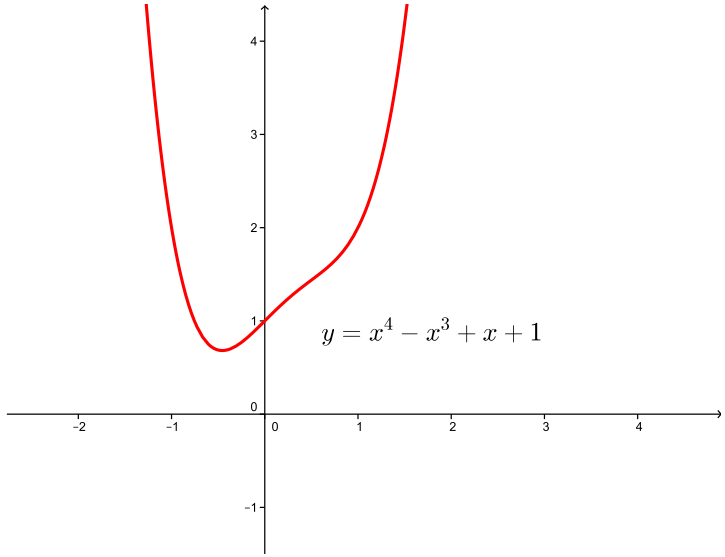





f
$y = -x^3 + 4x^2 - 4x$
$= -x(x-2)^2$


$y = x^3 + x + 1$
f


$y = x^4 - 6x^3 + 11x^2 - 6x$
$= x(x-1)(x-2)(x-3)$


$y = x^4 - x^3 + x + 1$

The Roots of a Polynomial

A number r is called a *root* (or zero) of the polynomial $P(x)$, if $P(r) = 0$.

A polynomial may have no, one or several real roots.

A polynomial may also have roots that are complex numbers.

If we count real roots as complex numbers $r = r + 0i$, then a polynomial of degree n has *exactly n roots in the complex numbers, counting multiplicities*.

This is *The Fundamental Theorem of Algebra*.

We just consider polynomials with real coefficients, but it also applies when the coefficients are complex numbers.

- A zero-degree polynomial has no roots since $P_0(x) = a_0 \neq 0$ for all x.
- A linear polynomial $P_1(x) = a_1 x + a_0$ has a unique real root $r = -\dfrac{a_0}{a_1}$.
- A quadratic polynomial $P_2(x) = a_2 x^2 + a_1 x + a_0$ has roots depending on the sign of the *discriminant* $\Delta = a_1^2 - 4a_0 a_2$.

1. $\Delta > 0$. The polynomial $P_2(x)$ has two real roots $r = \dfrac{-a_1 \pm \sqrt{\Delta}}{2a_2}$.
   The graph of the polynomial crosses the x-axis twice.
2. $\Delta = 0$. The polynomial $P_2(x)$ has one real root $r = -\dfrac{a_1}{2a_2}$, which is called a *double root* or *a root of multiplicity 2*.
   The graph of the polynomial touches the x-axis once and is in fact *tangent* to the x-axis at $x = r$.
3. $\Delta < 0$. The polynomial $P_2(x)$ has two complex roots $r = \dfrac{-a_1 \pm i\sqrt{-\Delta}}{2a_2}$.
   The roots are a complex conjugate pair. The graph of the polynomial never crosses the x-axis.

Two properties of polynomials with real coefficients

- If $r = \alpha + i\beta$ is a complex root of $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, then so is $\bar{r} = \alpha - i\beta$. (Proof: $P(\bar{r}) = \overline{P(r)} = 0$.)
  So the complex roots of real polynomials occur in complex conjugate pairs.
- A polynomial of odd degree has at least one real root. (Proof: if say $a_n > 0$, then $P(x) \to -\infty$ as $x \to -\infty$ and $P(x) \to +\infty$ as $x \to +\infty$. Since the graph is continuous it must cross the x-axis somewhere.)

Roots of a cubics, quartics etc.

All cubic polynomials have at least one real root.

A cubic can have (i) 3 distinct real roots, (ii) a double real root and a single real root, (iii) a triple real root or (iv) a single real root with a complex conjugate pair.

Examples:

(i) $x^3 - x = x(x-1)(x+1)$ which has roots $-1, 0, 1$;

(ii) $x^3 - 2x^2 + x = x(x-1)(x-1)$ which has roots $0, 1, 1$;

(iii) $x^3 - 3x^2 + 3x - 1 = (x-1)^3$ which has roots $1, 1, 1$;

(iv) $x^3 + x = x(x^2+1) = x(x-i)(x+i)$ which has roots $0, i, -i$.

A quartic can have four distinct real roots, a double real root and two other distinct real roots, two double real roots, a triple real root and a distinct real root, a quadruple real root, a complex conjugate pair and two distinct real roots, a complex conjugate pair and a double real root, two distinct complex conjugate pairs, or a double complex conjugate pair. Try construct examples of each of these.

