HW 5 due Fri

O.H.

Today & Tom. 2:30–4:00.

MATH CLUB TODAY 5 pm !

Now: "Partial Fractions".

We know how to add fractions

$$\frac{r}{p} + \frac{s}{q} = \frac{qr + ps}{pq}$$

But can we "UN-add" them??.

e.g. $\frac{8}{15} = \frac{?}{p} + \frac{?}{q}$ where $pq = 15$

Yes! If we can factor the denominator 15.

$15 = 3 \cdot 5$. prime decomposition.

$$\frac{8}{15} = \frac{?}{3} + \frac{?}{5}$$

Method: Since 3, 5 are primes we can find x, y s.t. $x3 + y5 = 1$.

Do it: $\bar{5} = 1 \cdot \bar{3} + \bar{2}$

$\bar{3} = 1 \cdot \bar{2} + \bar{1}$ $\quad$ $\gcd(3,5) = 1$.

$\bar{2} = 2 \cdot \bar{1} + \bar{0}$

$$\gcd(3,5) = \underline{1} = \bar{3} - 1 \cdot \bar{2}$$
$$= \bar{3} - 1(\bar{5} - 1 \cdot \bar{3})$$
$$= 2 \cdot \bar{3} - 1 \cdot \bar{5}.$$

$$1 = 2 \cdot 3 - 1 \cdot 5.$$

NOT unique.

$$(2+5k)3 + (-1+3k)5$$
$$= (2 \cdot 3 - 1 \cdot 5) + \cancel{3 \cdot 5k} - \cancel{3 \cdot 5 \cdot k}$$
$$= \underline{1} \quad \text{for any } k \in \mathbb{Z}$$

Divide by 15 to get.

$$\frac{1}{15} = \frac{2 \cdot 3}{15} - \frac{1 \cdot 5}{15} = \frac{2}{5} - \frac{1}{3}$$

Multiply by 8 to get

$$\underbrace{\frac{8}{15} = \frac{16}{5} - \frac{8}{3}}_{\text{a "partial fraction" decomposition.}} \quad \checkmark$$

We can do the same for polynomials.

Given $p(x), q(x) \in \mathbb{F}[x]$ we say

$\frac{p(x)}{q(x)}$ is a rational function of x

e.g. $\frac{3x^2+7}{x^3-x^2+4x-4} \in \mathbb{Q}(x)$

round brackets for rat. funcs.

Theorem (Partial fractions).

Let $\frac{p(x)}{q(x)} \in \mathbb{F}(x)$ and suppose

$$q(x) = \varphi_1(x)^{n_1} \varphi_2(x)^{n_2} \cdots \varphi_k(x)^{n_k}$$

is the prime decomp. of $q(x) \in \mathbb{F}[x]$.

Then $\exists!$ (there exist unique) polys.

$\beta(x), \alpha_{ij}(x) \in \mathbb{F}[x]$ such that

$$p(x)/q(x) = \beta(x)$$
$$+ \left(\frac{\alpha_{11}(x)}{\varphi_1(x)} + \frac{\alpha_{12}(x)}{\varphi_1(x)^2} + \cdots + \frac{\alpha_{1n_1}(x)}{\varphi_1(x)^{n_1}} \right)$$

the partial fraction decomp. $\longrightarrow$

$$+ \left(\frac{\alpha_{21}(x)}{\varphi_2(x)} + \frac{\alpha_{22}(x)}{\varphi_2(x)^2} + \cdots + \frac{\alpha_{2n_2}(x)}{\varphi_2(x)^{n_2}} \right)$$
$$\vdots$$
$$+ \left(\frac{\alpha_{k1}(x)}{\varphi_k(x)} + \cdots + \frac{\alpha_{kn_k}(x)}{\varphi_k(x)^{n_k}} \right)$$

where $\deg \alpha_{ij} < \deg \varphi_i$ OR $\alpha_{ij} = $ "0"

$\forall i, j$.

///.

Proof? ... just a sketch.
it uses Euclidean Algorithm.

Let $\dfrac{p(x)}{q(x)} = \dfrac{p(x)}{\varphi_1(x)\varphi_2(x)}$

where $\varphi_1(x) \neq \varphi_2(x)$ are "prime".

i.e. $\gcd(\varphi_1(x), \varphi_2(x)) = 1$ so.

$\exists.\ A(x), B(x) \in \mathbb{F}[x]$ s.t.

$$1 = A(x)\varphi_1(x) + B(x)\varphi_2(x).$$

Divide by $q(x) = \varphi_1(x)\varphi_2(x)$ to get,

$$\frac{1}{\varphi_1\varphi_2} = \frac{A\cancel{\varphi_1}}{\cancel{\varphi_1}\varphi_2} + \frac{B\varphi_2}{\varphi_1\varphi_2}$$

$$\frac{1}{q} = \frac{A}{\varphi_2} + \frac{B}{\varphi_1}$$

$$\frac{p(x)}{q(x)} = \frac{p(x)A(x)}{\varphi_2(x)} + \frac{p(x)B(x)}{\varphi_1(x)}.$$

then use long division.

$$= R(x) + \frac{\alpha_{11}(x)}{\varphi_1(x)} + \frac{\alpha_{21}(x)}{\varphi_2(x)}.$$

///

eg. $\dfrac{3x^2+7}{x^3-x^2+4x-4}$.

