Roots of a polynomial

Definition 42. Let $P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$ is said to be a root of P if and only if $P(\alpha) = 0$

Proposition 4. $(X - \alpha)$ divisor of $P \Leftrightarrow P(\alpha) = 0$

Theorem 11. Let $P \in \mathbb{K}_n[X]$ with $P(X) = a_0 + a_1X^1 + \cdots + a_{n-1}X^{n-1} + a_nX^n$ and $\alpha = \dfrac{a}{b} \in \mathbb{Q}$ with $a \wedge b = 1$

$$P(\alpha) = 0 \Rightarrow a|a_0 \text{ and } b|a_n$$

Proof. $P\left(\dfrac{a}{b}\right) = 0 \Rightarrow a_0 + a_1\left(\dfrac{a}{b}\right) + \cdots + a_{n-1}\left(\dfrac{a}{b}\right)^{n-1} + a_n\left(\dfrac{a}{b}\right)^n = 0$

Multiplying both sides by b^n, we get:

$a_0b^n + a_1ab^{n-1} + \cdots + a_{n-1}a^{n-1}b + a_na^n = 0$

$\Rightarrow a_0b^n = -(a_1ab^{n-1} + \cdots + a_{n-1}a^{n-1}b + a_na^n)$

$\qquad = -a(a_1b^{n-1} + \cdots + a_{n-1}a^{n-2}b + a_na^{n-1})$

a divides a_0b^n and $a \wedge b = 1$, thus a divides a_0.

On the other hand,

$a_na^n = -(a_0b^n + a_1ab^{n-1} + \cdots + a_{n-1}a^{n-1}b + a_na^n) = -b(a_0b^{n-1} + a_1ab^{n-2} + \cdots + a_{n-1}a^{n-1})$

b divides a_na^n and $a \wedge b = 1$, thus b divides a_n.

$\square$

Example 34. $P(X) = X^4 + X^3 - X^2 + X - 2$

Let $\alpha = a/b$ be a potential root of P. Then,

a divides $a_0 \Rightarrow a$ divides -2

b divides $a_4 \Rightarrow b$ divides 1

We choose $a = 1$ and $b = 1 \Rightarrow \alpha = 1$

We choose $a = -2$ and $b = 1 \Rightarrow \alpha = -2$

$P(1) = P(-2) = 0$

$Q(X) = 2X^3 - 3X^2 + 3X - 1$

Let $\alpha = a/b$ be a potential root of P. Then,

a divides $a_0 \Rightarrow a$ divides -1

b divides $a_3 \Rightarrow b$ divides 2

We choose $a = 1$ and $b = 2 \Rightarrow \alpha = \dfrac{1}{2}$

$P\left(\dfrac{1}{2}\right) = 0$

Root multiplicity

Proposition 5. $(X - \alpha)^m$ is a divisor of $P \Leftrightarrow \left[P(\alpha) = P^{(1)}(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0\right]$

Example 35. $P(X) = (X + 1)^2(X - 2) = X^3 - 3X - 2$

$P(-1) = 0 \quad P^{(1)}(-1) = 3(-1)^2 - 3 = 0$

We conclude that $(X + 1)^2$ divides P.

Definition 43. Let $P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$ and $m \in \mathbb{N}^*$

If $(X - \alpha)^m$ divides P and $(X - \alpha)^{m+1}$ is not a divisor of P, we say that α is a root of multiplicity m and we denote $mult(\alpha) = m$

Theorem 12. $mult(\alpha) = m \Leftrightarrow P(\alpha) = P^{(1)}(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ and $P^{(m)}(\alpha) \neq 0$

Example 36. $P(X) = (X+1)^2(X-2) = X^3 - 3X - 2 \qquad mult(-1) = 2 \quad mult(2) = 1$
$P(-1) = 0 \quad P^{(1)}(-1) = 3(-1)^2 - 3 = 0 \quad P^{(2)}(-1) = 6(-1) \neq 0$
We conclude that $\alpha = -1$ is a root of multiplicity 2

Theorem 13. All roots of Q (counted with their multiplicity) are also roots of $P \Leftrightarrow Q|P$

