Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geqslant 1$ has at most n roots.

Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots.

Proof by induction on n

Base Case: If $n=1$ ie polynomials of the form $ax-b$ have at most a root over $\mathbb{F}$, with $a \neq 0$. Root is $x = b/a$.

IH: Assume $P(k)$ is true for some $k \in \mathbb{N}$

I Step: Let $p(x) \in \mathbb{F}[x]$ of degree $k+1$. Either $p(x)$ has no root ✓ OR $p(x)$ has a root $c \in \mathbb{F}$. By FT, $x-c$ is a factor of $p(x)$. Write $p(x) = (x-c)\,q(x)$ for some $q(x) \in \mathbb{F}[x]$ of degree k. By IH, $q(x)$ has at most k roots. So $p(x)$ has at most $k+1$ root

L42P7

$\therefore$ by POMI, $P(n)$ is true $\forall n \in \mathbb{N}$. $\square$

Ex: Factor $f(x) = x^4 - 2x^3 + 3x^2 - 4x + 2$ over $\mathbb{Z}_7$.

Pf: Note $f(1) = 0$ thus by FT $x-1$ is a factor. By long division,

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

Now, the sum of the coefficients of the cubic is still 0 hence $x-1$ is another root of $f(x)$! By long division

$$f(x) = (x-1)^2(x^2+2)$$

Factor theorem says if x^2+2 could be factored, it must have a root since the factors must be linear.

x	0	1	2	3	4	5	6
$x^2+2 \bmod 7$	2	3	6	4	4	6	3

The table shows x^2+2 has no root.

Def'n: The multiplicity of a root $c \in \mathbb{F}$ of $f(x) \in \mathbb{F}[x]$ is the largest $k \in \mathbb{Z}$ s.t. $(x-c)^k$ is a factor of $f(x)$.

Ex: The multiplicity of 1 in the last example was 2.

Note: $x^4 + 2x^2 + 1 = (x^2+1)^2$ over $\mathbb{R}[x]$

BUT does not split into linear factors over

Fundamental Theorem of Algebra

Every non-constant complex polynomial has a complex root.

Notes: Roots need not be distinct.

- x^2+1 over $\mathbb{R}$ shows this does not happen over all fields.

Pf: $\boxtimes$

Solve: $x^3-x^2+x-1=0$ over $\mathbb{C}$.

Note $x-1$ is a factor. Either do long division or note:

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

Factor $iz^3 + (3-i)z^2 + (-3-2i)z - 6$ as a product of linear factors. Hint: There is an easy to find integer root!

Note $z=-1$ & $z=2$ are roots!

Hence $(z+1)(z-2)$ is a factor

$= z^2 - z - 2$

$f(z)$

$$\begin{array}{r|l} & iz+3 \\ \hline z^2-z-2 & iz^3+(3-i)z^2+(-3-2i)z-6 \\ & \underline{iz^3 - iz^2 - 2iz} \\ & \qquad 3z^2 - 3z - 6 \\ & \qquad \underline{3z^2 - 3z - 6} \\ & \qquad\qquad R\ 0 \end{array}$$

$\therefore f(z) = (z+1)(z-2)(iz+3)$.

(CPN) Complex Polynomials of Degree n Have n Roots.

A complex polynomial $f(z)$ of degree $n \geq 1$ can be written as

$$f(z) = c(z-c_1)(z-c_2)\cdots(z-c_n)$$

for some $c \in \mathbb{C}$, for $c_1, c_2, \ldots c_n \in \mathbb{C}$. (not necessarily distinct) roots of $f(z)$

Ex: $2z^7 + z^5 + iz + 7$ can be written as

$$2(z-z_1)(z-z_2)\cdots(z-z_7)$$

for roots $z_1, z_2, \ldots, z_7 \in \mathbb{C}$.

Note: Factorization depends on the field!

Eg: $\mathbb{C}$: $(z-i)(z+i)(z-\sqrt{2})(z+\sqrt{2})(z-1)$

$\mathbb{R}$: $(z^2+1)(z-\sqrt{2})(z+\sqrt{2})(z-1)$

$\mathbb{Q}$: $(z^2+1)(z^2-2)(z-1)$

Pf of CPN: We prove the given statement by induction

Base Case: $n=1$ take $az+b \in \mathbb{C}[z]$ rewrite as $a(z-(\frac{-b}{a}))$

IH: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form. (for some $k \in \mathbb{N}$).

IStep: Take $f(z) \in \mathbb{C}[z]$ of degree $k+1$. By FTA & FT, $z-c_{k+1}$ is a factor of $f(z)$ for some $c_{k+1} \in \mathbb{C}$. Write

$$f(z) = (z-c_{k+1})\, g(z)$$

where degree $g(z)$ is k. By IH, write $g(z) = c(z-c_1)(z-c_2)\cdots(z-c_k)$ for $c, c_1, c_2, \ldots c_k \in \mathbb{C}$. Combine toget

$$f(z) = c\prod_{i=1}^{k+1}(z-c_i).$$

$\therefore$ by POMI, the given statement is true $\forall n \in \mathbb{N}$.