HW5 due <u>now</u>.

"Cheat sheet for the fictional exam"
due Wed, May 6 (final day of class).

Today: HW5 Discussion + more.

Next week: Impossible Constructions
& the Gauss - Wantzel Theorem.

Problem 3: $\mathbb{F}$ field. for any
$f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0(x)$, $\exists$
$q(x), r(x) \in \mathbb{F}[x]$ such that

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

More generally, this is still true
if $f(x), g(x) \in R[x]$ for some <u>ring</u> R
where leading coefficient of $g(x)$
is ± 1 (more generally, any invertible
element of R).

(a) Prove that $q(x)$ & $r(x)$ are <u>unique</u>.

$$\begin{cases} f(x) = q_1(x)g(x) + r_1(x) \\ \deg(r_1) < \deg(g) \end{cases} \quad \Bigg| \quad \begin{cases} f(x) = q_2(x)g(x) + r_2(x) \\ \deg(r_2) < \deg(g). \end{cases}$$

We will prove $q_1(x) = q_2(x)$ & $r_1(x) = r_2(x)$.

First: $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$

$$(q_1 - q_2)g = (r_2 - r_1)$$

Assume for <u>contradiction</u> $q_1 \neq q_2$, so $q_1 - q_2 \neq 0(x)$. Since $g(x) \neq 0(x)$, this implies

$$\deg(r_2 - r_1) = \deg(q_1 - q_2) + \deg(g)$$
$$\geq \deg(g)$$

On the other hand we know that

$$\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\}$$
$$< \deg(g).$$

Contradiction. Hence $q_1(x) = q_2(x)$ and $(r_2 - r_1) = (q_1 - q_2)g$

$$r_2 - r_1 = 0$$

$$\Rightarrow \quad r_1(x) = r_2(x) \qquad \text{QED.}$$

(b) Strange but useful fact.

Suppose $R \subseteq \mathbb{F}$ subring of field.

Given $f(x) = q(x) g(x)$ for some

- $f(x), g(x) \in R[x]$
- $g(x)$ has leading coeff. ± 1
- $q(x) \in \mathbb{F}[x]$

Then I claim that in fact

$$q(x) \in R[x].$$

Let's apply this <u>before</u> we prove it.

Problem 4: Cyclotomic Polynomial

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \omega^k), \quad \omega = e^{2\pi i/n}.$$

By definition we have $\Phi_n(x) \in \mathbb{C}[x]$.

I claim that in fact $\Phi_n(x) \in \mathbb{Z}[x]$.

Induction on $n \geq 1$.

Base Case: $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ ✓

Induction: Fix $n \geq 2$ and assume that $\Phi_k(x) \in \mathbb{Z}[x]$ for all $1 \leq k < n$. Then we will show that $\Phi_n(x) \in \mathbb{Z}[x]$. Indeed, we have identity

$$x^n - 1 = \prod_{\substack{d \mid n \\ 1 \leq d \leq n}} \Phi_d(x).$$

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d \mid n \\ 1 \leq d < n}} \Phi_d(x)$$

$$f(x) = q(x)\, g(x).$$

We have

- $f(x) \in \mathbb{Z}[x]$
- By induction, each $\Phi_d(x)$, $d < n$, has integer coeffs (and leading coeff 1), hence $g(x) \in \mathbb{Z}[x]$ with leading coeff 1.
- $q(x) \in \mathbb{Q}[x]$.

$\xRightarrow[4(b)]{}$ Actually, $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$.

Proof of 4(b): $f(x) = q(x)g(x)$

Since $f(x), g(x) \in R[x]$, g leading coeff 1,
$\exists\, q'(x), r'(x) \in R[x]$ such that

$$\begin{cases} f(x) = q'(x)g(x) + r'(x), \\ \deg(r') < \deg(g). \end{cases}$$

On the other hand, in the larger ring $\mathbb{F}[x]$, we have

$$\begin{cases} f(x) = q(x)g(x) + 0(x), \\ \deg(0) < \deg(g). \end{cases}$$

Since these both hold in the ring $\mathbb{F}[x]$, we conclude from <u>uniqueness</u> that $q(x) = q'(x) \in R[x]$

$$\Longrightarrow q(x) \in R[x] \checkmark$$

Problem 6: Given fields $\mathbb{E} \supseteq \mathbb{F}$, suppose $\iota \in \mathbb{E}$ satisfies

$$\iota^2 \in \mathbb{F} \text{ but } \iota \notin \mathbb{F}.$$

[Think: $\mathbb{E} = \mathbb{C}$, $\mathbb{F} = \mathbb{R}$, $\iota = i$]

Then Define

$$\mathbb{F}(\iota) := \{ a + b\iota : a, b \in \mathbb{F} \}.$$

I claim:

- $\mathbb{F}(\iota)$ is a subfield of $\mathbb{E}$.

