3) Polynomials

Definition of polynomials:

Notation: used notation:

$$K[x]$$

where K is one of our numbers systems, K is one of our sets

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

- if K is $\mathbb{Z}$, then it is integer polynomials.
- if K is $\mathbb{Q}$ then it is rational polynomials
- if K is $\mathbb{R}$ then it is real polynomials
- if K is $\mathbb{C}$ then it is complex polynomials.

The point here is that whether you are integer, rational, real or complex polynomial, the role of x has played no part in determining the type of polynomial, it is the nature of K.

So <u>co-efficients determine type of polynomial</u>.

So in $K[x]$

↳ nature of x plays a part mostly when we tak about evaluating polynomial.

Suppose we have a polynomial $p(x)$

$$p(x) = \underbrace{a_0 + a_1 x + \cdots + a_k}_{\text{coefficients tell what polynomial is}} x^k$$

So integer polynomials have integer coefficients

So rational polynomials have rational coefficients

So real polynomials have real coefficients

So complex polynomials have complex coefficients

The set

$$K[x]$$

is the set of all polynomials

$$a_0 + a_1 x + a_2 x^2 + \dots + a_k x^k = \sum_{i=0}^{k} a_i x^i$$

where $a_i \in K$ are known as the coefficients of x and x is assumed to be a variable from a space X.

Note: Type of K i.e. type of polynomial / coefficients does not determine type of solution of x

For example: $x^2 - 2 = 0$

$x^2 - 2 = 0$ is an integer polynomial as it has integer coefficients, $x^2 - 2 \in \mathbb{Z}[x]$

But solution $x = \pm\sqrt{2} \in \mathbb{R}$ is a real solution

When we talk about polynomials, we write:

$p(x) \in K[x]$ and

$$p(x) = a_k x^k + \dots + a_1 x^1 + a_0 x^0 = \sum_{i=0}^{k} a_i x^i$$

- The <u>leading co-efficient</u> is a_k
- If $a_k \neq 0$, then polynomial has degree k denoted $\deg(p) = k$.

The "0 polynomial" is the polynomial where all co-efficients are zero.

$$0(x) = 0 \quad \text{and} \quad \deg(0(x)) = -\infty$$

defined to be $-\infty$.

Note: There is no reason X needs to be the same as K.

For example $K = \mathbb{Z}, X = \mathbb{R}$ is a common setting.

We call an element of $\mathbb{R}[x]$ a <u>real polynomial</u>

We call an element of $\mathbb{C}[x]$ a <u>complex polynomial</u>.

When we talk about polynomial functions, then we need to specify the nature of X.

For example

$$\boxed{p : \mathbb{R} \to \mathbb{C} : x \mapsto p(x)}$$

where p is a complex polynomial.

This a complex valued function that takes only real number inputs.

Note: If polynomial p has $\deg(p) = m$ and polynomial q has $\deg(q) = n$ then

polynomial $p \cdot q$ has $\deg(pq) = m+n$.

If you add a degree n polynomial with degree m with $m < n$ then you still have a degree n polynomial.

However if you add a degree n polynomial with degree n polynomial, you may end up with polynomial with degree less than n.

Binomial Theorem

Recall the binomial theorem:

$$(x+y)^n = \underbrace{(x+y)(x+y)\dots(x+y)}_{n \text{ times}}$$

$$= x^n + nx^{n-1}y + \frac{n(n-1)}{2}x^{n-2}y + \dots + nxy^{n-1} + y^n$$

$$= \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

Here $\binom{n}{j}$ is the binomial coefficient ${}_nC_r$

${}_nC_r = \binom{n}{j}$ is the number of ways of choosing j unordered things from a set of n objects without repetition.