Step 1: Factor the denominator. (sometimes HARD!)

$$x^3-x^2+4x-4 = (x-1)(x^2+4).$$

both prime over $\mathbb{Q}$.

Step 2: Theorem says $\exists!$ $A, B, C \in \mathbb{Q}$ s.t.

$$\frac{3x^2+7}{(x-1)(x^2+4)} = \frac{A}{(x-1)} + \frac{Bx+C}{(x^2+4)}.$$

Step 3: Find A, B, C.

$$\frac{3x^2+7}{(x-1)(x^2+4)} = \frac{A(x^2+4)+(Bx+C)(x-1)}{(x-1)(x^2+4)}.$$

Equate numerators

$$3x^2+7 = A(x^2+4)+(Bx+C)(x-1).$$

Put $x=1$ to get

$$3+7 = A\cdot 5 + 0.$$
$$10 = 5A \implies A=2.$$

So... $3x^2+7 = 2(x^2+4) + (Bx+C)(x-1)$.

$$= 2x^2 + 8 + Bx^2 + Cx - Bx - C.$$

$$3x^2 + 0x + 7. = (2+B)x^2 + (C-B)x + (8-C)$$

Equate coefficients

$$\left.\begin{aligned} 3 &= 2+B \\ 0 &= B-C \\ 7 &= 8-C \end{aligned}\right\} \Longrightarrow \begin{aligned} B&=1 \\ C&=1. \end{aligned}$$

Conclusion.

$$\boxed{\frac{3x^2+7}{(x-1)(x^2+4)} = \frac{2}{(x-1)} + \frac{x+1}{(x^2+4)}} \qquad \blacksquare$$

WHO CARES ?

Remark: "We" know how to integrate

$$\int \frac{1}{x-a}\,dx \qquad a \in \mathbb{R} \to \ln|x-a|$$

$$\int \frac{1}{x^2+b^2}\,dx \qquad b \in \mathbb{R}. \to \frac{1}{b}\tan^{-1}\left(\frac{x}{b}\right)$$

$$\int \frac{x}{x^2+c^2}\,dx \qquad c \in \mathbb{R}. \to \frac{1}{2}\ln(x^2+a^2)$$

HW 6 due Fri Apr 22
Exam 3 Fri Apr 29.

Today: HW 5 Solutions

Thm: Compute $\displaystyle\int \frac{3x^2+7}{(x-1)(x^2+4)}\,dx$

$(x-1)$ and (x^2+4) are coprime.

$$\begin{array}{r|l} & x+1 \\ x-1 & x^2+4 \\ & \underline{x^2-x} \\ & x+4 \\ & \underline{x-1} \\ & 5 \end{array}$$

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

$$\Longrightarrow 1 = -\frac{(x+1)}{5}(x-1) + \frac{x^2+4}{5}$$

$$\frac{1}{(x-1)(x^2+4)} = -\frac{(x+1)}{5}\frac{1}{x^2+4} + \frac{1}{5}\frac{1}{x-1}$$

$$\frac{3x^2+7}{(x-1)(x^2+4)} = -\frac{(x+1)(3x^2+7)}{5}$$

HW 6 due Fri Apr 22

Exam 3 Fri Apr 29.

Today: HW 5 solutions

Then: Compute $\int \frac{1}{(x-1)(x^2+4)}\,dx$.

$(x-1)$ & (x^2+4) are coprime:

$$\begin{array}{r|l} & x+1 \\ \hline x-1 & x^2+4 \\ & \underline{x^2-x} \\ & \quad x+4 \\ & \quad \underline{x-1} \\ & \qquad 5 \end{array}$$

$$x^2+4 = (x+1)(x-1) + \overline{5}.$$

$$\overline{5} = 1(x^2+4) - (x+1)(x-1)$$

$\boxed{\text{coprime}}$ $$1 = \frac{1}{5}\overline{(x^2+4)} - \frac{x+1}{5}\overline{(x-1)}$$

Divide by $(x-1)(x^2+4)$ to get

$$\frac{1}{(x-1)(x^2+4)} = \frac{1}{5}\frac{1}{(x-1)} - \frac{x+1}{5(x^2+4)}.$$

partial fractions

Now we can integrate.

Note. $\int \frac{1}{x-1}\,dx = \ln|x-1|$

$$\int \frac{1}{x^2+4}\,dx \qquad \begin{array}{l} x = 2u \\ dx = 2du. \end{array}$$

$$= \int \frac{1}{4u^2+4}\,2du.$$

$$= \frac{1}{2}\int \frac{1}{u^2+1}\,du.$$

$$= \frac{1}{2}\arctan(u).$$

$$= \frac{1}{2}\arctan\left(\frac{x}{2}\right).$$

$$\int \frac{x}{x^2+4}\,dx \qquad \begin{array}{l} u = x^2+4 \\ du = 2x\,dx. \end{array}$$

$$= \frac{1}{2}\int \frac{1}{u}\,du = \frac{1}{2}\ln|u|$$

$$= \frac{1}{2}\ln(x^2+4).$$

Finally

$$\int \frac{1}{(x-1)(x^2+4)}\,dx = \frac{1}{5}\int \frac{1}{x-1}\,dx - \frac{1}{5}\int \frac{1}{x^2+4}\,dx - \frac{1}{5}\int \frac{x}{x^2+4}\,dx$$

$$= \frac{1}{5}\left(\ln|x-1| + \frac{1}{2}\arctan\left(\frac{x}{2}\right) + \frac{1}{2}\ln(x^2+4)\right)$$

HW 6 due Fri Apr 22
Exam 3 Fri Apr 29.

