Exam 2 Total 25

Ave	17.5
Med	18
St Dev	4.5

Appox. Ranges

A = 20 +

B = 15 +

C = 10 +.

Segue:

Suppose cubic $f(x) \in \mathbb{Q}[x]$ has root $1+\sqrt{2}$. Then

Claim: $f(x)$ has a $\mathbb{Q}$-root.

Proof: Consider $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$

$$f(1+\sqrt{2}) = 0 \implies f(1-\sqrt{2}) = 0.$$

Hence

$$f(x) = (x-(1+\sqrt{2}))(x-(1-\sqrt{2}))\, g(x).$$
$$= (x^2-2x-1)\, g(x).$$

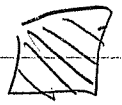
where $g(x)$ has degree 1.

If g had non-$\mathbb{Q}$ coeff then
so would f $\lightning$ Hence $g(x) \in \mathbb{Q}[x]$.

Say $g(x) = ax + b$ with $a, b \in \mathbb{Q}$, $a \neq 0$.

Then $g(-\frac{b}{a}) = 0$.

$\Rightarrow f(-\frac{b}{a}) = s'thing \cdot g(-\frac{b}{a}) = 0$.



This result FAILS for $\deg f \geq 4$.

eg. $f(x) = x^4 - 2x^3 - 4x^2 + 6x + 3 \in \mathbb{Q}[x]$

has root $1+\sqrt{2}$ (believe me).
Factor Theorem.

$$f(x) = (x-(1+\sqrt{2}))(x-(1-\sqrt{2}))(x^2-3)$$
$$= (x^2-2x-1)(x^2-3)$$

NO $\mathbb{Q}$-roots!
STUCK!

Moral: Roots <u>don't</u> always <u>exist</u>

New Topic: FTA
(Fundamental Theorem of Algebra)

Theorem (ℂFTA):
Every polynomial $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

(the field $\mathbb{C}$ is "algebraically closed")

Corollary: Every $f(x) \in \mathbb{C}[x]$ splits over $\mathbb{C}$.
i.e.

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

where $C, r_1, r_2, \ldots, r_n \in \mathbb{C}$.

Proof: by induction on degree.
Let $f(x)$ have degree n.
By ℂFTA, $\exists\, z \in \mathbb{C}$ s.t. $f(z) = 0$.
By Factor Theorem

$$f(x) = (x-z)\,g(x)$$

where $g(x) \in \mathbb{C}[x]$ has deg $n-1$.
By induction, $g(x)$ splits over $\mathbb{C}$.
Hence f splits ∎

Definition: given a root $z \in \mathbb{C}$ of $f(x) \in \mathbb{C}[x]$, the **multiplicity** of the root is

highest power of $(x-z)$ that divides $f(x)$.

eg. $f(x) = (x-\sqrt{2})^3 (x+\pi)(x-i)^2$.

Roots	$\sqrt{2}$	$-\pi$	i
Mult.	3	1	2

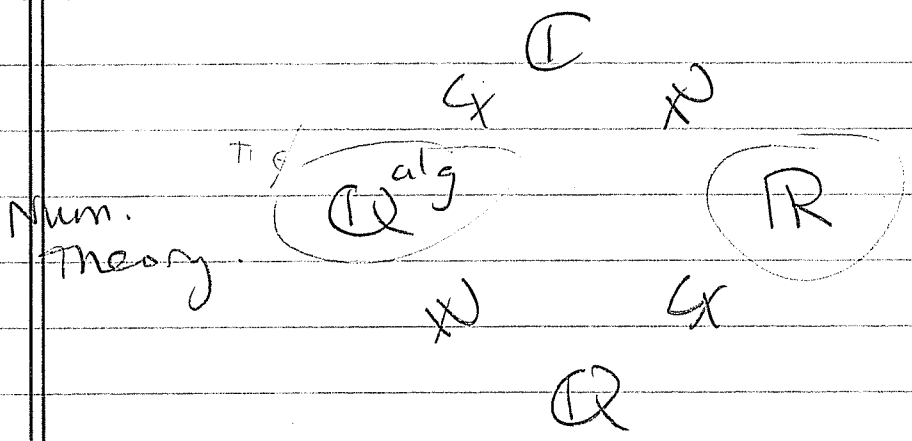
Corollary: Every $f(x) \in \mathbb{C}[x]$ of deg n has **exactly** n roots in $\mathbb{C}$.
(counting with multiplicity).

