Last time we discussed Laplace's (Tricky) proof of the F.T.A. There were two major gaps:

(1) Given $f(x) \in \mathbb{R}[x]$, the proof assumes existence of a field $\mathbb{F} \supseteq \mathbb{C}$ and elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

i.e. it assumes $f(x)$ has all of its roots somewhere ----.

This was only proved in 1880s. We'll discuss it later.

(2) Given a symmetric expression of the roots & real numbers:

$$S(x_1, \dots, x_n) = \mathbb{R}[x_1, \dots, x_n]$$

Say S is "symmetric" if for all $i<j$ we have

$$S(\ldots, x_i, \ldots, x_j, \ldots) = S(\ldots, x_j, \ldots, x_i, \ldots)$$

Example: $S(x_1, \ldots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$ is symmetric.

Then I claim that

$S(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}$!

S evaluated at the roots.

Amazing.

We will prove (2) today.

Definition: Suppose

$$x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n$$
$$= (x - r_1)(x - r_2) \cdots (x - r_n)$$

for some $e_1, \ldots, e_n, r_1, \ldots, r_n$ living in some field.

Expand both sides, equate coefficients:

$$e_1 = r_1 + r_2 + \cdots + r_n = \sum_i r_i$$

$$e_2 = r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n = \sum_{i<j} r_i r_j$$

$$e_3 = r_1 r_2 r_3 + \cdots + r_{n-2} r_{n-1} r_n = \sum_{i<j<k} r_i r_j r_k$$

$$\vdots$$

$$e_n = r_1 r_2 \cdots r_n$$

Observe: Each e_k is a symmetric function of the roots.

Proof: For any $i<j$,

$$(x-r_1)\cdots(x-r_i)\cdots(x-r_j)\cdots(x-r_n)$$

$$= (x-r_1)\cdots(x-r_j)\cdots(x-r_i)\cdots(x-r_n)$$

Expand and compare coefficients. QED.

Jargon: $e_1, \ldots, e_n$ are the "elementary symmetric functions" of $r_1, \ldots, r_n$.

General Claim: Any symmetric function of $r_1, \ldots, r_n$ can be expressed as a (not necessarily symmetric)

function of $e_1, \ldots, e_n$.

Application: If $f(x) \in \mathbb{R}[x]$ and

$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

for some $\alpha_1, \ldots, \alpha_n \in \mathbb{F} \supseteq \mathbb{C}$.

Then any symmetric combination of $\alpha_1, \ldots, \alpha_n$ & real numbers is a real function of the coefficients, hence is in $\mathbb{R}$.

This is why we care.

Example:

$$x^2 - e_1 x + e_2 = (x - r_1)(x - r_2)$$

$$\Rightarrow \quad \begin{aligned} e_1 &= r_1 + r_2 \\ e_2 &= r_1 r_2. \end{aligned}$$

Express the symmetric function

$$r_1^3 + r_2^3$$

as some function of e_1 & e_2.

Idea: The only way to obtain the term "r_1^3" is to consider

$$e_1^3 = (r_1+r_2)^3$$

$$= r_1^3 + \text{stuff}.$$

$$= r_1^3 + 3r_1^2 r_2 + 3r_1 r_2^2 + r_2^3.$$

$$= (r_1^3 + r_2^3) + \text{stuff}.$$

$$= (r_1^3 + r_2^3) + 3r_1 r_2 (r_1 + r_2)$$

$$= (r_1^3 + r_2^3) + 3e_2 e_1$$

$$\Rightarrow \quad r_1^3 + r_2^3 = \underbrace{e_1^3 - 3e_1 e_2}_{\text{Some (non-symmetric) function of } e_1 \& e_2} \quad \checkmark$$

Goal: Define an algorithm that works for a general symmetric function.

Here's the statement.

FTSP (Fundamental Theorem of Symmetic Polynomials)

Let $x^n - e_1 x^{n-1} + e_2 x^n \cdots - (-1)^n e_n$
$= (x - r_1) \cdots (x - r_n)$

for some $e_1, \ldots, e_n \in \mathbb{E}$ fields
$r_1, \ldots, r_n \in \mathbb{F} \supseteq \mathbb{E}$.

So $e_k = \sum_{1 \le n_1 < n_2 < \cdots < n_k \le n} r_{n_1} r_{n_2} \cdots r_{n_k} \in \mathbb{E}$.

By convention, say $e_0 = 1$
$e_k = 0$ when $k > n$.

Let $S(x_1, \ldots, x_n) \in \mathbb{E}[x_1, \ldots, x_n]$ be a symmetric polynomial. Then I claim $\exists$ some (possibly non-symmetric) polynomial $N(x_1, \ldots, x_n) \in \mathbb{E}[x_1, \ldots, x_n]$ such that

$$S(r_1, \ldots, r_n) = N(e_1, \ldots, e_n)$$

and hence $S(r_1, \ldots, r_n) \in \mathbb{E}$. ☺

Proof Postponed

Special Case was discovered by Isaac Newton (1666).

Let $p_k = r_1^k + r_2^k + \cdots + r_n^k$

be the kth "power sum symmetric polynomial."

He discovered a formula relating p_i & e_i:

$$p_k = e_1 p_{k-1} + e_2 p_{k-2} + \cdots + e_{k-1} p_1 - k e_k .$$

Assume for induction that $p_1, \ldots, p_{k-1}$ are polynomial expressions of $e_1, \ldots, e_n$, then so is p_k

☺

But he did not state the general FTSP. First stated in the 1770s.

The proof is really an algorithm, called "Waring's Algorithm," similar to long division of polynomials. Each step cancels the "leading term," so we have to define "leading term."

Given monomial $r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$, we define its multidegree:

$$\deg\left(r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}\right) = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$$

the ordered list of exponents

Order multidegrees by dictionary ("lexicographic") order.

$$(0,0,0) < (0,0,1) < (0,0,2) < \cdots < (0,0,57)$$
$$< \cdots < (0,1,0) < (0,1,12)$$
$$< \cdots < (1,0,0) < \text{etc.}$$

For any polynomial $f(x_1, x_2, \ldots, x_n)$

we let

$\deg(f)$ = highest multidegree that occurs in f.

e.g. $\deg\left(2x_2^1 + x_3^2 - x_1^1 x_2^1 x_3^2 + 5x_1^2 x_2\right)$

$(0,1,0)$ $(0,0,2)$ $(1,1,2)$ $(2,1,0)$

$= (2,1,0)$

PAUSE.