Combinatorially, therefore

$$\boxed{\binom{n}{j} = \frac{n(n-1)(n-2)\dots(n-j+1)}{j!} = \frac{n!}{j!(n-j)!}}$$

The binomial coefficients can be found by Pascal's triangle:

$$
\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \binom{3}{4} & \\
\binom{4}{0} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \binom{4}{5}
\end{array}
$$

which equals

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & + & 2 & + & 1 & & \\
 & 1 & & 3 & + & 3 & + & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

The binomial theorem leads to various identities for the sum of binomial coefficients being easily proven:

- By setting $x = y = 1$ we see that

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n$$

- By setting $x = 1$ and $y = -1$, we see that for $n \geq 1$

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$$

- By differentiating both sides wrt to x and then setting $x = y = 1$ we have

$$\sum_{j=0}^{n} j \binom{n}{j} = n 2^{n-1}$$

• By switching roles of x and y we see that

$$\binom{n}{j} = \binom{n}{n-j}$$

Also this symmetry is also obvious from the definition in terms of factorials

$$\binom{n}{j} = \frac{n!}{j!(n-j)!} = \binom{n}{n-j}$$

Facts:

If $p(x)$ and $q(x)$ are polynomials then

(i) $\deg(p(x)+q(x)) \leq \max\{\deg(p(x)), \deg(q(x))\}$

(ii) $\deg(p(x) \times q(x)) = \deg(p(x)) + \deg(q(x))$

(iii) $\deg((q \circ p)(x)) = \deg(p(x)) \times \deg(q(x))$

Division Theorem:

Theorem: (Division Theorem for polynomials):

Let p be a (real or complex) polynomial of degree n; $\deg(p)=n$, let q be a (real or complex) polynomial of degree m, $\deg(q)=m$ with

$$m \leq n.$$

There exists a polynomial s of degree $n-m$ and a polynomial r of degree $<m$ such that or $r(x)=0$ such that

$$p(x) = q(x)s(x) + r(x)$$

Defn: If $r(x)=0$ for all x (i.e. r is identically equal to 0) then we say q is a factor of p.

proof: Consider the set

$$S = \left\{ p(x) - q(x)s(x) \,\middle|\, \begin{array}{l} s(x) \text{ is a real/complex} \\ \text{polynomial} \end{array} \right\}$$

If the zero polynomial belongs to S, then there is $s(x)$ such that

$$p(x) - q(x)s(x) = 0, \text{ and so}$$

$$p(x) = q(x)s(x) + 0$$

and set $r(x) = 0$. And this will satisfy existence for $s(x)$ and $r(x)$.
(since degrees add up when we multiply and $\deg(r(x)) = \deg(0) = -\infty < 0$)

Therefore now assume q is not a factor of p.
i.e. Suppose, 0 is not in S, $0 \notin S$.

Since all polynomials in S have either degree 0 or some natural number.

Since $0 \notin S$, then all polynomials in S have degree $\mathbb{N} \setminus \{0\}$

S is not empty, $S \neq \emptyset$ as for example it contains $p(x) - q(x)$.

So we can apply well ordering principle on degree.

Therefore by well-ordering principle, there is a minimum degree for elements of S.

Pick r so that it has minimal degree.

Since $r(x) \in S$,

$r(x) = p(x) - q(x).s(x)$ for some polynomial $s(x)$.

Need to show that it satisfies the condition $\deg(r(x)) < m$

Let degree of r be l. Need to show: $l < m$.
Suppose for a contradiction.
Suppose that $l \geq m$. Say

$$r(x) = a_0 + a_1 x + \dots + a_{l-1} x^{l-1} + a_l x^l \quad (a_l \neq 0)$$

and

$$q(x) = b_0 + b_1 x + \dots + b_m x^m \quad (b_m \neq 0)$$

Define:

$$s_1(x) := s(x) + \frac{a_l}{b_m} \cdot x^{l-m}$$

this is a polynomial since $b_m \neq 0$ & $l-m \geq 0$

Consider the following element of S:

$$r_1(x) = p(x) - s_1(x)q(x)$$

$$= p(x) - q(x)\left(s(x) + \frac{a_l}{b_m}x^{l-m}\right)$$

$$= \underbrace{p(x) - q(x)s(x)}_{r(x)} - \frac{a_l}{b_m}x^{l-m} \cdot q(x)$$

$$= r(x) + \frac{a_l}{b_m}x^{l-m}$$

$$= a_0 + a_1 x + \cdots + a_{l-1}x^{l-1} + a_l x^l$$

$$- \frac{a_l x^{l-m}}{b_m}\left(b_0 + b_1 + \cdots + b_m x^m\right)$$

$b_m \neq 0$

$$= a_0 + a_1 x + \cdots + a_{l-1} x^{l-1} + \cancel{a_l x^l}$$

$$- \left(\frac{a_l b_z}{b_m} x^{l-m} + \cdots + \frac{a_l b_{m-1}}{b_m} x^{l-1} + \cancel{a_l x^l} \right)$$