Is $\mathbb{C}$ the only alg. closed field?
NO.

eg. $\mathbb{Q}^{alg} := \{\alpha \in \mathbb{C} : f(\alpha) = 0$ for some $f(x) \in \mathbb{Q}[x]\}$
= roots of all $\mathbb{Q}$-polynomials
= "algebraic numbers".

$\mathbb{Q}^{alg}$ is algebraically **closed**.

Both.



Picture: Wiki "algebraic number".

$\pi \notin \mathbb{Q}^{alg}$ Lindemann 1882.

$\mathbb{Q}^{alg}$ is countable.

Q: How hard is CFTA to prove?
A: Not as hard as people think.
Euler gave nice (incomplete) proof.

We'll follow him ☺

HW 5 Fri Apr 8
HW 6 Fri Apr 22
Exam 3 Fri Apr 29.

Now: FTA.

Modern Statement(s)

(1) Every $f(x) \in \mathbb{C}[x]$ has a root $\in \mathbb{C}$.
(2) Every $f(x) \in \mathbb{C}[x]$ splits over $\mathbb{C}$.
(3) Every $f(x) \in \mathbb{C}[x]$ of deg. n has exactly n roots $\in \mathbb{C}$ (counting multiplicity)

(1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) are called $\mathbb{C}$FTA.

Original Statement
- no mention of $\mathbb{C}$.

$\mathbb{R}$FTA:
Every $f(x) \in \mathbb{R}[x]$ is a product of linear & quadratic $\mathbb{R}$-polynomials.

eg. $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$.
Real quadratic.

Say $$f(x) = C \prod_{i=1}^{k} (x - r_i) \prod_{i=1}^{l} (x^2 + a_i x + b_i)$$

for $C, r_i, a_i, b_i \in \mathbb{R}$.
(we can assume $a_i^2 - 4b_i < 0$).

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

Q: Does $x^4 - 4x^3 + 2x^2 + 4x + 4 = f(x)$.
factor over $\mathbb{R}$??

N. Bernoulli (1742) thought "NO".
Euler (1743) proved him wrong.

$$f(x) = \left(x^2 - x\left(2 + \sqrt{4+2\sqrt{7}}\right) + 1 + \sqrt{7} + \sqrt{4+2\sqrt{7}}\right) \cdot \left(x^2 - x\left(2 - \sqrt{4+2\sqrt{7}}\right) + 1 + \sqrt{7} - \sqrt{4+2\sqrt{7}}\right)$$!

2 $\mathbb{R}$-quadratics.

CFTA vs. RFTA.
same or different?

Theorem: CFTA $\iff$ RFTA.
logically equivalent.

Proof: $\mathbb{C}$FTA $\Rightarrow$ $\mathbb{R}$FTA.

Assume $\mathbb{C}$FTA true, and let $f(x) \in \mathbb{R}[x]$.
Want to factor $f(x)$ into linears & quadratics $\in \mathbb{R}[x]$.

Since $f(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$.
$\mathbb{C}$FTA $\Rightarrow$ $f(x)$ splits over $\mathbb{C}$.
Know: non-$\mathbb{R}$ roots come in conj pairs.
Hence

$$f(x) = c \prod_{i=1}^{k} (x - r_i) \prod_{i=1}^{l} (x - z_i)(x - \overline{z_i}).$$

with $r_i \in \mathbb{R}$
$c \in \mathbb{R}$.
$z_i \in \mathbb{C} - \mathbb{R}$.

Hence $f(x) = c \prod (x - r_i) \prod (x^2 - (z_i + \overline{z_i})x + z_i \overline{z_i})$
Real. Real.

✓

$\mathbb{R}$FTA $\Rightarrow$ $\mathbb{C}$FTA.

Assume $\mathbb{R}$FTA and consider $p(x) \in \mathbb{C}[x]$.
Does $p(x)$ split over $\mathbb{C}$?
Define conjugate polynomial $\overline{p}(x)$ by

$$\overline{p}(z) := \overline{p(\overline{z})} \quad \text{for all } z \in \mathbb{C}.$$

Claim: $f(x) = p(x)\overline{p}(x) \in \mathbb{R}[x]$ (HW 5).