Example 37. Let $P(X) = X^{2n+1} + 1 \quad Q(X) = X + 1 \quad S(X) = (X+1)^2$
$Q(-1) = 0 \quad P(-1) = 0 \Rightarrow Q|P$
$P'(X) = (2n+1)X^{2n} \Rightarrow P'(-1) = (2n+1)(-1)^{2n} = 2n + 1 \neq 0 \Rightarrow S$ is not a divisor of P

Factorization for polynomials

Definition 44. A non-constant polynomial $P \in \mathbb{K}[X]$ is said to be irreducible if and only if it cannot be expressed as a product of two polynomials of lower degree.

remark

1. In $\mathbb{R}[X]$, irreducible polynomials are polynomials of degree 1 and polynomials of degree 2 with $\Delta < 0$.
2. In $\mathbb{C}[X]$, the only irreducible polynomials are polynomials of degree 1.

Example 38. $P(X) = X^2 + 1 \quad P$ is irreducible on $\mathbb{R}[X]$ and not in $\mathbb{C}[X]$

Theorem 14. Every polynomial P of $\mathbb{K}[X]$ is either irreducible or can be uniquely expressed as a product of irreducible polynomials of $\mathbb{K}[X]$.
This process is called **factorization** of P

remark

$$P \in \mathbb{C}[X] \Rightarrow P(X) = \lambda(X - a_1)^{n_1}(X - a_2)^{n_2} \cdots (X - a_k)^{n_p}$$

$P \in \mathbb{R}[X] \Rightarrow P(X) = \lambda(X - a_1)^{n_1}(X - a_2)^{n_2} \cdots (X - a_k)^{n_p}(X^2 + b_1X + c_1)^{k_1}$
$(X^2 + b_2X + c_2)^{k_2} \cdots (X^2 + b_qX + c_q)^{k_q}$ with $\Delta_i = b_i^2 - 4c_i < 0$

Example 39. $P(X) = X^3 - X^2 + X - 1$
First, we factorize P on $\mathbb{R}[X]$.
$P(1) = 0 \Rightarrow (X - 1)$ divides P

$$\begin{array}{rrrr|l} X^3 & -X^2 & +X & -1 & X-1 \\ \cline{5-5} X^3 & -X^2 & & & X^2+1 \\ \hline & & X & -1 & \\ & & X & -1 & \\ \cline{3-4} & & & 0 & \end{array}$$

$P(X) = (X-1)(X^2+1)$
Let us now factorize P on $\mathbb{C}[X]$, in fact we still have to factorize $X^2 + 1$
$X^2 + 1 = 0 \Rightarrow X^2 = -1 \Rightarrow X = i$ ou $X = -i \Rightarrow X^2 + 1 = (X+i)(X-i)$
$P(X) = (X-1)(X+i)(X-i)$

Example 40. $P(X) = X^4 + 1$

First, we factorize P on $\mathbb{R}[X]$.

$P(X) = X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + 1)^2 - 2X^2$

$\boxed{P(X) = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)}$

Now, we factorize P on $\mathbb{C}[X]$.

$\Delta_1 = 2 - 4 = 2i^2 \Rightarrow \alpha_1 = \dfrac{-\sqrt{2} + \sqrt{2}i}{2} \qquad \alpha_2 = \dfrac{-\sqrt{2} - \sqrt{2}i}{2}$

$\Delta_2 = 2 - 4 = 2i^2 \Rightarrow \alpha_3 = \dfrac{\sqrt{2} + \sqrt{2}i}{2} \qquad \alpha_4 = \dfrac{\sqrt{2} - \sqrt{2}i}{2}$

$$P(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$$

$$P(X) = \left(X + \frac{\sqrt{2} - \sqrt{2}i}{2}\right)\left(X + \frac{\sqrt{2} + \sqrt{2}i}{2}\right)\left(X - \frac{\sqrt{2} + \sqrt{2}i}{2}\right)\left(X - \frac{\sqrt{2} - \sqrt{2}i}{2}\right)$$

Definition 45. A polynomial $P \in \mathbb{K}[X]$ is said to split over the field $\mathbb{K}$ if:

$$P(X) = \alpha \prod (X - x_i), \text{ with } \alpha, x_i \in \mathbb{K}$$

Example 41. $X^4 + 1$ splits over $\mathbb{C}$ but does not split over $\mathbb{R}$.