Today: $\mathbb{R}$FTA.

Theorem (Euler, etc....)

Every $f(x) \in \mathbb{R}[x]$ can be factored into deg 1 and deg 2 polynomials.

Equivalently, if $f(x) \in \mathbb{R}[x]$ is irreducible ("prime") over $\mathbb{R}$ then $\deg(f) = 1$ or 2.

Why did he care?

He wanted to integrate

$$\int \frac{p(x)}{q(x)}\,dx \quad \text{where } p(x), q(x) \in \mathbb{R}[x].$$

If $q(x)$ has deg 1 & 2 factors, this can be done through partial fractions

eg. Last Time we computed

$$\int$$

$$\int \frac{1}{(x-1)(x^2+4)}\,dx$$

$$= \frac{1}{5}\left[\ln|x-1| + \frac{1}{2}\arctan\left(\frac{x}{2}\right) + \frac{1}{2}\ln(x^2+4) \right]$$

Hence

$\mathbb{R}$FTA $\Longrightarrow$ all $\frac{p(x)}{q(x)} \in \mathbb{R}(x)$ can be integrated.

~~(in terms of ln, arctan, etc...)~~

How did he do it?

Let's see...

Start with $\deg(f) = 1$

~~If $f(x) = ax + b$, $a, b \in \mathbb{R}$, DONE.~~

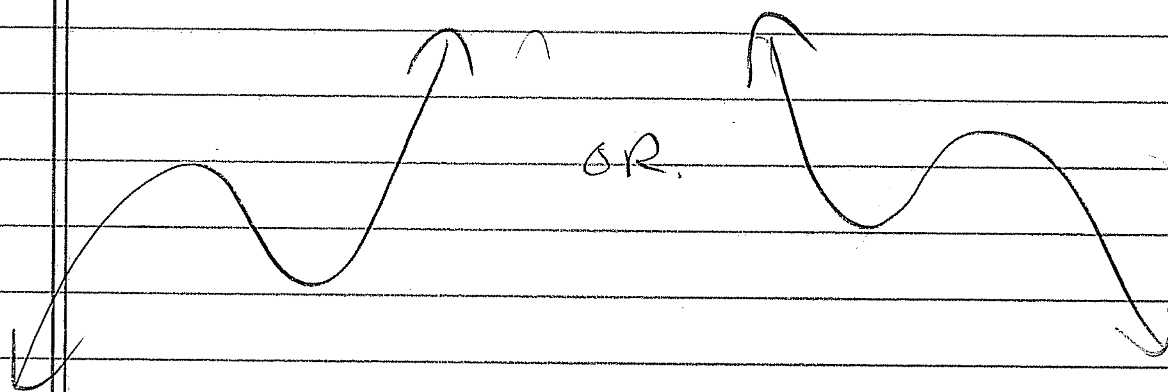
~~$f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{R}$, DONE.~~

Let $f(x) \in \mathbb{R}[x]$ and try to factor.

If $\deg(f) = 1$ or 2, nothing to do.

So sp. $\deg(f) = 3$.

Graph of f looks like:



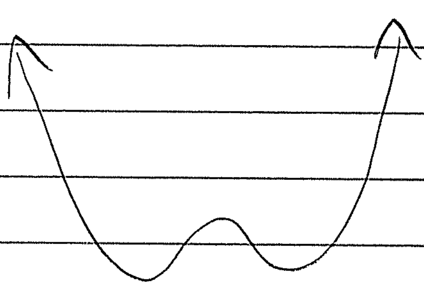
In either case IVT $\Rightarrow$ $\exists$ real root $f(r) = 0$.

Then use Factor Theorem to get

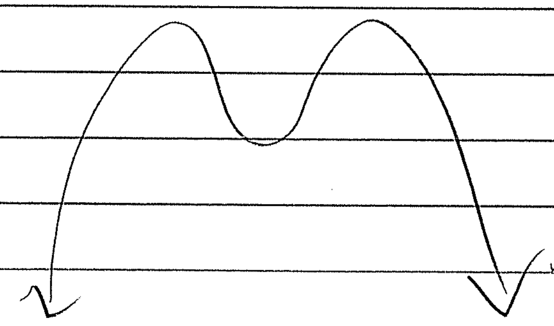
$$f(x) = (x-r)g(x), \quad g \in \mathbb{R}[x], \ \deg(g) = 2$$

Next Case: $\deg(f) = 4$.