By IBFTA we can write

$$f(x) = C\prod(x-r_i)\prod(x^2+a_ix+b_i) \text{ over } \mathbb{R}.$$

But $x^2+a_ix+b_i = (x-z_i)(x-\overline{z_i})$

where $z_i, \overline{z_i} = \dfrac{-a_i \pm \sqrt{a_i^2-4b_i}}{2}$ Quad. formula.

Hence $f(x) = C\prod(x-r_i)\prod(x-z_i)(x-\overline{z_i})$
splits over $\mathbb{C}$.

Claim: Hence $p(x)$ splits over $\mathbb{C}$.

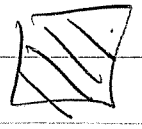
Eg. $f(x) = (x-w_1)(x-w_2)\cdots(x-w_{2n})$ over $\mathbb{C}$.

For each i, $(x-w_i) \mid f(x) = p(x)\overline{p}(x)$.

$\Rightarrow$ $(x-w_i) \mid p(x)$ OR $(x-w_i) \mid \overline{p}(x)$.

? "Euclid's Lemma". (HW 5).

$\Rightarrow$ $p(x)$ & $\overline{p}(x)$ both split.



We used FACT.

$(x - w_i)$ is "prime" in $\mathbb{C}[x]$.
What does that mean?

Chapter 6 of the text.

Let F be a field.
Analogy:

$\mathbb{Z}$	$F[x]$
Eucl. Algorithm	✓
Eucl. Lemma	✓
Unique Prime Fact.	✓
GCD.	✓

very similar to $\mathbb{Z}$

- an "integral domain"

Recall: For $a, b \in \mathbb{Z}$, $b \neq 0$, $\exists!\ q, r \in \mathbb{Z}$ such that:

"there exist unique"

$$a = qb + r, \quad |r| < |b|.$$

q: quotient, r: remainder.

the zero polynomial.

Similarly: For $P(x), D(x) \in \mathbb{F}[x]$, $D(x) \neq 0$,
$\exists!$ $Q(x), R(x) \in \mathbb{F}[x]$ such that

$$P(x) = Q(x)D(x) + R(x).$$

where $\deg R < \deg D$ or $R(x) = 0$

To simplify, we could define $\deg(\text{"0"}) = -1$
(↑ zero poly.)

Proof: Boring ▨

Easy to compute, eg. $\dfrac{x^5+x^4+x^2+1}{x^3+x+1}$.

$$\begin{array}{r|l}
x^3+x+1 & x^5+x^4+0+x^2+0+1 \\
 & \quad (\text{quo}) \; x^2+x-1 \\
\hline
 & x^5+x^4+x^2+1 \\
 & x^5 \quad +x^3+x^2 \\
\hline
 & x^4-x^3+1 \\
 & x^4 \quad +x^2+x \\
\hline
 & -x^3-x^2-x+1 \\
 & -x^3 \quad -x-1 \\
\hline
 & -x^2+2 \quad (\text{rem})
\end{array}$$

$$x^5+x^4+x^2+1 = (x^2+x-1)(x^3+x+1) + (-x^2+2)$$

quo. REM.

HW 5 due Fri Apr 8.
(I'm out of town Apr 8?)

Now: Chapter 6.

$\mathbb{Z}$ vs. $\mathbb{F}[x]$.

Recall

The Division Algorithm:
for $a, b \in \mathbb{Z}$, $b \neq 0$ $\exists!$ ("there exist unique")
$q, r \in \mathbb{Z}$ s.t.

$$a = qb + r, \quad |r| < |b|.$$

(q: quotient, r: remainder.)

Division Alg. ⟶ Unique Prime Factorization. $\mathbb{Z}$

New: Division Algorithm for Polynomials

Theorem (Prop. 6.14) Let $\mathbb{F}$ be a field.
Given $P(x), D(x) \in \mathbb{F}[x]$, $D(x) \neq 0$
(0 = the zero polynomial). $\exists!$ $Q(x), R(x) \in \mathbb{F}[x]$
s.t.

$$P(x) = Q(x)D(x) + R(x)$$

where $\deg(R) < \deg(D)$ or $R(x) = 0$ ///

Proof: - well-ordering of $\mathbb{N}$ (uses)
- Boring
- omitted.

