HW 5 due Fri, May 1st.

Any Questions ?

Last time we proved FTA:

Every $f(x) \in \mathbb{R}[x]$ of deg ≥ 1 has a root in $\mathbb{C}$.

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

Jargon: The field $\mathbb{C}$ is "algebraically closed."

But there is still an unresolved issue from the proof.

Given $f(x) \in \mathbb{R}[x]$ (or $\mathbb{C}[x]$), Laplace assumed that $\exists$ field $\mathbb{F} \supseteq \mathbb{C}$ and elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that

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

Jargon: We call such $\mathbb{F}$ a

"splitting field" for $f(x)$. ///

Gauss criticized the assumption, and provided 4 proofs of his own.
In my opinion, Gauss' proofs are not better, and the gap in Laplace's proof was filled in 1880s by Leopold Kronecker.

Kronecker's Theorem: Let $\mathbb{F}$ be a field. For any $f(x) \in \mathbb{F}[x]$ of degree $n \geq 1$, there exists some field $\mathbb{E}_1 \supseteq \mathbb{F}$ and a root $\alpha_1 \in \mathbb{E}_1$, so that

$$f(x) = (x - \alpha_1) g_1(x)$$

for some $g_1(x) \in \mathbb{E}_1[x]$. By repeating the construction we obtain fields

$$\mathbb{F} \subseteq \mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \cdots \subseteq \mathbb{E}_n$$ and

elements $\alpha_i \in \mathbb{E}_i$ such that

$$f(x) = (x-\alpha_1)\,g_1(x)$$
$$= (x-\alpha_1)(x-\alpha_2)\,g_2(x)$$
$$= (x-\alpha_1)\cdots(x-\alpha_n).$$

Thus $\mathbb{E}_n \supseteq \mathbb{F}$ is a splitting field for $f(x) \in \mathbb{F}[x]$. ///

Turns out that Kronecker's Theorem is closely related to "modular arithmetic."

<u>Def</u>: Fix $m \in \mathbb{Z}$, $m \geq 1$. Then for all $a, b \in \mathbb{Z}$ we define a relation

Gauss (1800).

$$a \underset{m}{\sim} b \iff m \mid (a-b).$$

"congruence modulo m"
equivalence
⋮

[More commonly: $a \equiv b \pmod{m}$.]

Facts (you may have seen before):

- $a \sim a$
- $a \sim b \iff b \sim a$

- $a \sim b$ & $b \sim c \Longrightarrow a \sim c$.
- $a \sim a'$ & $b \sim b'$

  $\Longrightarrow$ $a+b \sim a'+b'$ & $ab \sim a'b'$.

In other words

$$\mathbb{Z}_m := (\mathbb{Z}, +, \cdot, 0, 1, \underset{m}{\sim})$$

instead of "="

is a ring. Claim: This ring has exactly m elements. Specifically,

$$\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}.$$

e.g. $m \underset{m}{\sim} 0$

$m+1 \underset{m}{\sim} 1$ because $m \mid [(m+1) - m]$

$\vdots$

In other words, for all $n \in \mathbb{Z}$ there exists a unique integer $0 \leq r < m$ such that

$$n \underset{m}{\sim} r.$$

Proof: This r is just the unique

remainder of n modulo m. Indeed,

$$\begin{cases} n = qm + r \\ 0 \leq r < m \end{cases}$$

Then $n \underset{m}{\sim} r$ because

$$n - r = qm \Rightarrow m \mid (n-r) \quad \checkmark$$

///

Remarks:

- The rings $\mathbb{Z}_m$ are <u>bad</u> in some ways.

e.g. $2 \underset{6}{\not\sim} 0$ but $2 \cdot 3 = 6 \underset{6}{\sim} 0$!
$3 \underset{6}{\not\sim} 0$

Two nonzero elements multiply to 0.
In other words $\mathbb{Z}_6$ is not an <u>integral domain</u>.