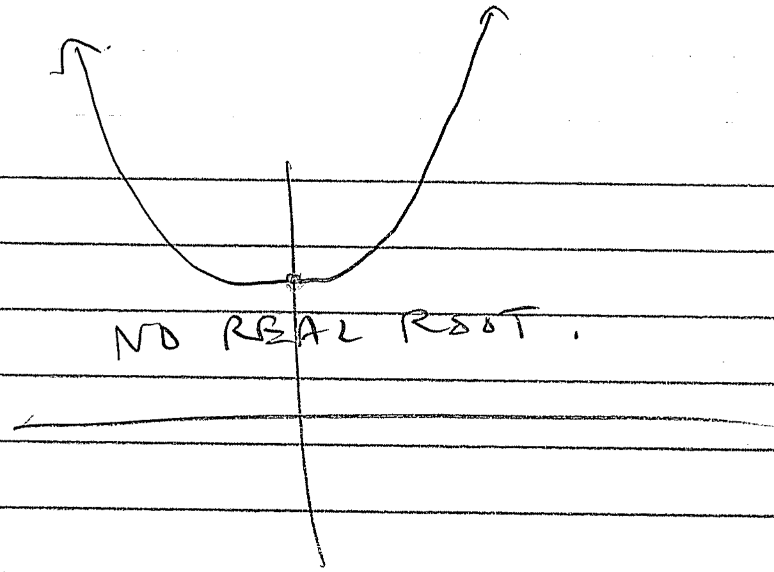
Looks like



Maybe it has NO REAL ROOTS.



Eg. x^4+4.



But it still factors
$$(x^4+4) = (x^2-2x+2)(x^2+2x+2)$$

Sometimes it's much harder

eg. $f(x) = x^4 - 4x^3 + 2x^2 + 4x + 4$.

$$= \left(x^2 - \left(2+\sqrt{2\sqrt{7}+4}\,\right)x \;\cdots\cdots\right) \text{ etc.}$$

Bernoulli $\to$ Euler
No Yes!

Is there a general method?

Theorem (Euler)
Every $f(x) \in \mathbb{R}[x]$, $\deg(f) = 4$
factors into 2 real quadratics. ///.

Proof...
We may assume
$$f(x) = x^4 + Bx^2 + Cx + D \qquad \text{(Why?)}$$

Now we are looking for Real u, α, β.
where

$$x^4 + Bx^2 + Cx + D = (x^2 + ux + \alpha)(x^2 - ux + \beta)$$

$$= x^4 + (u-u)x^3 + (\alpha - u^2 + \beta)x^2 + (u\beta - u\alpha)x + \alpha\beta.$$

Equate Coeffs:

$$B = \alpha + \beta - u^2, \quad C = u(\beta - \alpha), \quad D = \alpha\beta.$$

Hence

$$\text{(1)} \quad \alpha + \beta = B + u^2$$
$$\text{(2)} \quad \beta - \alpha = C/u.$$

$$\text{(1)} + \text{(2)} \Rightarrow 2\beta = u^2 + B + \frac{C}{u}$$

$$\text{(1)} - \text{(2)} \Rightarrow 2\alpha = u^2 + B - \frac{C}{u}.$$

Then $D = \alpha\beta \Rightarrow$

$$4D = 2\alpha 2\beta = \left(u^2 + B + \frac{C}{u}\right)\left(u^2 + B - \frac{C}{u}\right).$$

$$= u^4 + 2Bu^2 + B^2 - \frac{C^2}{u^2}$$

$\Longrightarrow$

$$u^6 + \underbrace{2B}_{\mathbb{R}} u^4 + \underbrace{(B^2 - 4D)}_{\mathbb{R}} u^2 \underbrace{- C^2}_{\mathbb{R}} = 0$$

Even degree.
leading coeff. $= 1 > 0$.
const. term $= -C^2 < 0$.

$\Longrightarrow$ $\exists$ a real solution $u \in \mathbb{R}$.

Then $\alpha = \frac{1}{2}\left(u^2 + B + \frac{C}{u}\right)$

$\beta = \frac{1}{2}\left(u^2 + B - \frac{C}{u}\right)$

Also exist and are Real.
We have solved the problem $\blacksquare$

EVERY REAL QUARTIC FACTORS :)

HW 6 due next Fri
Exam 3 in 2 Fridays.

Today: RFTA.

In 1749, Euler claimed:

Theorem 7 (pg. 26) in his paper:

Every $f(x) \in \mathbb{R}[x]$ of degree 2^n factors as $f(x) = g(x)h(x)$ where

- $g(x), h(x) \in \mathbb{R}[x]$
- $\deg(g) = \deg(h) = 2^{n-1}$.

Claim: This result $\Rightarrow$ RFTA.

Proof: Consider $f(x) \in \mathbb{R}[x]$ of degree m. and choose n such that

$$2^{n-1} < m \leq 2^n.$$

$$n-1 < \log_2(m) \leq n.$$

Then let $g(x) = x^{2^n - m} f(x)$.

Note: $\deg(g) = 2^n - \cancel{m} + \cancel{m} = 2^n$.

By Euler, $g(x) = \prod$ real quadratics

Euclid's Lemma: $\Rightarrow$ prime factors of g have deg 1 & 2.

But every prime factor of f is a prime factor of g.

$\Rightarrow$ prime factors of f have deg 1 & 2

How did Euler prove "Thm 7"?