$$= a_0 + \cdots + \left(a_{l-1} - \frac{a_l b_{m-1}}{b_m} \right) x^{l-1}$$

Hence $r_1(x)$ has degree at most $l-1$, a contradiction for the minimality of degree of $r(x)$.

We know show that r and s are unique. Let r_1, s_1 be other polynomials such that

$$p(x) = s_1(x) q(x) + r_1(x) \text{ and } \deg(r_1(x)) < m$$

Then $r_1 = b - s_1 q$ since $r = p - sq$ we get

$$r - r_1 = p - sq - (p - s_1 q) = (s_1 - s) q$$

as r_1, r_2 have degree $< m$ so does $r - r_1$. As q has degree m and degrees add up, when you multiply, the only possible solution is

$$r = r_1 = 0, \quad s_1 = s \implies r = r_1 \text{ and } s = s_2$$

$\blacksquare$

Defn: If $p = qs + r$, we call s the quotient of p/q, and polynonomial r the remainder of p/q

One way of finding $s(x)$ and $r(x)$ is long division

Example: Find $s(x)$ and $r(x)$ for $p(x) = x^3 + 2x^2 + 3x + 4$ and $q(x) = 5x^2 + 6x + 7$

$$5x^2 + 6x + 7 \overline{\smash{\big)}\, x^3 + 2x^2 + 3x + 4}$$

Step 1: cancel out leading factor x^3.

To do this divide x^3 by the leading term of $q(x)$

$$\frac{x^3}{5x^2} = \frac{1}{5}x$$

This is the first value of $s(x)$

Now multiply $\frac{1}{5}x$ with $5x^2 + 6x + 7 = q(x)$

and subtract from $p(x) = x^3 + 2x^2 + 3x + 4$

$$\frac{1}{5}x \times q(x) = x^3 + \frac{6}{5}x^2 + \frac{7x}{5}$$

$$
\begin{array}{r}
\frac{1}{5}x \\
5x^2+6x+7 \overline{\smash{\big)}\ x^3+2x^2+3x+4} \\
(-)\ \cancel{x^3} \ (-)\ \frac{6}{5}x^2 \ (-)\ \frac{7}{5}x \\
\hline
\frac{4}{5}x^2+\frac{8}{5}x+4
\end{array}
$$

Step 2: Cancel out next leading term $\frac{4}{5}x^2$

To do this divide $\frac{4}{5}x^2$ by the leading term of $q(x)$

$$\frac{\frac{4}{5}x^2}{5x^2} = \frac{4}{25}$$

This is the next value of $s(x)$.

Now multiply $\frac{4}{25}$ with $5x^2+6x+7=q(x)$

and subtract from $p(x)=x^3+2x^2+3x+4$

$$\frac{4}{25} \times q(x) = \frac{4}{25}x^2 + \frac{24}{25}x + \frac{28}{25}$$

$$
\begin{array}{r|l}
 & \frac{1}{5}x + 4/25 \quad \leftarrow s(x) \\
\hline
5x^2+6x+7 & \cancel{x^3} + 2x^2 + 3x + 4 \\
(-) & \cancel{x^3} \; (-)\; \frac{6}{5}x^2 \; (-)\; \frac{7}{5}x \\
\hline
 & \cancel{\frac{4}{5}x^2} + \frac{8}{5}x + 4 \\
(-) & \cancel{\frac{4}{5}x^2} \; (-)\; \frac{24}{25}x \; (-)\; \frac{28}{25} \\
\hline
 & \frac{16}{25}x + \frac{72}{25} \quad \leftarrow r(x)
\end{array}
$$

The last line is now a linear equation, so of smaller degree than quadratic $q(x)$.

