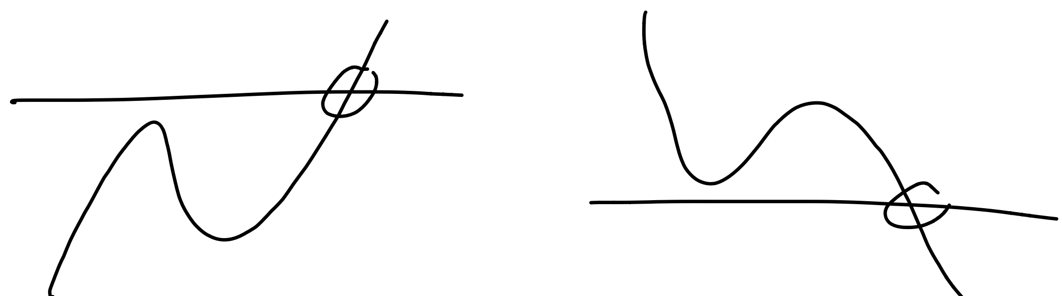
New Topic:

- Symmetric Functions
- Laplace's Proof of the F.T.A.

Recall: The F.T.A. implies that every nonconstant $f(x) \in \mathbb{R}[x]$ factors as a product of <u>real</u> polynomials of degrees 1 & 2.

[In fact we will see that the F.T.A. is <u>equivalent</u> to this statement.]

If $f(x) \in \mathbb{R}[x]$ has degree 3, we know from I.V.T. that $f(x)$ has a real root $a \in \mathbb{R}$.



Hence $f(x) = (x-a)\,g(x)$ where $g(x) \in \mathbb{R}[x]$ has degree 2. ✓

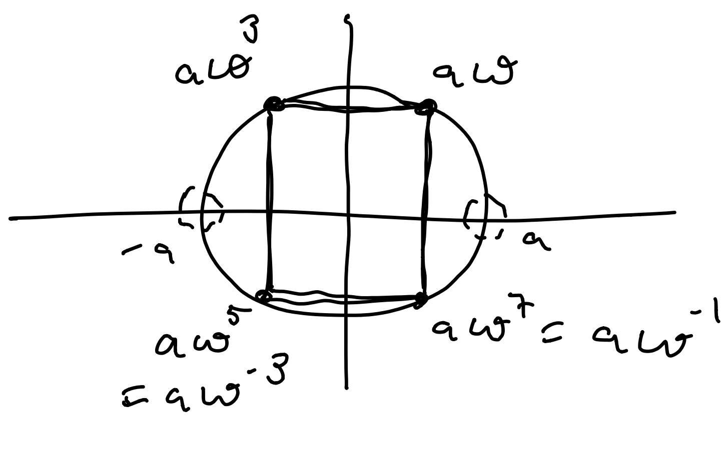
Problem: Show how to factor real polynomials of degree ≥ 4. (1702)

Leibniz' Mistake: For $a \in \mathbb{R}$, Leibniz mistakenly claimed that $x^4 + a^4 \in \mathbb{R}[x]$ does not factor over $\mathbb{R}$.

He was wrong:
$$x^4 + a^4 = 0$$
$$x^4 = -a^4$$
$$x^4 = a^4 e^{i\pi} \quad \text{(polar)}$$

$$\Rightarrow x = ae^{i\pi/4},\ ae^{i3\pi/4},\ ae^{i5\pi/4},\ ae^{i7\pi/4}$$

$\omega = e^{2\pi i/8}$



Group the roots into conjugate pairs:

$$x^4+a^4 = \underbrace{(x-a\omega)(x-a\omega^{-1})}\ \underbrace{(x-a\omega^3)(x-a\omega^{-3})}$$

$$= (x^2 - a(\omega+\omega^{-1})x + a^2)(x^2 - a(\omega^3+\omega^{-3})x + a^2)$$

$$= \left(x^2 - 2a\cos\left(\tfrac{2\pi}{8}\right)x + a^2\right)\left(x^2 - 2a\cos\left(\tfrac{6\pi}{8}\right)x + a^2\right)$$

Done ✓

$$= (x^2 - a\sqrt{2}\,x + a^2)(x^2 + a\sqrt{2}\,x + a^2)$$

The answer even looks good. :)

From this we can compute

$\int \frac{1}{x^4+a^4}\,dx$ explicitly. (But the formula is a big mess.)

Confusion Remained: In 1742, Nicholas Bernoulli claimed to Euler that $x^4 - 4x^3 + 2x^2 + 4x - 4$ <u>cannot</u> be factored over $\mathbb{R}$.

This would have been a counterexample to the F.T.A.

Not only did Euler factor this polynomial, he also gave a proof that <u>every</u> polynomial in $\mathbb{R}[x]$ of degree 4 factors.

He also claimed a proof up to degree 8 and sketched ideas for a full proof of F.T.A.

Here's his proof for degree 4.