Last time saw his NICE proof

$$\underset{\deg 4}{f(x)} = \underset{\deg 2}{g(x)} \cdot \underset{\deg 2}{h(x)}.$$

TRY for deg $8 = 2^3$.

Assume $f(x) \in \mathbb{R}[x]$ has form

$$x^8 + Bx^6 + Cx^5 + Dx^4 + Ex^3 + Fx^2 + Gx + H.$$

Suppose it factors as

$$(x^4 - ux^3 + \alpha x^2 + \beta x + \gamma)$$

$$\times\ (x^4 + ux^3 + \delta x^2 + \varepsilon x + \zeta)$$

Goal: Solve for $u, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in \mathbb{R}$.

Expand and equate coefficients:

$$B = \alpha + \delta - u^2$$
$$C = u(\alpha - \delta) + (\beta + \varepsilon)$$
$$D = u(\beta - \varepsilon) + (\gamma + \zeta) + \alpha\delta$$
$$E = u(\gamma - \zeta) + \beta\delta + \alpha\varepsilon$$
$$F = \alpha\zeta + \beta\varepsilon + \gamma\delta$$
$$G = \beta\zeta + \delta\varepsilon$$
$$H = \gamma\zeta$$

Eliminate α & δ
then β & ε
then γ & ζ

Get an equation for u in terms of B, C, D, E, F, G, H.
Hope it has a real root ...

Bernoulli to Euler 29 Nov 1743: "But who among mortals wants to resolve equations in this manner? For I believe that speculation on this is more curious than useful."

So Euler had a new idea

Back to deg 4.

Consider $\overset{f(x)}{x^4 + Bx^2 + Cx + D} \in \mathbb{R}[x]$.

Suppose $f(x)$ has roots a, b, c, d somewhere.

$$a, b, c, d \in \mathbb{F} \quad \text{some field somewhere}$$

$$\begin{matrix} \cup\!\!\mid \\ \mathbb{R} \end{matrix} \quad \text{(mysterious)}$$

Then $f(x) = (x-a)(x-b)(x-c)(x-d)$.

$$= x^4 - \underset{\overset{\shortparallel}{0}}{(a+b+c+d)}x^3 + (ab+ac+ad+bc+bd+cd)x^2$$

$$+ (abc+abd+acd+bcd)x + abcd.$$

If $f(x) = (x^2 - ux + \alpha)(x^2 + ux + \beta)$

Then must have

$$u \in \{a+b \text{ or } a+c, \text{ or } a+d$$
$$b+c, \ b+d, \ c+d\}.$$

Let

$$p = a+b \qquad -p = c+d$$
$$q = a+c \qquad -q = b+d$$
$$r = a+d. \qquad -r = b+c.$$

Then u satisfies.

$$(u-p)(u+p)(u-r)(u+r)(u-q)(u+q) = 0.$$

$$(u^2-p^2)(u^2-r^2)(u^2-q^2) = 0.$$

(*) $$1u^6 + \cdots\cdots - p^2q^2r^2 = 0$$

even degree

neg const term

$\Longrightarrow u \in \mathbb{R}$ exists !

Issue: Why does (*) have $\mathbb{R}$-coeffs?

this
HW 6 due Fri
Exam 3 next Fri

Now: Symmetric Functions

Suppose that

$$f(x) = x^4 + Ax^3 + Bx^2 + Cx + D \in \mathbb{R}[x]$$

has roots $a, b, c, d \in \mathbb{F} \supseteq \mathbb{R}$.

in some field.
maybe we don't know anything about $\mathbb{F}$.

Factor Theorem $\Longrightarrow$

$$f(x) = (x-a)(x-b)(x-c)(x-d).$$

$$\begin{aligned} &= x^4 \\ &\quad - (a+b+c+d)\,x^3 \\ &\quad + (ab+ac+ad+bc+bd+cd)\,x^2 \\ &\quad - (abc+abd+acd+bcd)\,x \\ &\quad + abcd \end{aligned}$$

Compare coefficients.

$\Downarrow$

$-A = a+b+c+d = e_1(a,b,c,d)$

$B = ab+ac+ad+bc+bd+cd = e_2(a,b,c,d)$

$-C = abc+abd+acd+bcd = e_3(a,b,c,d)$

$D = abcd. = e_4(a,b,c,d)$

Elementary Symmetric Polynomials.

Sometimes we write

e_i for $e_i(a,b,c,d)$
if variables are understood.

Remark: even though a, b, c, d are mysterious, we know $a+b+c+d = -A \in \mathbb{R}$.

General Definition:

Given $r_1, r_2, \cdots, r_n \in \mathbb{F}$, we say

$$f(x) = (x-r_1)(x-r_2)\cdots(x-r_n)$$

$$=: x^n - e_1 x^{n-1} + e_2 x^{n-2} - e_3 x^{n-3} + \cdots$$

$$\cdots\cdots (-1)^{n-1} e_{n-1} x^1 + (-1)^n e_n x^0.$$

Here.

$e_k = e_k(r_1, r_2, \ldots, r_n)$.

$$= \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} r_{i_1} r_{i_2} r_{i_3} \cdots r_{i_k}$$

sum the roots taken k at a time.

= the k^{th} elementary symmetric poly.