This process tells us that

$$x^2 + 2x^2 + 3x + 4 = \left(5x^2+6x+7\right)\left(\frac{1}{5}x + \frac{4}{25}\right) + \left(\frac{16}{25}x + \frac{72}{25}\right)$$

So

$$s(x) = \frac{1}{5}x + \frac{4}{25} \qquad r(x) = \frac{16}{25} + \frac{72}{25}$$

Example: $p(x) = 2x^3 + 5x^2 + 4x + 1$

$q(x) = 2x + 1$

long division yields:

$$
\begin{array}{r|l}
 & x^2 + 2x + 1 \\
\hline
2x+1 & 2x^3 + 5x^2 + 4x + 1 \\
 & \underline{(-)\cancel{2x^3} \; (-)x^2} \\
 & \qquad \cancel{4x^2} + 4x \\
 & \qquad \underline{(-)\cancel{4x^2} + 2x\,(-)} \\
 & \qquad\qquad 2x + \cancel{1} \\
 & \qquad\qquad \underline{(-)\cancel{2x} + \cancel{1}\,(-)} \\
 & \qquad\qquad\quad \underline{0}
\end{array}
$$

$\frac{2x^3}{2x} = \underline{x^2}$

$x^2 \times (2x+1) = 2x^3 + x^2$

$\frac{4x^2}{2x} = \underline{2x}$

$2x \times (2x+1) = 4x^2 + 2x$

$\frac{2x}{2x} = \underline{1}$

$1 . (2x+1)$

which says that

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

That is we have partially factored $p(x)$.

<u>Example:</u> $p(x) = x^2 + 1 \quad q(x) = x + 2i$ (complex polynonomials)

<u>Solution:</u>

$$
\begin{array}{r l}
 & \quad x - 2i \\
\cline{2-2}
x + 2i \; \big) & \cancel{x^2} + 0x + 1 \\
 & (-)\cancel{x^2} + 2ix(-) \\
\cline{2-2}
 & \quad \cancel{-2ix} + 1 \\
 & (+)\cancel{-2ix} + 4(-) \\
\cline{2-2}
 & \qquad\quad -3
\end{array}
$$

$$\frac{x^2}{x} = x$$

$$x(x+2i) = x^2 + 2ix$$

$$\frac{-2ix}{x} = -2i$$

$$-2i(x+2i)$$
$$= -2ix + 4$$

So we have

$$x^2 + 1 = (x+2i)(x-2i) - 3$$

GCD of polynomials (say $f(x)$, $g(x)$)

Defn: If p and q are polynomials ($p(x), q(x) \in K[x]$) such that there exists a polynomial s with $p = qs$ then we say q is a factor of p denoted $q(x) | p(x)$

Remark Note that if a polynomial q is a factor of polynomial p then so is the polynomial cq for any $c \in \mathbb{R}$ or $c \in \mathbb{C}$ where c is a constant.

This is different to integer factors

Defn: If p_1 and p_2 are polynomials ($p_1(x), p_2(x) \in K[x]$) and both have a factor of q then we say q is common factor of p_1 and p_2.

Defn: Let $p_1(x)$ and $p_2(x)$ be polynomials, both not 0. i.e. $p_1(x), p_2(x) \in K[x]$.
The polynomial $q(x)$ is the greatest common divisor of $p_1(x)$ and $p_2(x)$ denoted by

$$\gcd(p_1(x), p_2(x)),$$

if and only if, the following conditions hold:

(on next page) ($K = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$)

1) $q(x) \mid p_1(x)$ and $q(x) \mid p_2(x)$

2) if $r(x) \mid p_1(x)$ and $r(x) \mid p_2(x)$ then $r(x) \mid q(x)$

(*1) 3) $q(x)$ is monic

$\hookrightarrow$ ensures uniqueness

$\rightarrow \deg(r(x)) \leq \deg(q(x))$.

So gcd is the common factor with highest possible degree

(*1) Defn: A polynomial p of degree k is monic if and only if $a_k = 1$ where

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + \underbrace{a_k}_{=1} x^k$$

Euclids Algorithm for polynomials.