Given $f(x) \in \mathbb{R}[x]$ of degree 4 we can eliminate the x^3 term to get

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

Euler assumed that there exist some "imaginary numbers" a, b, c, d such that

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

Expand:

$$f(x) = x^4 - (a+b+c+d)x^3$$
$$+ (ab + ac + ad + bc + bd + cd)x^2$$
$$- (abc + abd + acd + bcd)x$$
$$+ abcd$$

Equating coefficients:

$$\begin{cases} a+b+c+d = 0 \\ ab + \cdots + cd = +B \\ abc + \cdots + bcd = -C \\ abcd = +D \end{cases} \rightsquigarrow \begin{cases} a = ? \\ b = ? \\ c = ? \\ d = ? \end{cases}$$

4 equations in 4 unknowns

Too Hard.

More modest goal:

Find $u, v, \alpha, \beta \in \mathbb{R}$ such that

$$f(x) = (x^2 - ux + \alpha)(x^2 - vx + \beta)$$
$$= x^4 - (u+v)x^3 + \cdots$$
$$(u+v = 0)$$

So $v = -u$:

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

What do we know about u, α, β ?

By unique prime factorization of polynomials,

$$
\begin{aligned}
x^2 - ux + \alpha = \; & (x-a)(x-b) \\
\text{or} \quad & (x-a)(x-c) \\
\text{or} \quad & \vdots \\
\text{or} \quad & (x-c)(x-d)
\end{aligned}
$$

$$\Rightarrow u \in \left\{ \overset{p}{a+b}, \overset{q}{a+c}, \overset{r}{a+d}, \underset{-p}{c+d}, \underset{-q}{b+d}, \underset{-r}{b+c} \right\}$$

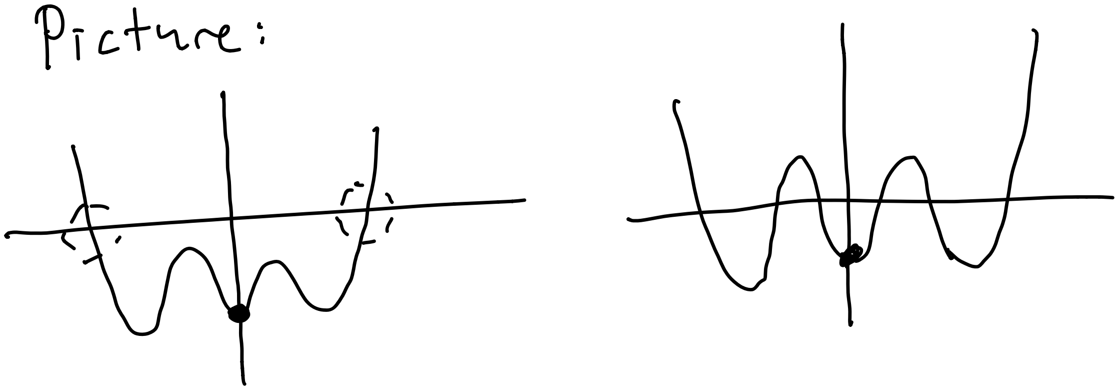
In other words, u is a root of the "auxiliary polynomial"

$$
\begin{aligned}
g(u) &= (u-p)(u+p)(u-q)(u+q)(u-r)(u+r) \\
&= (u^2-p^2)(u^2-q^2)(u^2-r^2) \\
&= 1u^6 + \cdots + (-1)p^2q^2r^2 .
\end{aligned}
$$

So what?

Observation: $g(u)$ has <u>even degree</u> and constant term $-p^2q^2r^2 < 0$.

Picture:



By I.V.T. the polynomial $g(u)$ has at least one real root $u \in \mathbb{R}$.

We can then use this u to find values for α & β.

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

$$\begin{cases} \alpha + \beta - u^2 = B \\ u(\alpha - \beta) = C \\ \alpha\beta = D \end{cases} \rightsquigarrow \begin{cases} \alpha = ? \\ \beta = ? \end{cases}$$

This is easy:

$$\alpha + \beta = B + u^2$$
$$\alpha - \beta = C/u$$

$$2\alpha = B + u^2 + C/u$$
$$\alpha = (B + u^2 + C/u)/2$$
$$\beta = B + u^2 - \alpha \quad \checkmark$$

We have proved that some numbers $u, \alpha, \beta \in \mathbb{R}$ exist.

Whew!

But I fooled you!

There is a gap in this proof.

How do we know that

$$g = (u^2 - p^2)(u^2 - q^2)(u^2 - r^2)$$

has <u>real</u> <u>coefficients</u>??

We know that

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

These p, q, r are not necessarily <u>real</u> numbers.

[Recall: $x^4 + a^4$ has <u>no</u> real roots but it still factors.]

We can't assume that a, b, c, d are real. But we do know something important:

$$ab + ac + \cdots + cd = B \in \mathbb{R}$$
$$abc + \cdots + bcd = -C \in \mathbb{R}$$
$$abcd = D \in \mathbb{R}$$

"Elementary symmetric combinations" of a, b, c, d are real.

From this, we need to show that

the coefficients of

$$g(u) = (u^2-p^2)(u^2-q^2)(u^2-r^2)$$

are real. Sounds very hard, but it follows from an important general principle, first stated by Isaac Newton.

Fundamental Theorem of Symmetric Polynomials

Any symmetric combination of the roots of a polynomial can be expressed in terms the coefficients.

e.g. $a^2+b^2+c^2+d^2$

is symmetric, hence it must be real.

MORE NEXT TIME.