Important Fact (Newton → Waring → Gauss)
"Fundamental Theorem of Symmetric Polynomials/Functions".

Let $f(r_1, r_2, \ldots, r_n)$ be any function symmetric in $r_1, r_2, \ldots, r_n$

(i.e. $f(r_1, \ldots, r_i, r_{i+1}, \ldots, r_n) = f(r_1, \ldots, r_{i+1}, r_i, \ldots, r_n)$ for any $1 \le i \le n-1$.)

Then f has a unique expression in terms of $e_1, e_2, \ldots, e_n$.

↓

Eg. suppose $x^3+23x+1$ has roots r, s, t.

What polynomial has roots $1+r, 1+s, 1+t$?

First note.

$$e_1 = r+s+t = -0$$
$$e_2 = rs + rt + st = +23$$
$$e_3 = rst = -1$$

We are looking for

$$g(x) = (x-(1+r))(x-(1+s))(x-(1+t)).$$

$$= x^3 - (1+r+1+s+1+t)x^2 + ((1+r)(1+s)+(1+r)(1+t)+(1+s)(1+t))x$$
$$- (1+r)(1+s)(1+t)$$

symmetric in r, s, t.

$\Rightarrow$ express in terms of e_1, e_2, e_3

$$1+r+1+s+1+t = 3+r+s+t = 3+e_1 = 3-0 = 3$$

$$(1+r)(1+s) + (1+r)(1+t) + (1+s)(1+t)$$
$$= 1+r+s+rs + 1+r+t+rt + 1+s+t+st.$$
$$= 3+2(r+s+t) + (rs+rt+st)$$
$$= 3+2e_1 + 1e_2.$$
$$= 3+2\cdot 0 + 1\cdot 23 = 26.$$

$$(1+r)(1+s)(1+t).$$
$$= 1+(r+s+t)+(rs+rt+st)+(rst)$$
$$= 1+e_1+e_2+e_3.$$
$$= \cancel{1}-0+23-\cancel{1} = 23.$$

Hence

$$g(x) = x^3-3x^2+26x-23$$

has roots $1+r$, $1+s$, $1+t$ ///

Exercise:

Express $r^3+s^3+t^3$ in terms of e_1, e_2, e_3.

Gauss' Proof of FTSP

Let $f(x_1, x_2, \dots, x_n)$ be symmetric poly. in n variables $x_1, x_2, \dots, x_n$.

A general term looks like

$$f(x) = \cdots + a x_1^{i_1} x_2^{i_2} x_3^{i_3} \cdots x_n^{i_n} + \cdots$$

$$\downarrow$$

$$(i_1, i_2, \dots, i_n)$$

called the "degree sequence".

Order degree sequences "lexicographically" (like a dictionary).

e.g. $(0,0,0) < (0,0,1) < (0,1,1) < (0,1,2)$

Def: the leading term of $f(x)$ has "biggest" degree sequence, say

$$a x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Claim: $i_1 \geq i_2 \geq \cdots \geq i_n$

Proof: suppose $i_k < i_{k+1}$ for some k.

Then by symmetry, $a x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_{k+1}^{i_{k+1}} x_k^{i_k} x_{k+2}^{i_{k+2}} \cdots$

is also a term of f with a "bigger" degree sequence $\lightning$

Hence leading term has $i_1 \geq i_2 \geq \cdots \geq i_n$.

Note: $a e_1^{i_1 - i_2} e_2^{i_2 - i_3} \cdots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}$
also has leading term

$$a x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Hence $f - a e_1^{i_1 - i_2} \cdots e_n^{i_n}$
is symmetric with smaller leading term.
Proceed by induction.

HW 6 due this Fri

Exam 3 next Fri

O.H

Today & Tom. 2:30 — 4:00.

Now : FTSP

Fund. Thm. of Symm. Polynomials.

Recall: if

$$(x-r_1)(x-r_2)\cdots(x-r_n)$$

$$= x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n x^0.$$

Then $e_1, e_2, \ldots, e_n$ are polynomials in the $r_1, r_2, \ldots, r_n$.

$$\begin{cases} e_1 = r_1 + r_2 + \cdots + r_n \\ e_2 = r_1 r_2 + r_1 r_3 + \cdots + r_1 r_n + r_2 r_3 + \cdots + r_{n-1} r_n \\ \vdots \\ e_n = r_1 r_2 \cdots r_n. \end{cases}$$

elementary symmetric polynomials

Theorem (FTSP).

Any symmetric poly $f(r_1, r_2, \dots, r_n)$. can be expressed as

$$f = g(e_1, e_2, \dots, e_n)$$

for some unique poly g.

eg. Let $(r_1, r_2) = (a, b)$

Then $f(a,b) = a^3 + b^3$ is symmetric.

Note: $e_1 = a + b$
$e_2 = ab$.

$$e_1^3 = (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

$$f - e_1^3 = -3a^2b - 3ab^2$$
$$= -3ab(a+b) = -3e_2e_1.$$

Hence $f - e_1^3 = -3e_1e_2$.

$$f = e_1^3 - 3e_1e_2$$
$$= \underbrace{g(e_1, e_2)}_{\text{UNIQUE}}.$$

Another eg.