First we prove the following lemma:

Lemma: Suppose f, g are polynomials with some common factor e and suppose further that

$$f = gs + r.$$

Then e also divides r. In particular

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x))$$

$e | f$ & r and $e | g$ & r

proof: Since e is a factor of f, we can write

$$f = s_1 e \qquad \text{for some polynomial } s_1$$

Similarly since e is a factor of g, we write

$$g = s_2 e \qquad \text{for some polynomial } s_2$$

and

$$s_1, s_2 \in K[x]$$

$$f = gs + r \Rightarrow r = f - sg$$

$$\Rightarrow r = s_1 e - s(s_2 e)$$

$$\Rightarrow r = e(s_1 - s s_2)$$

Therefore $e | r$ as $s_1 - s s_2 \in K[x]$

So any common factor of f and g is a common factor of f and r and g and r

$e | f \,\&\, g \Rightarrow e | f \,\&\, r$ and $e | g \,\&\, r$

In particular

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x))$$

Let $d(x) = \gcd(f(x), g(x))$

Then $d(x) | g(x)$ and $d(x) | r(x)$ & d is monic

Let $\hat{e} | g$ and $\hat{e} | r$. Then we need to show $\hat{e} | d$.

$\hat{e} | g \Rightarrow g = \hat{e}.h_1$ for some polynomial $h_1 \in K[x]$

$\hat{e} | r \Rightarrow r = \hat{e}.h_2$ for some polynomial $h_2 \in K[x]$

$f = s.g + r \Rightarrow f = s.\hat{e}.h_1 + \hat{e}.h_2$

$$\Rightarrow f = \hat{e}(sh_1 + h_2)$$

$sh_1 + h_2 \in K[x]$. Therefore

$$\hat{e} | f$$

So $\hat{e} | f$ and $\hat{e} | g$

and by defn of gcd of polynomials,

$$\hat{e} | d.$$

$\blacksquare$

Euclidean algorithm for polynomials $k[x]$:
($k = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$)

Let $f(x)$ and $g(x) \neq 0$ by polynomials.

Calculate $\gcd(f(x), g(x))$

By division theorem for $k[x]$

- $f(x) = q_0(x)\, g(x) + r_0(x)$ with $\deg r_0 < \deg g$

$\gcd(f(x), g(x)) = \gcd(g(x), r_0(x))$

- $g(x) = q_1(x)\, r_0(x) + r_1(x)$ $\deg r_1 < \deg r_0$

$\gcd(g(x), r_0(x)) = \gcd(r_0(x) + r_1(x))$

- $r_0(x) = q_2(x) r_1(x) + r_2(x)$ $\deg r_2 < \deg r_1$

$\gcd(r_0(x), r_1(x)) = \gcd(r_1(x) + r_2(x))$

$\vdots$

- $r_{n-2}(x) = q_n(x)\, r_{n-1}(x) + r_n(x)$ $\deg_n < \deg r_{n-1}$

$\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$

$$r_{n-1}(x) = q_{n+1}(x)\,r_n(x) + 0$$ → stopping condition

$$\gcd(r_{n-1}, r_n) = \gcd(r_n, 0).$$

The $\gcd(r_n, 0)$ is the <u>monic polynomial derived from r_n</u>.

i.e. $$\gcd(r_n, 0) = \frac{1}{\alpha_k} r_n$$

where $r_n = \alpha_0 + \alpha_1 x^1 + \alpha_2 x^2 + \dots + \alpha_k x^k$

<u>Bezout's thm for polynomials $K[x]$</u>

Let $f(x)$ and $g(x) \neq 0$ be polynomials

If $d(x) = \gcd(f(x), g(x))$ then there exists polynomials $s(x)$ and $t(x)$ s.t

$$d(x) = s(x)f(x) + t(x)g(x)$$

$$d = sf + tg$$

↳ similar process to integers to find f and g.

