Examples of F.T.S.P. :

$$x^2 - e_1 x + e_2 = (x-r)(x-s)$$

$$\begin{cases} e_1 = r+s, \\ e_2 = rs. \end{cases}$$ "elementary symm. functions"

FTSP says <u>any</u> symmetric function of $r$ & $s$ can be expressed as a function of $e_1$ & $e_2$.

e.g. let $\Delta = (r-s)^2$ (the discriminant)

symmetric ✓

Algorithm:

$$\Delta = (r-s)^2 = \underset{(2,0)}{r^2} - \underset{(1,1)}{2rs} + \underset{(0,2)}{s^2}$$

leading term.

$$e_1^2 = (r+s)^2 = r^2 + 2rs + s^2$$

same leading term.

Subtract:

$$\Delta - e_1^2 = \underset{(1,1)}{-4rs}$$

degree of leading term went <u>down</u>!

Repepeat: $-4e_2 = -4rs$ Done ✓

$$\Delta - e_1^2 = -4e_2$$

$$\boxed{\Delta = e_1^2 - 4e_2}$$

That was too easy, so let's consider a cubic polynomial:

$$x^3 - e_1x^2 + e_2x - e_3 = (x-r)(x-s)(x-t)$$

$$\begin{cases} e_1 = r+s+t \\ e_2 = rs + rt + st \\ e_3 = rst \end{cases}$$

By definition, the discriminant is

$$\Delta = (r-s)^2(r-t)^2(s-t)^2.$$

Observe:

- $\Delta = 0 \iff$ repeated root.
- $\Delta$ is symmetric in $r, s, t$.

By FTSP we can express $\Delta$

in terms of coefficients $e_1, e_2, e_3$.

Algorithm:

$$\Delta = (r-s)^2(r-t)^2(s-t)^2$$

$$= \boxed{\begin{matrix} r^4 s^2 \\ (4,2,0) \end{matrix}} + \text{lower terms.}$$

$$(4-2, 2-0, 0) = (2,2,0)$$

$$e_1^2 e_2^2 e_3^0 = (r+s+t)^2 (rs+rt+st)^2$$

$$= r^4 s^2 + \text{lower terms}$$

Cancel (using computer):

$$\Delta - e_1^2 e_2^2 = \boxed{\begin{matrix} -4r^4 st \\ (4,1,1) \end{matrix}} + \text{Lower terms.}$$

$$(4-1, 1-1, 1)$$

$$-4e_1^3 e_2^0 e_3^1 = \boxed{-4r^4 st} + \text{Lower terms.}$$

$$\Delta - e_1^2 e_2^2 - (-4e_1^3 e_3)$$

$$= \text{some symmetric polynomial}$$

in $r, s, t$ with lower degree.

Repeat ...

$$\boxed{\Delta = e_1^2 e_2^2 - 4e_1^3 e_3 - 4e_2^3 + 18 e_1 e_2 e_3 - 27 e_3^2}$$

The discriminant of a cubic.

Please do not memorize!

Easier example on HW5.2.

---

Why do we care?

If $f(x) \in \mathbb{R}[x]$ has roots $r, s, t$ in some field somewhere ...

Then $\Delta = (r-s)^2 (r-t)^2 (s-t)^2$ is a real number!

More generally, any symmetric function of the roots is real!

Application: Laplace's Proof of FTA.

Theorem (FTA):

Every (nonconstant) $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.

Proof: Suppose $\deg(f) = 2^e \cdot m$ where $m \in \mathbb{Z}$ is odd. We will prove the statement by induction on $e$.

Base case: $e = 0$, i.e., $\deg(f) = $ odd.
By I.V.T. $f(x)$ has a real root (hence also a complex root).

Now let $e \geq 1$ and assume for induction that any real poly. of degree $2^{e-1} \cdot$odd has a root in $\mathbb{C}$.

Let $n = \deg(f) = 2^e \cdot m$.
We assume $\exists$ some field $\mathbb{F} \supseteq \mathbb{C}$ and elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that

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

We will show that at least one

root $\alpha_i$ is in $\mathbb{C}$.

TRICK: For any $\lambda \in \mathbb{R}$, $1 \le i < j \le n$, define $\beta_{ij\lambda} = \alpha_i + \alpha_j + \lambda \alpha_i \alpha_j \in \mathbb{F}$, and consider auxiliary polynomial

$$g_\lambda(x) = \prod_{1 \le i < j \le n} (x - \beta_{ij\lambda}) \in \mathbb{F}[x].$$

I claim that in fact

$$g_\lambda(x) \in \underline{\mathbb{R}}[x] \quad !$$

Indeed, each coefficient of $g_\lambda(x)$ is a symmetric function of the $\beta_{ij\lambda}$, hence a symmetric function of $\alpha_i$, hence (by FTSP) a function of the coeffs of $f(x) \in \mathbb{R}[x]$, hence is re<u>al</u>.

(Of course, we would never want to write down the formulas ! )

Next, compute $\deg(g_\lambda)$.

$\deg(g_\lambda) = \#$ pairs $1 \le i < j \le n$

$$= \binom{n}{2} = \frac{n(n-1)}{2}$$

$$= \frac{2^e m (2^e m - 1)}{2}$$

$$= 2^{e-1} [\underbrace{m(2^e m - 1)}_{\text{odd}}]$$

By induction, $g_\lambda(x)$ has at least one complex root.

In other words, given $\lambda \in \mathbb{R}$, $\exists$ some pair $1 \le i < j \le n$ such that

$$\beta_{ij\lambda} = \alpha_i + \alpha_j + \lambda \alpha_i \alpha_j \in \underline{\underline{\mathbb{C}}}$$

Since $\mathbb{R}$ is in<u>fi</u>nite and $\#$ pairs $i<j$ is <u>fini</u>te, $\exists$ $\mu \ne \lambda$ and some $i<j$ such that

$\beta_{ij\lambda}$ & $\beta_{ij\mu}$ are <u>both</u> in $\mathbb{C}$.

So what?

$$\alpha_i + \alpha_j + \lambda \alpha_i \alpha_j \in \mathbb{C}$$
$$\alpha_i + \alpha_j + \mu \alpha_i \alpha_j \in \mathbb{C}$$

Subtract:

$$\lambda \alpha_i \alpha_j - \mu \alpha_i \alpha_j \in \mathbb{C}$$
$$\cancel{(\lambda - \mu)}\, \alpha_i \alpha_j \in \mathbb{C}.$$
$$\alpha_i \alpha_j \in \mathbb{C}$$

$$\Rightarrow \quad \alpha_i + \alpha_j = -\lambda \alpha_i \alpha_j \in \mathbb{C}.$$

Summary: $\alpha_i + \alpha_j \in \mathbb{C}$
$\alpha_i \alpha_j \in \mathbb{C}$

Does this mean that $\alpha_i, \alpha_j \in \mathbb{C}$ ?

Yes. Because $\alpha_i, \alpha_j$ are the roots of the quadratic polynomial

$$(z - \alpha_i)(z - \alpha_j) = z^2 - (\alpha_i + \alpha_j) z + \alpha_i \alpha_j .$$

$$\Rightarrow \quad \alpha_i, \alpha_j = \frac{(\alpha_i + \alpha_j) \pm \sqrt{(\alpha_i + \alpha_j)^2 - 4(\alpha_i \alpha_j)}}{2}$$

Since every complex number has

a complex square root, we conclude that $\alpha_i, \alpha_j \in \mathbb{C}$,

hence $f(x)$ has at least one complex root.

Q.E.D.