There is an explicit formula for the roots of a cubic called *Cardano's formula* (analogous to the "$-b\pm$" formula). There is also one for quartics, but not for quintics (*cf* Galois).

Remainder Theorem and Factor Theorem

If we divide an nth degree polynomial $P_n(x)$ by $(x-\alpha)$, where $n \geq 1$, it will result in a polynomial $Q_{n-1}(x)$ of degree $n-1$ and a remainder R (a number).

We write this as $P_n(x) = Q_{n-1}(x)(x-\alpha) + R$.

The *Remainder Theorem* says that $R = P_n(\alpha)$.

Proof: put $x = \alpha$ in the previous equation.

Note this applies to real and complex α.

The *Factor Theorem* says that if α is a root of $P_n(x)$, then $(x-\alpha)$ is a factor of $P_n(x)$, that is it divides evenly into $P_n(x)$.

Proof: Use the Remainder Theorem with $R = P_n(\alpha) = 0$.

The Fundamental Theorem of Algebra tells us that there are n roots $r_1, r_2, \ldots, r_n$, possibly complex and including multiplicities. So we can peel off these roots one by one until we reach a constant. That is we can write a polynomial as a product of its factors as

$$P_n(x) = a_n(x-r_1)(x-r_2)\cdots(x-r_n).$$

Connection between coefficients and roots

A polynomial $P_n(x)$ of degree n can be uniquely specified by

- its $n+1$ coefficients $a_0, a_1, \ldots, a_n$; or by
- the leading coefficient a_n and the n (possibly complex) roots $r_1, \ldots, r_n$.

Vieta's formulae explore the connection between these.

For convenience in what follows, we look , without loss of generality, at monic polynomials ($a_n = 1$).

First we need some notation.

The Elementary Symmetric Polynomials

(Aside: these are multivariate polynomials but we just need their definitions).

The *Elementary Symmetric Polynomials* $x_1, x_2, \ldots, x_n$, written $e_k(x_1, \ldots, x_n)$ for $k = 0, 1, \ldots, n$ are defined by

$$
\begin{aligned}
e_0(x_1, \ldots, x_n) &= 1, \\
e_1(x_1, \ldots, x_n) &= \sum_{1 \le j \le n} x_j, \\
e_2(x_1, \ldots, x_n) &= \sum_{1 \le j < k \le n} x_j x_k, \\
e_3(x_1, \ldots, x_n) &= \sum_{1 \le j < k < l \le n} x_j x_k x_l,
\end{aligned}
$$

$\ldots \quad \ldots$

$$e_n(x_1, \ldots, x_n) = x_1 x_2 \cdots x_n.$$

So, for example,

$$e_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

We can write these in general as

$$e_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Observe that $e_k(x_1, \ldots, x_n)$ has $\binom{n}{k}$ terms.

Vieta's formulae

A monic polynomial can be written as

$$
\begin{aligned}
P_n(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\
&= (x - r_1)(x - r_2) \cdots (x - r_n).
\end{aligned}
$$

By multiplying out the latter form we get

$$P_n(x) = x^n - x^{n-1}(r_1 + \cdots + r_n) + \cdots + (-1)^n r_1 \cdots r_n.$$

More concisely

$$P_n(x) = x^n - x^{n-1}e_1(r_1, \ldots, r_n) + \cdots + (-1)^n e_n(r_1, \ldots, r_n).$$

Vieta's formulae relate the coefficients to the elementary symmetric polynomials in $r_1, \ldots, r_n$.

$\frac{a_k}{a_n} = (-1)^{n-k} e_{n-k}(r_1, r_2, \ldots, r_n)$

for $k = 0, 1, \ldots n$. (Here, for completeness, I restored a_n).

Example 1 *Solve the system of equations* $abc = 6$, $ab + bc + ca = 11$, $a + b + c = 6$ *for* a, b, c.

Suppose a, b, c is a solution.

Define the polynomial $p(x) = (x - a)(x - b)(x - c)$.

By multiplying out the right side, we get

$p(x) = x^3 - 6x^2 + 11x - 6$.

This factors into $p(x) = (x - 1)(x - 2)(x - 3)$.

So $\{a, b, c\} = \{1, 2, 3\}$, and so we get solutions $(a, b, c) = (1, 2, 3)$ and five other permutations.

Example 2

Let $p_5(x) = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. *Prove that if* $2a_4^2 < 5a_3$, *then* $p_5(x)$ *cannot have all real roots.*

Call the roots r_i, for $i = 1, 2, 3, 4, 5$ (possibly complex).

Then $0 > 2a_4^2 - 5a_3 = 2\left(\sum_{i=1}^{5} r_i\right)^2 - 5 \sum_{1 \le i < j \le 5} r_i r_j$

$= 2\sum_{i=1}^{5} r_i^2 - \sum_{1 \le i < j \le 5} r_i r_j = \frac{1}{2} \sum_{1 \le i < j \le 5} (r_i - r_j)^2.$

If all the roots were real, the right side, being a sum of squares, would be non-negative. Since that is not the case, some of them must be complex.