Do an example

If $P(x) = Q(x)D(x) + 0$

we say $D(x) \mid P(x)$ "D divides P"

We say $P(x)$ is irreducible over $\mathbb{F}$ if we cannot write

$$P(x) = A(x)B(x) \text{ with}$$

$$A(x), B(x) \in \mathbb{F}[x], \quad \deg(A), \deg(B) > 0$$

eg. $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$

$x^2 + 1$ is irreducible / $\mathbb{R}$

$x + i$ is irred / $\mathbb{C}$.

Remark: irred polys are the "primes" of $\mathbb{F}[x]$.

"irreducible" = "prime" in $\mathbb{F}[x]$.

Define: Say $G(x)$ is a **GCD** of $A(x), B(x)$ if

1. $G(x) \mid A(x)$ and $G(x) \mid B(x)$.
2. if $H(x) \mid A(x)$ and $H(x) \mid B(x)$ then $\deg(H) \leq \deg(G)$.

Fact: If $P(x) = Q(x)D(x) + R(x)$ Then $\gcd(P, D) = \gcd(D, R)$.

Proof: $G(x) \mid P$ and $D \iff G(x) \mid D$ and R ∎

The Euclidean Algorithm.

$$P(x) = Q_1(x)D(x) + R_1(x). \qquad \deg R_1 < \deg D$$
$$D(x) = Q_2(x)R_1(x) + R_2(x) \qquad \deg R_2 < \deg R_1$$
$$\vdots$$
$$R_k(x) = Q_{n+2}(x)R_{n+1}(x) + R_{n+2}(x).$$

$$\deg D > \deg R_1 > \cdots > \deg R_n \cdots$$

eventually you get $R_{k-1}(x) \neq 0$, $R_k(x) = 0$

Conclusion: $R_{k-1}(x) = \gcd(P(x), D(x))$.

$$R_{k-2}(x) = Q_k(x) R_{k-1}(x) + R_k(x) \qquad \deg R_k < \deg R_{k-1}$$
$$R_{k-1}(x) = Q_{k+1}(x) R_k(x) + \bigcirc$$

Conclusion.

$$R_k = \gcd(R_k, R_{k-1}) = \gcd(R_{k-1}, R_{k-2})$$

$$= \cdots = \gcd(R_2, R_1) = \gcd(R_1, D) = \gcd(D, P).$$

Last nonzero remainder is $\gcd(P, D)$. ☺

example:

$$(x^5 + x^4 + x^2 + 1) = (x^2 + x - 1)(x^3 + x + 1) + (-x^2 + 2)$$
$$P \qquad\qquad Q_1 \qquad\qquad D \qquad\qquad R_1.$$

$$\begin{array}{r|l} & -x \\ \hline -x^2 + 2 & x^3 + 0 + x + 1 \\ & x^3 + 0 - 2x + 0 \\ \hline & 3x + 1. \end{array}$$

$$(x^3 + x + 1) = (-x)(-x^2 + 2) + (3x + 1).$$
$$Q_2 \qquad R_1 \qquad R_2.$$

$$
\begin{array}{r|l}
 & -\frac{1}{3}x + \frac{1}{9} \\
\hline
3x+1 & -x^2 + 0 + 2 \\
 & -x^2 - \frac{1}{3}x + 0 \\
\hline
 & +\frac{1}{3}x + 2 \\
 & \frac{1}{3}x + \frac{1}{9} \\
\hline
 & 0 \quad 17/9
\end{array}
$$

$$
(-x^2+2) = \underbrace{\left(-\tfrac{1}{3}x+\tfrac{1}{9}\right)}_{Q_2}\underbrace{(3x+1)}_{R_2} + \underbrace{\frac{17}{9}}_{R_3}
$$

$$
(3x+1) = \underbrace{\frac{9}{17}(3x+1)}_{Q_3}\underbrace{\frac{17}{9}}_{R_3} + \underbrace{0}_{R_4}
$$

$$
\Longrightarrow \gcd_{\mathbb{Q}}\left(x^5+x^4+x^2+1,\ x^3+x+1\right) = \frac{17}{9} \quad ?
$$

Note: If $G(x)$ is a gcd for $A(x), B(x)$ then so is $c\,G(x)$ for any $c \neq 0 \in \mathbb{F}$.

So we say

$$
\gcd_{\mathbb{Q}}\left(x^5+x^4+x^2+1,\ x^3+x+1\right) = 1
$$

they are coprime (over $\mathbb{Q}$)

HW 5 due Friday.