Consider $x^3 + Ax^2 + Bx + C$
with roots r, s, t.

So $-A = e_1(r,s,t) = r+s+t$
$+B = e_2(r,s,t) = rs + rt + st$
$-C = e_3(r,s,t) = rst$.

Problem: Express $\Delta = (r-s)^2(r-t)^2(s-t)^2$
in terms of A, B, C.

Where to begin? .....

Expand Δ and look for the
"biggest" term

what does this mean?

General term is: $k\, r^l s^m t^n$

"degree" $= (l, m, n)$.

How to say which degrees are big?

$(2,1,0) \underset{?}{\overset{<}{>}} (0,1,2)$

Use lexicographic (dictionary) order

e.g. $(0,0,0) < (0,0,1) < (0,1,0) < (0,1,2)$.

For us ...

$$\Delta = \underbrace{\overset{(4,2,0)}{r^4 s^2}}_{\text{leading term}} + \text{lower terms}.$$

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

$$= \underbrace{r^4 s^2}_{\text{same leading term}} + \text{lower terms}.$$

Cancel leading term:

$$\Delta - e_1^2 e_2^2 = \underbrace{-4\overset{(4,1,1)}{r^4 st}} + \text{lower terms}$$

$(4,2,0) > (4,1,1)$

leading term went down!

$$-4 e_1^3 e_3 = -4(r+s+t)^3 rst.$$

$$= -4r^3 rst + \text{lower terms}.$$

$$= -4r^4 st + \text{l.t.} \ldots$$

$\checkmark$

$(3,3,0)$.

$$\Delta - e_1^2 e_2^2 + 4e_1^3 e_3 = -4r^3s^3 + \text{l.t.}$$

$$(4,2,0) > (4,1,1) > (3,3,0)$$

$$-4e_2^3 = -4(rs+rt+st)^3$$
$$= -4r^3s^3 + \text{l.t.}$$

$$\Delta - e_1^2 e_2^2 + 4e_1^3 e_3 + 4e_2^3 = \underline{18 r^3 s^2} t + \text{l.t.}$$

$$18 e_3 e_2 e_1 = \underline{18 r^3 s^2} t + \text{l.t.}$$

$$\Delta - e_1^2 e_2 + 4e_1^3 e_2 + 4e_2^3 - 18 e_1 e_2 e_3$$

$$= -27 r^2 s^2 t^2 + 0$$

that's all

$$= -27 e_3^2.$$

Conclusion:

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

$$= (-A)^2 B^2 - 4(-A)^3(-C) - 4B^3 + 18(-A)B(-C) - 27(-C)^2$$

$$= \underbrace{A^2B^2 - 4A^3C - 4B^3 + 18ABC - 27C^2}_{\text{The discriminant of a cubic poly.}}$$

So ... how to prove FTSP ?

Proof (Gauss) : ALGORITHMIC

Induction on degree sequence.
Let $f(r_1, \ldots, r_n)$ be symmetric with lex-leading term

$$c\, r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$$

Claim: $i_1 \geq i_2 \geq \cdots \geq i_n$. ✓
Otherwise we would have $i_k < i_{k+1}$ for some k. By symmetry $r_k \leftrightarrow r_{k+1}$.

$$c\, r_1^{i_1} \cdots r_k^{i_{k+1}} r_{k+1}^{i_k} \cdots r_n^{i_n}$$

is also a term of f with "bigger" lex deg. sequence
CONTRADICTION ///

$c\, e_1^{i_1 - i_2} e_2^{i_2 - i_3} \cdots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}$ has <u>same</u> leading term.

$\implies$ $f - c\, e_1^{i_1 - i_2} \cdots e_n^{i_n}$ is symm. with <u>smaller</u> leading term. By <u>induction</u> we're done. $\blacksquare$

HW6 due now.
Exam 3 <u>next</u> Fri.

Today: ?? (Grand Finale)

We know how to go from

the roots of a polynomial $\rightsquigarrow$ the coefficients

$$r_1, r_2, \ldots, r_n \rightsquigarrow \underbrace{-e_1, e_2, -e_3, \ldots, (-1)^n e_n}_{\text{elem. symm. polys.}}$$

But can we go <u>back</u>?

the coefficients $\overset{?}{\rightsquigarrow}$ the roots

$e_1, e_2, \ldots, e_n$ $\qquad$ $r_1, r_2, \ldots, r_n$

<u>eg.</u> Given $e_1 = r_1 + r_2$, $e_2 = r_1 r_2$, <u>find</u> r_1 and r_2.

Now let
$$\left.\begin{aligned} s_1 &= r_1 + r_2 \\ s_2 &= r_1 - r_2 \end{aligned}\right\} \text{ Method due to } \underline{\text{Lagrange}}$$

$$\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

Invert: $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = -\frac{1}{2}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$

$\Rightarrow \quad r_1 = \frac{1}{2}(s_1 + s_2)$

$r_2 = \frac{1}{2}(s_1 - s_2)$.

But what are s_1, s_2?

$s_1 = r_1 + r_2 = e_1$ ✓

$s_2 = r_1 - r_2$ NOT symmetric.

$s_2^2 = (r_1 - r_2)^2$ symmetric ☺

$= r_1^2 - 2r_1r_2 + r_2^2$.