Example 3

Let r_1, r_2, r_3 *be the roots of* $x^3 - 6x^2 + 8x - 2$.

Evaluate the sum $\sum_{i=1}^{3} \frac{r_i+3}{r_i-1}$. *Note* 1 *is not a root.*

Call the sum S. Then $S = \sum_{i=1}^{3}(1 + \frac{4}{r_i-1}) = 3 + \sum_{i=1}^{3} \frac{4}{r_i-1}$.

The numbers $r_i - 1$ are the roots of the polynomial

$(y + 1)^3 - 6(y + 1)^2 + 8(y + 1) - 2 = y^3 - 3y^2 - y + 1$.

The numbers $\frac{1}{r_i-1}$ then satisfy the equation

$\left(\frac{1}{z}\right)^3 - 3\left(\frac{1}{z}\right)^2 - \left(\frac{1}{z}\right) + 1 = 0$ and so are roots of the cubic $z^3 - z^2 - 3z + 1$. The sum of its roots is 1.

So $\sum_{i=1}^{3} \frac{1}{r_i-1} = 1$ and hence $S = 3 + 4(1) = 7$.

Locating roots: Descartes' Rule of Signs

There are some quick things we can say about the roots of a polynomial without finding them. For example:

- $x^4 + 3x^2 + 6x + 10$ has no real roots, since it can be written as $(x^2 + 1)^2 + (x + 3)^2 \ge 1$.
- $P(x) = x^4 - 3x^2 - 6x + 5$ has at least one root in $(0, 1)$, since $P(0) = 5 > 0$ and $P(1) = -3 < 0$, so by continuity it must be zero somewhere between.

Descartes' Rule of Signs says *that a polynomial* $P(x)$ *cannot have more positive real roots than the number of sign changes in the (non-zero) coefficients.*

For example, x^3+x^2-x-2 has signs $++--$ and hence has one sign change; so $P(x)$ has at most one positive real root.

The result can be strengthened by stating that *the number of positive real roots is equal to the number of sign changes in $P(x)$ or is less by an even number.*

So for example, $P(x)=x^6-4x^5-3x+1$ has either two or no positive real roots.

Since $P(1)=-5<0,$ we conclude it must be two.

Note that multiplicities of roots are counted, so for example we see that $(x-1)^2(x+1)=x^3-x^2-x+1$ has two sign changes, so the double root $x=1$ counts as two.

The result can be extended to negative roots by considering $P(-x)$.

The number of sign changes in $P(-x)$ equals the number of negative real roots or the number of negative real roots less an even number.

In the previous example, $P(-x)=x^6+4x^5+3x+1$ which has no sign change, so there is no negative root.

So $P(x)=x^6-4x^5-3x+1$ has exactly two real roots, both of which are positive.

Since $P(0)>0,\ P(1)<0,\ P(4)<0$ and $P(5)>0,$ we can locate them in $(0,1)$ and $(4,5)$.

Example -Irish MO 1990

Find all polynomials $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ such that (i) all the roots are real numbers and (ii) each coefficient $a_i\in\{1,-1\}$ for $i=0,1,2,\ldots,n-1$.

Call the roots $r_i,$ for $i=1,2,\ldots,n.$

First note that, since $a_0\neq 0,$ none of the roots is zero.

Also $\sum_{1\le i\le n} r_i=-a_{n-1}=\pm 1$ and $\sum_{1\le i<j\le n} r_ir_j=a_{n-2}=\pm 1.$

Since the roots are all real,

$0\le \sum_{1\le i\le n} r_i^2=(\sum_{1\le i\le n} r_i)^2-2\sum_{1\le i<j\le n} r_ir_j=1\pm 2.$

Consequently $\sum_{1\le i\le n} r_i^2=3$ and $a_{n-2}=\sum_{1\le i<j\le n} r_ir_j=-1$, a result that we will use later.

Now $1=a_0^2=r_1^2r_2^2\cdots r_n^2,$ so applying the AGM to $r_1^2,\ldots,r_n^2$ gives $\frac{3}{n}\ge 1$, and hence $n\le 3$.

So the only possibilities are linear, quadratic and cubic polynomials.

The linear polynomials $x+1$ and $x-1$ work.

It's easy to show that the only quadratics that work are x^2+x-1 and x^2-x-1.

There are eight possible cubics to be considered.

From the above (with $n = 3$), we must have $a_1 = -1,$ so this rules out four of them.

The cubics $x^3 + x^2 - x - 1 = (x+1)^2(x-1)$ and $x^3 - x^2 - x + 1 = (x-1)^2(x+1)$ both work.

The cubic $P(x) = x^3 + x^2 - x + 1 \geq x^2 - x + 1 > 0$ if $x \geq 0,$ and so has no positive root. Now $P(-x) = -x^3 + x^2 + x + 1$ has one sign change so, by Descartes' Rule, $P(x)$ has at most one negative root and so has exactly one real root.