Roots of Polynomials

Defn: A root $\alpha \in X$ of polynomial $p \in K[x]$ is a number α such that $p(\alpha) = 0 \in X$

i.e. roots of polynomial p are the values of x such that $p(x) = 0$

So

$$\boxed{\alpha \in X \text{ is a root of } p(x) \in K[x] \iff p(\alpha) = 0}$$

X can be a different set to K

Remark: The issue is that X can be different to K

For example

let $p_\pm(x) = x^2 \pm 2 \in \mathbb{Z}[x]$ $\quad (K = \mathbb{Z})$

Take $p_-(x) = x^2 - 2 = 0$

You can only solve this equation in $X = \mathbb{R}$ or $\mathbb{C}$

$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
✗	✗	✓	✓

for $p_-(x)$

X - no solution in set
✓ - solution in set

Similarly

Take $p_+(x) = x^2 + 2 = 0$

You can only solve this equation in $\underline{\underline{X = \mathbb{C}}}$.

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
for $p_+(x)$	X	X	X	✓

$\to \mathbb{Z}[x]$

So this is an integer polynomial with real or complex roots.

In general

$\mathbb{Z}[x]$ with real or complex roots ($x \in \mathbb{R}$ or $x \in \mathbb{C}$) is a really interesting objects.

$\mathbb{Z}[x]$ with $x \in \mathbb{R}$ or $x \in \mathbb{C}$ is the heart of "algebraic numbers."

$\alpha \in \mathbb{C}$ or $\mathbb{R}$ is an "<u>algebraic number</u>" iff ($\Leftrightarrow$)
$\exists\ p(x) \in \mathbb{Z}[x]$ st

$$p(\alpha) = 0$$

If there is no polynomial with integer coefficients
i.e. no $p(x) \in \mathbb{Z}[x]$ s.t $x = \beta$ is a root then
we call β a trancendal number.

i.e.

β is trancendental $\Leftrightarrow \nexists\ p(x) \in \mathbb{Z}$ s.t $p(\beta) = 0$
$(\beta \in \mathbb{R}$ or $\mathbb{C})$

in other words

β is trancendental $\Leftrightarrow \forall\ p(x) \in \mathbb{Z},\ p(\beta) \neq 0$

What is surpring is how few algebraic numbers there are.

↳ There are no more algebraic numbers than there are natural numbers, i.e.

$|A| = |\mathbb{N}|$

set of algebraic numbers.

$\Rightarrow$ set of algebraic numbers are countable.

Roughly: pretty much all complex numbers are trancendental.

Some facts of $\mathbb{A}$:

1) $\mathbb{A}$ is countable

2) The sum, difference, product and quotient of 2 algebraic numbers is algebraic.

3) Any number which can be constructed from any finite combination of sums, differences, products, divisions and taking n^{th} roots where $n \in \mathbb{N}$ is an algebraic number.

Proving a number α is algebraic is straightforward:

__Example:__ show $\alpha = 2 + \sqrt[3]{7} \in \mathbb{A}$

$$\alpha = 2 + \sqrt[3]{7} \Rightarrow \alpha - 2 = \sqrt[3]{7}$$

$$\Rightarrow (\alpha - 2)^3 = 7$$

$$\Rightarrow \alpha^3 + 3\alpha^2(-2) + 3\alpha(4) - 8 = 7$$

$$\Rightarrow \alpha^3 - 6\alpha^2 + 12\alpha - 15 = 0$$

So α is a root of $p(x) = x^3 - 6x^2 + 12x - 15$ hence algebraic.

Lemma: Let $p \in K[x]$ and α be a root of p. Then $\exists$ a polynomial $q \in K[x]$ such that

$$p(x) = (x-\alpha)\,q(x)$$ → factorisation

and $\deg(q) = \deg(p) - 1$

proof: By division thm $\exists$ $q(x)$, $r(x)$ s.t

$$p(x) = (x-\alpha)q(x) + r(x)$$ where

$r(x) = 0$ or $0 \leq \deg(r(x)) < \deg(x-\alpha)$

But $\deg(x-\alpha) = 1 \Rightarrow 0 \leq \deg(r(x)) < 1$

1) So $\deg(r(x)) = 0 \Rightarrow r(x) = c$ (c is a constant)