The hard part:

$$\frac{1}{a+b\iota} = \frac{1}{a+b\iota} \frac{a-b\iota}{a-b\iota}$$

$$= \frac{a-b\iota}{a^2 - \iota^2 b^2}$$

$$= \underbrace{\left(\frac{a}{a^2-\iota^2 b^2}\right)}_{\in \mathbb{F}} + \underbrace{\left(\frac{-b}{a^2-\iota^2 b^2}\right)}_{\in \mathbb{F}} \iota \quad \checkmark$$

Jargon: $\mathbb{F}(\iota) \supseteq \mathbb{F}$ is called a "Quadratic Field Extension."

- Also have a conjugation operator

$$(a+b\iota)^* := a - b\iota$$

satisfying the usual rules:

$$\alpha^* = \alpha \iff \alpha \in \mathbb{F}.$$

$$(\alpha+\beta)^* = \alpha^* + \beta^*$$

$$(\alpha\beta)^* = \alpha^* \beta^*$$

- Follows that for $f(x) \in \mathbb{F}[x]$, the roots $f(\alpha) = 0$, $\alpha \in \mathbb{F}(\iota)$, come in conjugate pairs:

$$f(\alpha) = 0 \iff (f(\alpha))^* = 0$$

$$\iff f^*(\alpha^*) = 0$$

$$\iff f(\alpha^*) = 0 \qquad ///$$

Strange Lemma:

Given $f(x) \in \mathbb{F}[x]$ of degree 3,

$f(x)$ has a root in $\mathbb{F}(\iota)$ $\implies$ $f(x)$ has a root in $\mathbb{F}$.

Proof: Suppose $f(\alpha) = 0$, $\alpha \in \mathbb{F}(\iota)$.

If $\alpha \in \mathbb{F}$ then we're done.

Otherwise, $\alpha^* \neq \alpha$ is another root.

Descartes' Theorem says

$$f(x) = (x-\alpha)(x-\alpha^*)\, q(x)$$

for some $q(x) \in \mathbb{F}(i)[x]$ of degree 1. But observe that

$$\begin{aligned} g(x) &:= (x-\alpha)(x-\alpha^*) \\ &= x^2 - (\alpha+\alpha^*)x + \alpha\alpha^* \\ &\in \mathbb{F}[x] \end{aligned}$$

because
$$(\alpha+\alpha^*)^* = \alpha+\alpha^*$$
$$(\alpha\alpha^*)^* = \alpha\alpha^*$$

$\Rightarrow \alpha+\alpha^* \in \mathbb{F}$ & $\alpha\alpha^* \in \mathbb{F}$.

We're in the situation of 4(b):

$$\underset{\mathbb{F}}{f(x)} = \underset{\mathbb{F}}{g(x)}\; \underset{\mathbb{F}(i)\ ?}{q(x)}$$

$$\Big\downarrow 4(b)$$

$$\mathbb{F} \checkmark$$

Hence $q(x) = ax+b$, $a, b \in \mathbb{F}$.

This implies

$$f\left(-\frac{b}{a}\right) = g\left(-\frac{b}{a}\right) q\left(-\frac{b}{a}\right) = 0$$

where $-\frac{b}{a} \in \mathbb{F}$.

QED.

What did we do?

Next Time we will prove that the classical construction problems

- double the cube
- trisect the angle
- construct the regular 7-gon

are impossible, by means of the following theorem:

Given $f(x) \in \mathbb{Q}[x]$ of degree 3, we will show that f(x) has a root in $\mathbb{Q}$sqrt $\Longrightarrow$ f(x) has a root in $\mathbb{Q}$.

Contrapositively:

f(x) has <u>no</u> root in $\mathbb{Q}$ $\Longrightarrow$ f(x) has <u>no</u> root in $\mathbb{Q}$sqrt.

We will use this to show that

$\sqrt[3]{2}$, $\cos\left(\frac{2\pi}{9}\right)$, $\cos\left(\frac{2\pi}{7}\right) \notin \mathbb{Q}$sqrt,

and it will follow that the classical construction problems are impossible.

Stay Tuned . . .