Finally $x^3 - x^2 - x - 1 = -P(-x),$ so it has the same number of roots as $P(x)$, that is one. In conclusion, the polynomials with the desired properties are $x+1, x-1, x^2+x-1, x^2-x-1, x^3+x^2-x+1, x^3-x^2-x-1.$

Some useful factorisations

$$x^2 - a^2 = (x-a)(x+a);$$

$$x^3 - a^3 = (x-a)(x^2 + ax + a^2).$$

More generally, for integer $n \geq 2$,

$$x^n - a^n = (x-a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}).$$

If $n \geq 3$ is odd, then

$$x^n + a^n = (x+a)(x^{n-1} - ax^{n-2} + a^2x^{n-3} + \cdots + (-1)^{n-1}a^{n-1}).$$

Even for $n = 4$, we can write

$$\begin{aligned} x^4 + a^4 &= (x^2 + a^2)^2 - 2a^2x^2 = (x^2 + a^2)^2 - (\sqrt{2}ax)^2 \\ &= (x^2 + \sqrt{2}ax + a^2)(x^2 - \sqrt{2}ax + a^2). \end{aligned}$$

Irreducible Polynomials

A polynomial over a ring/field F means a polynomial all of whose coefficients are in F. Here we will take F to be $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

A polynomial $P(x)$ over F is said to be **irreducible over** F if and only if

(i) $\deg P \geq 1$ and

(ii) if $P = QR$ for polynomials over F, then either Q or R is constant.

A polynomial that is not irreducible is called **reducible**.

For example, all linear polynomials are irreducible.

Consider the polynomials $p_1(x) = x^2 - 9 = (x-3)(x+3),$

$p_2(x) = x^2 - 1/4 = (x - 1/2)(x + 1/2),$

$p_3(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$

$p_4(x) = x^2 + 1 = (x - i)(x + i).$

The polynomial $p_1(x)$ is reducible over $\mathbb{Z},$ the rest are not. (In fact, $p_2(x)$ is not a polynomial over $\mathbb{Z}$). The polynomials $p_1(x), p_2(x)$ are reducible over $\mathbb{Q},$ the rest are not. The polynomials $p_1(x), p_2(x), p_3(x)$ are reducible over $\mathbb{R},$ the last is not. All four are reducible over $\mathbb{C}$.

Gauss's Lemma: A polynomial with integer coefficients is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.

Polynomials over $\mathbb{Z}$; Eisenstein's Criterion

If r is a rational root of a monic polynomial with integer coefficients then r must be an integer (exercise!)

Eisenstein's Criterion Consider a polynomial with integer coefficients $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

If there exists a prime number p such that:

- p divides each a_i for $i \neq n$, and
- p does not divide a_n, and
- p^2 does not divide a_0,

then $P(x)$ is irreducible over the rational numbers, and hence by Gauss's lemma is also irreducible over the integers.

Consider, for example, the polynomial $P(x) = 5x^4 + 14x^2 + 63$.

We want primes p that divide a_0, a_1, a_2, a_3.

Clearly $p = 7$ works. Also 7 doesn't divide a_4 and its square 49 doesn't divide a_0.

So Eisenstein's Criterion applies and hence $P(x)$ is irreducible over $\mathbb{Q}$ (and over $\mathbb{Z}$).

Note that we could not have reached this conclusion by only checking that $P(x)$ has no rational roots (which eliminates possible linear factors), since a decomposition into two quadratic factors could also be possible.

Example: IMO 1993,1 (T. J. Laffey)

Let $n > 1$ be an integer and let $f(x) = x^n + 5x^{n-1} + 3$. Prove that there do not exist polynomials $g(x)$, $h(x)$, each having integer coefficients and degree at least one, such that $f(x) = g(x)h(x)$.

First observe that $f(x)$ has no integer roots, since $f(m) \geq 3$ for $m \geq 0$; $|f(m)| \geq 3$ for $m \leq -5$ and the cases $m = -1, -2, -3, -4$ can easily be checked.

Now suppose that $f(x) = g(x)h(x)$, where $g(x)$, $h(x)$, are nonconstant polynomials with integer coefficients.

Since $|f(0)| = 3$, then either $|g(0)| = 1$ or $|h(0)| = 1$.

Without loss of generality, we assume $|g(0)| = 1$ and write $g(x) = (x - \alpha_1) \cdots (x - \alpha_k)$.

Then $|\alpha_1 \alpha_2 \cdots \alpha_k| = 1$.

Since each α_i is a root of $f(x)$, then $\alpha_i^{n-1}(\alpha_i + 5) = -3$ for $i = 1, 2, \ldots, k$.

Taking the product of these gives $|(\alpha_1 + 5) \cdots (\alpha_k + 5)| = 3^k$. So $|g(-5)| = 3^k$.

But $|f(-5)| = |g(-5)||h(-5)| = 3$. The only possibility is $k = 1$ and hence $|\alpha_1| = 1$.

Consequently $g(x)$ (and hence $f(x)$) must have an integer root — contradiction. So no such $g(x)$, $h(x)$, exist.