- But in some ways they are <u>good</u>.

e.g. $3 \cdot 5 = 15 \underset{7}{\sim} 1$

Thus we could say that

$$3 \underset{7}{\sim} \frac{1}{5} \quad \& \quad 5 \underset{7}{\sim} \frac{1}{3}.$$

i.e. it is possible to "divide" by the elements 3 & 5 in the ring $\mathbb{Z}_7$.

This allows us to solve certain equations.

e.g. Solve $3x \underset{7}{\approx} 4$.

Answer: Divide both sides by 3.

$$\frac{1}{3} \cdot 3x \underset{7}{\approx} \frac{1}{3} \cdot 4$$

$$5 \cdot 3x \underset{7}{\approx} 5 \cdot 4$$

$$1x \underset{7}{\approx} 20$$

$$x \underset{7}{\approx} 6. \quad \checkmark$$

Theorem: For all $a, m \in \mathbb{Z}$, $m \geq 1$.

$$\frac{1}{a} \text{ exists in } \mathbb{Z}_m \iff \gcd(a, m) = 1.$$

In particular, if p is prime then $\mathbb{Z}_p$ is a field.

[This is our first example of a FINITE FIELD.]

<u>Proof</u>: Suppose $\gcd(a,m)=1$.

$$\underset{\text{Bézout}}{\Longrightarrow} \quad ax + my = 1 \qquad (x, y \in \mathbb{Z}).$$

$$\Longrightarrow \quad m \mid my = 1 - ax$$

$$\Longrightarrow \quad ax \underset{m}{\cong} 1$$

$$\Longrightarrow \quad x \underset{m}{\cong} \text{"}\frac{1}{a}\text{"}. \quad \checkmark$$

Conversely, suppose $ax \underset{m}{\cong} 1$ for some $x \in \mathbb{Z}$. Then by definition

$$m \mid (ax - 1)$$

Say $my = ax - 1 \qquad (y \in \mathbb{Z})$

$$1 = ax + my$$

$$\underset{(?)}{\Longrightarrow} \quad \gcd(a,m) = 1.$$

Q.E.D.

What does this have to do with Kronecker's Theorem?

Gauss' "congruence" of integers $\mathbb{Z}$ applies equally well to the ring $\mathbb{F}[x]$.

<u>Def</u>: Given $m(x) \in \mathbb{F}[x]$ of deg ≥ 0. For all $f(x), g(x) \in \mathbb{F}[x]$ we define the relation

$$f(x) \underset{m}{\sim} g(x) \iff m(x) \Big| \left[f(x) - g(x) \right].$$

For all the same reasons,

$$\mathbb{F}[x]_m = \left(\mathbb{F}[x], +, \cdot, 0, 1, \underset{m}{\sim} \right)$$

instead of "="

is a <u>ring</u>. It is not finite in general, but we have the following theorem: If $\deg(m) = n \geq 1$ then

$$\mathbb{F}[x]_m = \{ a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 : a_i \in \mathbb{F} \},$$

and these representations are unique.

<u>Proof</u>: For all $f(x) \in \mathbb{F}[x]$ you will show on HW5.4 that there exists a <u>unique</u> polynomial $r(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q(x)m(x) + r(x) \\ \deg(r) < \deg(m) = n. \end{cases}$$

Since $\deg(r) < n$ we have

$r(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

for some $a_i \in \mathbb{F}[x]$ and then

$$f(x) = q(x)m(x) + r(x)$$

$$f(x) \underset{m}{\sim} r(x)$$

$$f(x) \underset{m}{\sim} a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

///

Furthermore, if $p(x) \in \mathbb{F}[x]$ is a <u>prime</u> polynomial then for the same reasons as for $\mathbb{Z}$ one can show that

$\mathbb{F}[x]_p$ is a <u>field</u>.

[Note finite in general.].

This fact leads immediately to a proof of Kronecker's Theorem.

NEXT TIME!