$= (r_1 + r_2)^2 - 4r_1r_2$

$= e_1^2 - 4e_2$.

Let $s_2 = \sqrt{e_1^2 - 4e_2}$.
choose some value.

Then

$$\left.\begin{aligned} r_1 &= \tfrac{1}{2}(s_1 + s_2) = \tfrac{1}{2}\left(e_1 + \sqrt{e_1^2 - 4e_2}\right) \\ r_2 &= \tfrac{1}{2}(s_1 - s_2) = \tfrac{1}{2}\left(e_1 - \sqrt{e_1^2 - 4e_2}\right) \end{aligned}\right\} \text{Quad. Formula}$$

☺

Apply Lagrange to the cubic.

Let r_1, r_2, r_3 be the roots of a cubic.

Prob: Express in terms of $\underbrace{e_1, e_2, e_3}_{\text{the coefficients.}}$

Set $\omega = e^{2\pi i/3}$ and let

$$\left.\begin{aligned} s_1 &= r_1 + r_2 + r_3 \\ s_2 &= r_1 + \omega r_2 + \omega^2 r_3 \\ s_3 &= r_1 + \omega^2 r_2 + \omega r_3. \end{aligned}\right\} \text{finite Fourier transform}$$

Invert:

$$r_1 = \tfrac{1}{3}(s_1 + s_2 + s_3)$$
$$r_2 = \tfrac{1}{3}(s_1 + \omega^2 s_2 + \omega s_3)$$
$$r_3 = \tfrac{1}{3}(s_1 + \omega s_2 + \omega^2 s_3)$$

Now solve for s_1, s_2, s_3.

$s_1 = e_1$ ✓

s_2, s_3 are NOT symmetric in r_1, r_2, r_3

But $A = s_2^3 + s_3^3$ and $B = s_2^3 + s_3^3$ ~~ARE symmetric~~.

Use Gauss' Algorithm to get.

$$\boxed{\begin{aligned} A &= 2e_1^3 - 9e_1e_2 + 27e_3. \\ B &= e_1^2 - 3e_2. \end{aligned}}$$

Then s_2^3 & s_3^3 are the roots of

$$(x - s_2^3)(x - s_3^3) = x^2 - (s_2^3 + s_3^3)x + s_2^3 s_3^3$$
$$= x^2 - Ax + B.$$

So $s_2^3, s_3^3 = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)$. ~~Quad~~ formula

$$\Rightarrow \quad s_2, s_3 = \sqrt[3]{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)},$$

choose some value

functions of e_1, e_2, e_3

Recall $s_1 = e_1$.

Finally

Cardano's formula

$$r_1 = \frac{1}{3}(s_1 + s_2 + s_3)$$
$$r_2 = \frac{1}{3}(s_1 + \omega^2 s_2 + \omega s_3)$$
$$r_3 = \frac{1}{3}(s_1 + \omega s_2 + \omega^2 s_3)$$

in terms of e_1, e_2, e_3.

We "solved" the cubic !!

Lagrange also works on the quartic
BUT it's complicated.
(See Chapter 6.5)

Lagrange tried to solve the quintic and failed.

Then he tried to show quintic cannot be solved.

i.e. Conjecture: There does NOT exist a formula for r_1, r_2, r_3, r_4, r_5 in terms of e_1, e_2, e_3, e_4, e_5

$$e_1 = r_1 + r_2 + \cdots + r_5$$
$$e_2 = r_1 r_2 + r_1 r_3 + \cdots + r_4 r_5$$
$$\vdots$$
$$e_5 = r_1 r_2 r_3 r_4 r_5.$$

and using only $\underbrace{+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \text{etc.}}_{\text{an expression in Radicals}}$

Paraphrase:
The general quintic is (unsolvable / insolvable / insoluble).

What happened next?

Lagrange

$\downarrow$

Ruffini

$\downarrow$

~~Niels Henrik Abel (1802–1829)~~.

Theorem (Abel):

The general quintic is <u>unsolvable</u>.

Issues:

- His proof was COMPLICATED.
- it had a gap.
- <u>some</u> quintics are solvable

(<u>eg</u> $x^5 - 1$ has roots.

$1, \omega, \omega^2, \omega^3, \omega^4$ where $\omega = e^{2\pi i/5}$.)

Which ones?

$\downarrow$

Évariste Galois (1811 - 1832)

Let $f(x) \in \mathbb{F}[x]$

some field.

Let $\mathbb{E} \supseteq \mathbb{F}$ be the splitting field for $f(x)$. (it contains all the roots of f).

Let $Gal(\mathbb{E}/\mathbb{F})$ = automorphisms of $\mathbb{E}$ that leave $\mathbb{F}$ fixed.

eg. $Gal(\mathbb{C}/\mathbb{R})$ = conjugation.

$Gal(\mathbb{E}/\mathbb{F})$ is called the <u>Galois group</u> of $f(x)$.

<u>Theorem</u> (Galois).

$f(x)$ is solvable $\Longleftrightarrow$ $Gal(\mathbb{E}/\mathbb{F})$ is "solvable".

I won't define this.

$\boxed{\text{ICOSAHEDRON}}$