Greatest Common Divisor of Polynomials

The *greatest common divisor* of the polynomials $A(x)$ and $B(x)$, denoted $\gcd(A,B)(x)$ is the monic polynomial $C(x)$ of maximum degree that is a factor of both $A(x)$ and $B(x)$.

We find it using the *Euclidean Algorithm*.

Suppose wlog that $\deg A \geq \deg B$.

By long division of polynomials, we get

$A(x) = q_0(x)B(x) + r_0(x)$, and $\deg r_0 < \deg B$.

Moreover, $\gcd(A,B)(x) = \gcd(B,r_0)(x)$.

Next we write $B(x) = q_1(x)r_0(x) + r_1(x)$, where $\deg r_1 < \deg r_0$.

Again $\gcd(B,r_0)(x) = \gcd(r_0,r_1)(x)$.

We continue by writing $r_k(x) = q_{k+2}(x)r_{k+1}(x) + r_{k+2}(x)$, with $\deg r_{k+2} < \deg r_{k+1}$.

We eventually reach $r_{N+2} = C$ constant.

If $C \neq 0$, then there is no gcd of degree ≥ 1.

If $C = 0$, then $\gcd(A,B)(x) = \gcd(r_N, r_{N+1})(x) = r_{N+1}(x)$.

For example, if $A(x) = x^3 + x - 2$ and $B(x) = x^2 - 1$, we write $x^3 + x - 2 = x(x^2-1) + 2x - 2$.

Then $x^2 - 1 = (\frac{1}{2}x + \frac{1}{2})(2x-2) + 0$.

So $\gcd(x^3 + x - 2, x^2 - 1) = x - 1$.

Roots of Unity

Let $n \geq 2$ be a positive integer.

The roots of $z^n - 1$ are $1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}$,

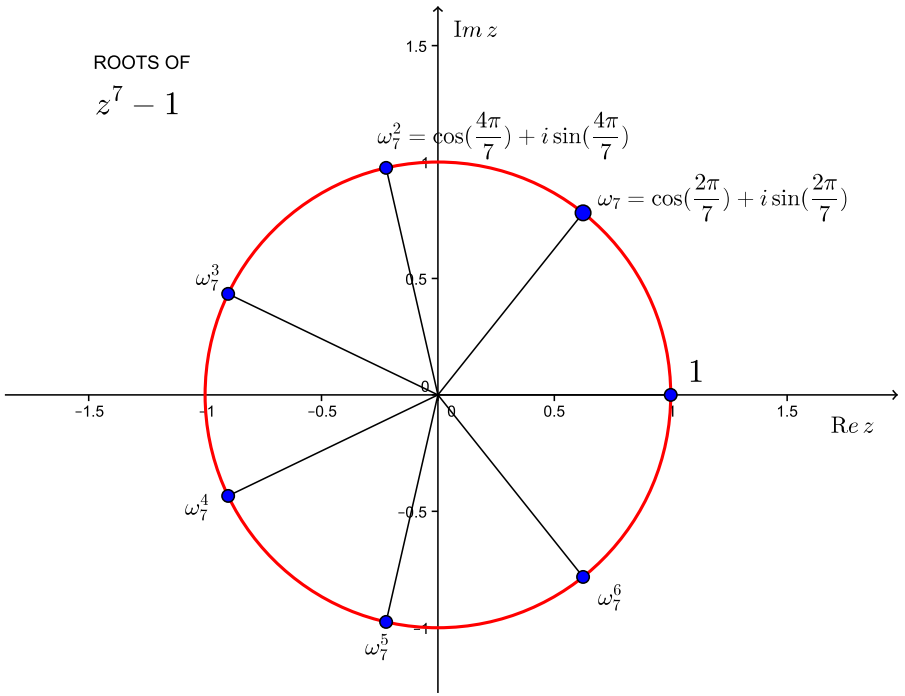
where $\omega_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$,

called the *nth roots of unity*.

By *de Moivre's Theorem*, $\omega_n^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$.

Note $|\omega_n| = 1$ and $\overline{\omega_n} = \dfrac{1}{\omega_n} = \omega_n^{n-1}$.

Also $1 + \omega_n + \omega_n^2 + \cdots + \omega_n^{n-1} = \dfrac{\omega_n^n - 1}{\omega_n - 1} = 0$.



Primitive Roots of Unity

We say w is a *primitive nth root of unity*, if $w^n = 1,$ but $w^k \neq 1,$ for $1 \leq k < n$.

We see ω_n^k is a primitive root of unity if and only if $\gcd(k, n) = 1$. For example, the primitive sixth roots of unity are ω_6 and ω_6^5.

Given a primitive root of unity $w,$ the set $\{w^k | \, k = 0, 1, 2, \ldots, n-1\}$ contains all the roots of unity.

The number of nth primitive roots of unity is $\varphi(n)$, where φ is Euler's totient function.

Cyclotomic polynomials

The nth cyclotomic polynomial, for any positive integer n, is the unique irreducible polynomial with integer coefficients, which is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$.

Its roots are the nth primitive roots of unity ω^k , where k runs over the integers less than n and coprime to n.