2) or $r(x) = 0$

Case 1) if $r(x) = 0$, then $p(x) = (x-\alpha)q(x)$

↳ and we are done

Case 2: $r(x) \neq 0, \quad \deg(r(x)) = 0$

Then $\exists\, c$ st $r(x) = c \quad \forall x, \quad c \neq 0$

$p(\alpha) = 0$ as α is a root

So

$$p(\alpha) = (\alpha - \alpha)\, q(x) + \underset{\neq 0}{c} = 0$$

$$\Rightarrow \quad p(\alpha) = 0 = c \neq 0$$

contradiction, so case 2 is <u>not</u> possible

Thus we must have $r(x) \neq 0$

So

$$p(x) = q(x)(x - \alpha)$$

$$\blacksquare$$

$p \in K[x]$ where $K = \mathbb{R}$ or $\mathbb{C}$

Theorem: A real or complex polynomial of degree n has at most n roots.

proof. (by mathematical induction):

Suppose α is a root of $p(x)$. By division thm: $\exists$ polynomials $q(x)$ and $r(x) \in K[x]$ s.t

$$p(x) = q(x)(x-\alpha) + r(x)$$

$r(x)$ has degree $0 \leq \deg(r(x)) \leq (x-\alpha)$

$r(x) = 0$ or $0 \leq \deg(r(x)) < \deg(x-\alpha)$

But $\deg(x-\alpha) = 1 \Rightarrow 0 \leq \deg(r(x)) < 1$

1) So $\deg(r(x)) = 0 \Rightarrow r(x) = c$ (c is a constant)

2 or $r(x) = 0$

Case 1) if $r(x) = 0$, then $p(x) = (x-\alpha)q(x)$

↳ and we are done

<u>Case 2</u>: $r(x) \neq 0$, $\deg(r(x)) = 0$

Then $\exists\, c$ st $r(x) = c$ $\forall x$, $c \neq 0$

$p(\alpha) = 0$ as α is a root

So

$$p(\alpha) = (\alpha - \alpha)\, q(x) + \underset{\neq 0}{c} = 0$$

$$\Rightarrow p(\alpha) = 0 = c \neq 0$$

contradiction, so case 2 is <u>not</u> possible

Thus we must have $r(x) \neq 0$

So

$$p(x) = q(x)\,(x - \alpha)$$

Now we show statement by <u>induction</u> on <u>degree</u> <u>n</u> of polynomial $p(x)$

<u>Base cases</u>: $n=0$, $n=1$

If $n=0$: then $p(x) = p_0$ is a constant and so has no roots.

If $n=1$ then $p(x) = p_0 + p_1 x^1$ has exactly <u>one</u> root $-\frac{p_0}{p}$

$$p(-p_0/p) = p_0 + \cancel{p_1}\left(\frac{-p_0}{\cancel{p_1}}\right)$$
$$= p_0 - p_0 = 0$$

<u>Inductive hypothesis</u>:

Suppose the statement holds for polynomials of degree $n=k$

<u>Inductive step</u>:
Show that if polynomials hold for degree $n=k$ then it holds for $n=k+1$:

If $p(x)$ has no roots, we are good as $0 \leq k+1$.

Suppose $p(x)$ has a root α.

By the previous argument:

$$p(x) = (x-\alpha)q(x).$$

with $q(x)$ of polynomial degree k.
Further roots of $q(x)$ have to be roots of $p(x)$

So

$$\{\text{roots of } p(x)\} = \{\alpha\} \cup \{\text{roots of } q(x)\}$$

By inductive hypothesis, $q(x)$ has at most k roots since $\deg(q(x)) = q$.
So $p(x)$ must have at most

$$|\{\alpha\}| + |\{\text{roots of } q(x)\}$$

$= 1 + k = k+1$ roots $\Rightarrow$ $p(x)$ has at most $k+1$ roots

So by induction principle, property holds for polynomials of degree $n \geq 0$ ∎

Fundemental Theorem of Algebra

Theorem: (Fundemental Theorem of Algebra):

A degree n polynomial in $\mathbb{C}[x]$ has exactly n, not necessarily distinct complex roots