Recall:
Division Algorithm
- given $f(x), g(x) \in \mathbb{F}[x]$ $\quad g(x) \neq "0"$
$\exists!$ $q(x), r(x)$ s.t.

$$f(x) = q(x)\,g(x) + r(x)$$

where $\deg(r) < \deg(g)$ OR $r(x) = "0"$.

Define $\gcd_{\mathbb{F}}(f,g)$ = any common divisor with largest degree.

HW 5: If $d(x), e(x)$ are gcd's of $f(x), g(x)$
Then
$$d(x) = k\,e(x)$$
for some $k \neq 0 \in \mathbb{F}$.

So... if we say gcd must be monic (highest coeff. = 1) then the gcd is UNIQUE.

Lemma: If $f(x) = q(x)g(x) + r(x)$ then

$$\gcd(f,g) = \gcd(g,r). \quad ///$$

Corollary: Euclidean Algorithm. (pulverizer)

- to compute $\gcd(f,g)$, divide and repeat:

$$f(x) = q_1(x)g(x) + r_1(x) \qquad \deg r_1 < \deg g$$
$$g(x) = q_2(x)r_1(x) + r_2(x) \qquad \deg r_2 < \deg r_1$$
$$\vdots$$
$$r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x) \qquad \deg r_k < \deg r_{k-1}$$
$$r_{k-1}(x) = q_{k+1}(x)r_k(x) + 0$$

DONE

$$\Longrightarrow \gcd(f,g) = r_k(x)$$

last nonzero remainder.

Example: Compute $\gcd(x^5+x^4+x^2+1,\ x^3+x+1)$.

$$(x^5+x^4+x^2+1) = \underbrace{(x^2+x-1)}_{Q_1}(x^3+x+1) + \underbrace{(-x^2+2)}_{R_1}$$
$$(x^3+x+1) = (-x)(-x^2+2) + (3x+1)$$
$$(-x^2+2) = -\tfrac{1}{3}\left(x-\tfrac{1}{3}\right)(3x+1) + 17/9$$
$$(3x+1) = \underbrace{\tfrac{9}{17}(3x+1)}_{Q}\tfrac{17}{9} + 0$$

$\Rightarrow \gcd(x^5+x^4+x^2+1,\ x^3+x+1) = \frac{17}{9} \quad (=1)$

So "the" gcd is 1

we say they are coprime.

> $\gcd(f,g) = 1$ means f, g are coprime

Exercise: show that

$$\gcd(x^3-4x^2+x+6,\ x^3-x^2-4x+4) = x-2$$

Important Idea:

If $\gcd(f(x), g(x)) = d(x)$,
then we can run Euc. Alg. backward
to find $a(x), b(x)$ such that

$$f(x)a(x) + g(x)b(x) = d(x)$$

($f(x)$, $g(x)$: ↑ ↑; $d(x)$: gcd)

Prop 6.10 in the text.

eg. $\overline{\frac{17}{9}} = \overline{(-x^2+2)} + \frac{1}{3}(x-\frac{1}{3})\overline{(3x+1)}$

$= \overline{(-x^2+2)} + \frac{1}{3}(x-\frac{1}{3})\left[\overline{(x^3+x+1)} + x\overline{(-x^2+2)}\right]$

$= \left(1 + \frac{1}{3}(x-\frac{1}{3})x\right)\overline{(-x^2+2)} + \frac{1}{3}(x-\frac{1}{3})\overline{(x^3+x+1)}$

$= \left[\overline{(x^5+x^4+x^2+1)} - (x^2+x-1)\overline{(x^3+x+1)}\right]$

$+ \frac{1}{3}(x-\frac{1}{3})\overline{(x^3+x+1)}$

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

$+ \left(\frac{1}{3}(x-\frac{1}{3}) - (x^2+x-1)\left(1+\frac{1}{3}(x-3)x\right)\right)\overline{(x^3+x+1)}$

Hence.

$1 = \frac{9}{17}\left(1+\frac{1}{3}(x-\frac{1}{3})x\right)\overline{(x^5+x^4+x^2+1)}$.

$+ \frac{9}{17}\left(\frac{1}{3}(x-\frac{1}{3}) - (x^2+x-1)\left(1+\frac{1}{3}(x-\frac{1}{3})x\right)\right)\overline{(x^3+x+1)}$

Done.