That is, the nth cyclotomic polynomial is $\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega_n^k)$.

If p is prime, then $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

If $n = 2p$, where p is an odd prime, then $\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1}$.

Examples: $\Phi_0(x) = 1$

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = x^2 - x + 1$

$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_8(x) = x^4 + 1$

$\Phi_9(x) = x^6 + x^3 + 1$

The coefficients can be bigger than 1 in magnitude, for example in $\Phi_{105}(x)$. The cyclotomic polynomials are monic polynomials, with integer coefficients that are irreducible over the field of the rational numbers. Except for $n = 1, 2$, they are palindromic polynomials of even degree. The degree of Φ_n, or in other words the number of nth primitive roots of unity, is $\varphi(n),$ the Euler totient function. A fundamental property is $\prod_{d|n} \Phi_d(x) = x^n - 1,$ which means that each nth root of unity is a primitive dth root of unity for a unique d dividing n.

It then follows that $\sum_{d|n} \varphi(d) = n.$

Symmetric Polynomials and Newton's Identities

A polynomial that is a function of several independent variables $x_1, x_2, \ldots, x_n$ is called *symmetric* if it is unchanged by the interchange of any pair of variables.

This implies that it is unchanged by any permutation of the variables.

An example is $P(x_1, x_2, x_3) = x_1^3+x_2^3+x_3^3-6x_1x_2x_3-5x_1x_2-5x_2x_3-5x_3x_1+3x_1+3x_2+3x_3-8$.

This satisfies $P(x_1, x_2, x_3) = P(x_1, x_3, x_2) = P(x_2, x_1, x_3) = P(x_2, x_3, x_1) = P(x_3, x_1, x_2) = P(x_3, x_2, x_1)$.

The *Fundamental Theorem of Symmetric Polynomials* states that any symmetric polynomial in $x_1, x_2, \ldots, x_n$ can be written as a polynomial in $e_1, e_2, \ldots, e_n$.

For example,

$$x_1^2 + x_2^2 + \cdots + x_n^2 = \left(\sum_{1\le i\le n} x_i\right)^2 - 2\sum_{1\le i<j\le n} x_i x_j = e_1^2 - 2e_2.$$

This is an example of one of *Newton's identities*.

These identities relate the symmetric power sums $s_k = x_1^k + x_2^k + \cdots + x_n^k$ $(k = 1, 2, 3, \ldots)$ to the elementary symmetric polynomials.

So, for example, $s_2 = e_1^2 - 2e_2$.

To derive the next one we observe that

$e_1e_2 = \sum_{1\le i<j\le n} (x_ix_j^2 + x_i^2x_j) + 3e_3$ and

$e_1^3 = s_3 + 3\sum_{1\le i<j\le n} (x_ix_j^2 + x_i^2x_j) + 6e_3$, so eliminating the symmetric polynomial in both equations gives the third Newton identity $s_3 = e_1^3 - 3e_1e_2 + 3e_3$.

These relationships can be inverted to get $2e_2 = s_1^2 - s_2$ and $6e_3 = s_1^3 - 3s_1s_2 + 2s_3$.

One can continue for higher powers, but there is a convenient iterative scheme that we won't derive namely:

$$\begin{aligned} e_1 &= s_1 \\ 2e_2 &= e_1s_1 - s_2 \\ 3e_3 &= e_2s_1 - e_1s_2 + s_3 \\ 4e_4 &= e_3s_1 - e_2s_2 + e_1s_3 - s_4 \\ \cdots &\quad \cdots \end{aligned}$$

Example 1: *Find all solutions of the system of four simultaneous equations:*

$x + y + z + w = 6,$

$x^2 + y^2 + z^2 + w^2 = 14,$

$x^3 + y^3 + z^3 + w^3 = 36,$

$x^4 + y^4 + z^4 + w^4 = 98.$

These just say that $s_1 = 6,\ s_2 = 14,\ s_3 = 36$ and $s_4 = 98$.

So $e_1 = 6,\ e_2 = (36 - 14)/2 = 11,$
$e_3 = ((11)(6) - (6)(14) + 36)/3 = 6$ and
$e_4 = ((6)(6) - (11)(14) + (6)(36) - 98)/4 = 0.$

So x, y, z, w are the roots of the quartic
$t^4 - 6t^3 + 11t^2 - 6t = t(t-1)(t-2)(t-3).$

So x, y, z, w are all 24 permutations of the numbers
$0, 1, 2, 3.$

Lots of examples: Example 1

Suppose $P(x)$ and $Q(x)$ are two polynomials that satisfy the identity $P(Q(x)) \equiv Q(P(x))$, for all real numbers x. If the equation $P(x) = Q(x)$ has no real solution, show that $P(P(x)) = Q(Q(x))$ also has no real solution.

Since $P(x) = Q(x)$ has no real solution, we may assume, without loss of generality, that $P(x) > Q(x)$ for all x.

Suppose $x = a$ is a solution of $P(P(x)) = Q(Q(x))$.

Then
$P(Q(a)) > Q(Q(a)) = P(P(a)) > Q(P(a)) = P(Q(a)),$
thus giving a contradiction.

Example 2

Let $P(x)$ be the polynomial
$P(x) = 1 - x + x^2 - x^3 + \cdots + x^{20}$.
Let $Q(x) = a_0 + a_1 x + \cdots + a_{20} x^{20}$ be the polynomial obtained by expanding $P(x+4)$.
Find the sum of the coefficients of $Q(x)$.

Summing the geometric series, $P(x) = \dfrac{1 + x^{21}}{1 + x}$.

Then $Q(x) = P(x+4) = \dfrac{(x+4)^{21} + 1}{x + 5}$.

So $a_0 + a_1 + \cdots + a_{20} = Q(1) = \dfrac{5^{21} + 1}{6}$.

Example 3

Given the polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with integer coefficients $a_0, \ldots a_{n-1}$ and given also that there exist four distinct integers a, b, c, d such that $P(a) = P(b) = P(c) = P(d) = 5$, show that there is no integer k such that $P(k) = 8$.

The polynomial $P(x) - 5$ has four distinct integer roots a, b, c, d and hence we can write
$P(x) = 5 + (x-a)(x-b)(x-c)(x-d)Q(x),$
where $Q(x)$ is a monic polynomial of degree $n - 4$.

Moreover when a monic polynomial with integer coefficients has a factor $(x - m)$, for some integer m,

then the polynomial obtained upon division by $(x-m)$, is also a monic polynomial with integer coefficients (Exercise!).

So $Q(x)$ is a monic polynomial with integer coefficients.

Now suppose that there is an integer k such that $P(k) = 8$. Then $Q(k)$ is an integer and

$(k-a)(k-b)(k-c)(k-d)Q(k) = 3.$

Looking at the integer factorisations of 3, we see that at least three of $(k-a)$, $(k-b)$, $(k-c)$, $(k-d)$ must belong to the set $\{-1, 1\}$ and so at least two of them must be equal. This contradicts a, b, c, d being distinct.

Hence no such k exists.

Example 4

Let k be a positive integer. Find all polynomials $P(x)$ with real coefficients that satisfy $P(P((x)) = (P(x))^k$, for all real numbers x.

Either $P(x)$ is a constant or $P(x)$ takes on infinitely many values.

Case (i): If $P(x) \equiv c$, then $c = c^k$. Then either $k = 1$ and c is arbitrary or $k \geq 2$ and $c = 0$ or 1.

Case (ii): if P is not constant, then the functional equation gives $P(y) = y^k$, for infinitely many values of y.

So $P(x) - x^k$ is a polynomial with infinitely many roots and hence must vanish identically.

That is $P(x) \equiv x^k$ and this works.

Example 5 *Find all positive solutions of* $nx^{n+1} - (n+1)x^n + 1 = 0$.

Define $P(x) = nx^{n+1} - (n+1)x^n + 1$.

Clearly 1 is a root since $P(1) = 0$.

We write $P(x) = n(x^{n+1} - x^n) - (x^n - 1)$.

$= (x-1)(nx^n - x^{n-1} - \cdots - x - 1)$.

Define $Q(x) = nx^n - x^{n-1} - \cdots - x - 1$.

Then $Q(1) = 0$, so $(x-1)$ is a factor.

So $P(x)$ has a double root at $x = 1$.

There are two sign changes in the coefficients, so by Descartes' Rule, $P(x)$ has at most two positive real roots. So there are no positive roots other than the double root at $x = 1$.

Example 6

Find all real polynomials f such that
$xf(x)f(1-x)+x^3+100\geq 0$, *for all* $x\in\mathbb{R}$.

Define $g(x) = xf(x)f(1-x)+x^3+100.$

Since $g(x)\geq 0,$ for all x, it must have even degree.

Suppose f has degree n. The leading term of $f(x)$ is then a_nx^n and the leading term of $f(1-x)$ is $a_n(-x)^n$.

So the leading term of $xf(x)f(1-x)$ is $a_n^2(-1)^nx^{2n+1},$ which has an odd power of x.

If $n>1,$ it is also the leading term of $g(x),$ contradicting its degree being even.

So we require that $n=1$ and that x^3 cancels the leading term exactly.

Hence $-a_1^2+1=0,$ that is $a_1=\pm 1.$

So $f(x)$ has the form $f(x)=x+b$ or $f(x)=-x+b$ for some constant b.

Case 1: $f(x)=x+b$

The original equation then gives
$x(x+b)(1-x+b)+x^3+100\geq 0$ for all x, which when simplified gives $x^2+(b^2+b)x+100\geq 0$ for all x.

This holds iff the discriminant $(b^2+b)^2-4(100)\leq 0.$

So $-20\leq b^2+b\leq 20,$ Hence $-\frac{79}{4}\leq (b+\frac{1}{2})^2\leq\frac{81}{4}$.

So $(b+\frac{1}{2})^2\leq\left(\frac{9}{2}\right)^2,$ and hence $-\frac{9}{2}\leq b+\frac{1}{2}\leq\frac{9}{2}$.

That is $-5\leq b\leq 4$.

Case 2: $f(x)=-x+b$

The original equation then gives
$x(-x+b)(1+x+b)+x^3+100\geq 0$ for all x, which when simplified gives $x^2+(b-b^2)x+100\geq 0$ for all x.

This holds iff the discriminant $(b^2-b)^2-4(100)\leq 0.$

So $-20\leq b^2-b\leq 20.$

Hence $-\frac{79}{4}\leq (b-\frac{1}{2})^2\leq\frac{81}{4}$.

So $(b-\frac{1}{2})^2\leq\left(\frac{9}{2}\right)^2,$ and hence $-\frac{9}{2}\leq b-\frac{1}{2}\leq\frac{9}{2}$.

That is $-4\leq b\leq 5$.

In conclusion the polynomials that work are $f(x)=x+b$, for $-5\leq b\leq 4$, and $f(x)=-x+b$, for $-4\leq b\leq 5$.

Example 7 *Find the roots of* $x^4+ax^3+bx^2+ax+1.$

A root r satisfies $r^4+ar^3+br^2+ar+1=0.$

Clearly $r\neq 0,$ so dividing by r^2 and regrouping gives
$$r^2+\frac{1}{r^2}+a\left(r+\frac{1}{r}\right)+b=0.$$

If we define $u=r+\dfrac{1}{r},$ this gives $u^2-2+au+b=0.$

We solve this for u and then solve $r^2-ru+1=0$ for r.

Example 8

Find all real polynomials f such that $f(x^2) = f(x)f(x-1)$, for all $x \in \mathbb{R}$.

We first look for constant solutions $f(x) = a_0$.

Then $a_0 = a_0^2$, so $a_0 = 0$ or $a_0 = 1$.

The constant solutions $f(x) = 0$ and $f(x) = 1$ both work.

Now suppose f has degree ≥ 1.

So f has a root α (possibly complex).

Then $f(\alpha) = 0$, so $f(\alpha^2) = f(\alpha)f(\alpha - 1) = 0$.

So α^2 is also a root.

Likewise $\alpha^4, \alpha^8, \alpha^{16}, \ldots, \alpha^{2^n} \ldots$ are all roots.

Since a polynomial has a finite number of roots, there must exists $r > s$ with $\alpha^{2^r} = \alpha^{2^s}$.

So $\alpha = 0$, or there is a number $m \geq 1$ with $\alpha^m = 1$.

If 0 is a root of f, then $f(1) = f(1)f(0) = 0$, so 1 is a root.

Next $f(4) = f(2)f(1) = 0$, so 4 is a root.

Next $f(16) = f(4)f(3) = 0$, so 16 is a root.

We can proceed to generate an infinite number of distinct roots 2^{2^n} -contradicting the number of roots being finite.

So all roots satisfy $\alpha^m = 1$ for some $m \geq 1$ (that is α is a root of unity).

Hence if α is a root of f, then $|\alpha| = 1$.

Now if α is a root, then $f((\alpha+1)^2) = f(\alpha+1)f(\alpha) = 0$, so $(\alpha+1)^2$ is a root.

Hence $|\alpha + 1| = 1$.

Hence

$$1 = |\alpha+1|^2 = (\alpha+1)(\bar{\alpha}+1) = \alpha\bar{\alpha}+\alpha+\bar{\alpha}+1 = 2+\alpha+\bar{\alpha},$$

so $\alpha + \bar{\alpha} = -1$.

Now if α is real, then $\alpha = -\frac{1}{2}$, which contradicts $|\alpha| = 1$.

So the roots occurs in complex conjugate pairs $\alpha, \bar{\alpha}$.

The corresponding real factor is

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - x(\alpha+\bar{\alpha}) + \alpha\bar{\alpha} = x^2 + x + 1.$$

So $x^2 + x + 1$ is a factor of $f(x)$.

Now we write $f(x) = (x^2+x+1)^k g(x)$, where x^2+x+1 is **not** a factor of $g(x)$.

Now $f(x^2) = (x^4+x^2+1)^k g(x^2)$,

while $f(x)f(x-1) = (x^2+x+1)^k g(x)(x^2-x+1)g(x-1)$

$$= (x^4+x^2+1)^k g(x)g(x-1).$$

So the functional equation gives $g(x^2) = g(x)g(x-1)$.

We can repeat the argument above to conclude that $g(x) = 0$ or $g(x) = 1$ or x^2+x+1 divides into $g(x)$.

Clearly the last option is impossible, so we get
$g(x) = 0 \quad (\Rightarrow f(x) = 0),$ or $g(x) = 1.$

So the solutions are $f(x) = 0,\ f(x) = 1$ or
$f(x) = (x^2 + x + 1)^k,$ for any $k \geq 1.$

For completeness we show that the third solution works:

$$f(x)f(x-1) = (x^2+x+1)^k(x^2-x+1) = (x^4+x^2+1)^k = f(x^2).$$