3032 Lecture 9 (11 Feb 2021)

Next week: no classes. (Feb break)

week after next: OH by appt/email

HW 4 due today

HW 5 due in two weeks

Today: irreducible polynomials

Fix a com unital ring R (domain)

<u>Defn:</u> $f \in R[x]$ is called <u>irreducible</u> over R if

- it is not a unit
- it cannot be factored as $f = a \cdot b$ with both a, b are non-units.

x^2+1 is irred over $\mathbb{R}$, but not over $\mathbb{C}$.

Compare: prime numbers in $\mathbb{Z}$.

<u>Lemma:</u> If R is a field, then every poly of $\deg = 1$ is irred

<u>Pf:</u> If $f = ab$ then $\deg(f) = \deg(a) + \deg(b)$
if $\deg(f) = 1$, then one of a, b has $\deg 0$, and so is a unit.

<u>Lemma:</u> Suppose $R = \mathbb{F}$ is a field. Then $f \in \mathbb{F}[x]$ of deg 2 or 3 is irred over $\mathbb{F}$ iff f it has no <u>roots</u> in $\mathbb{F}$.

$= $ zero.

<u>Pf:</u> • We proved last time that if a is a root of f, then

($\Rightarrow$) $f(x) = (x-a)\cdot q(x)$ for some q.

If $\deg f > 1$, then $\deg q > 0$ so q not a unit.

does not require $\deg f \leq 3$.

does not require R a field.

($\Leftarrow$) • Suppose f is reducible, i.e. $f = a\cdot b$, both non units. Then $\deg a, \deg b \geq 1$ (because $\mathbb{F}$ a field)

But $\underbrace{\deg f}_{\leq 3} = \underbrace{\deg a}_{\geq 1} + \underbrace{\deg b}_{\geq 1}$ so one of a,b has $\deg = 1$.

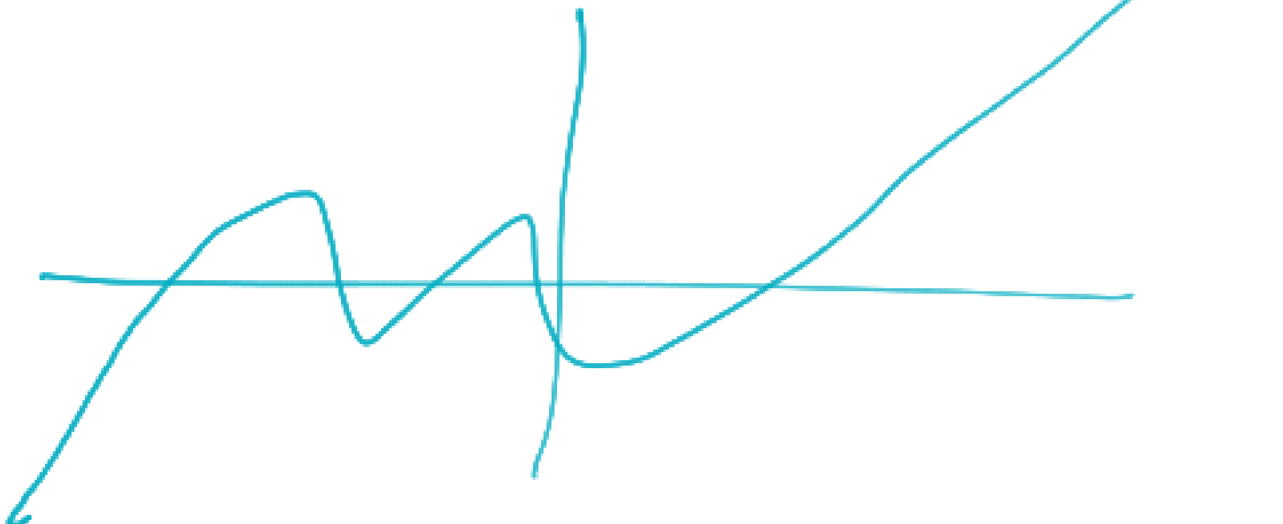
Suppose $a(x) = \alpha x + \beta$ then $-\frac{\beta}{\alpha} \in \mathbb{F}$ is a root of f. $\square$

Some lightning examples:

(High school): $\mathbb{F} = \mathbb{R}$.

- $x^2 + c$ is irred over $\mathbb{R}$ iff $c > 0$.
- every cubic is reducible over $\mathbb{R}$ (in fact, over $\mathbb{R}$ every poly of deg ≥ 3 is reducible.)
  (every poly of odd degree)

Pf: If $f(x) \in \mathbb{R}[x]$ has odd degree, then ($= a_n x^n + \ldots$)
the graph $y = \frac{f(x)}{a_n}$ must cross x-axis
because when $x \ll 0$,
$\frac{f(x)}{a_n} \ll 0$, and $\frac{f(x)}{a_n} \gg 0$
if $x \gg 0$.



So must have a zero by continuity.

Pythagorus: • x^2-2 is irred over $\mathbb{Q}$.

i.e. $\sqrt{2}$ is irrational.

• $\overset{=:f(x)}{x^3-x+1}$ is irred over $\mathbb{F}_3 = \mathbb{Z}/3 = \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$

number thy ↓ topologists ↓ physicist ↙

Pf: if $a \in \mathbb{F}_3$, then $a^3 = a$ by FLT,

so $f(a) = 1$ for all $a \in \mathbb{F}_3$. So no roots.

FLT: if $a \in \mathbb{F}_p$, • $a^{p-1} = 1$ if $a \neq 0$

• $a^p = a$ even if $a = 0$.

$a^3 - a + 1 = a - a + 1 = 1$. So a not a root of f for all a.

Thm (Gauss' Lemma): A poly in $\mathbb{Z}[x]$ is irred over $\mathbb{Z}$ iff it is irred over $\mathbb{Q}$.

Not quite true. 3 is irred over $\mathbb{Z}$, but unit over $\mathbb{Q}$.
But this is the only thing preventing it from being true.

Actual statement: If $f(x) \in \mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ as

$$f(x) = a(x) \cdot b(x)$$

then there are nonzero rational numbers α, β s.t. for $A(x) := \alpha \cdot a(x)$, $B(x) := \beta \cdot b(x)$,

$$f(x) = A(x) \cdot B(x) \text{ and } A(x), B(x) \in \mathbb{Z}[x].$$

Pf: Let $f \in \mathbb{Z}[x]$, $f = ab$ w/ $a, b \in \mathbb{Q}[x]$.

Let $a(x) = a_n x^n + a_{n-1} x^{n-1} + \dots$ So by clearing denominators, can write

$$a(x) = \frac{a'(x)}{m}, \quad b(x) = \frac{b'(x)}{n}$$

where $m, n \in \mathbb{Z}$, $m, n > 0$ and $a', b' \in \mathbb{Z}[x]$.

So $m \cdot n \cdot f(x) = a'(x)\, b'(x)$ is a factorization over $\mathbb{Z}$.

If $m \cdot n = 1$, certainly done.

Otherwise, $\exists$ prime p so that $p \mid mn$.

$$\Big[\ \underbrace{m \cdot n \cdot f(x) \overset{(\star)}{=} a'(x)\, b'(x)}_{\text{in } \mathbb{Z}[x]} \quad \text{and } p \text{ divides } m \cdot n \Big]$$

Reduce equation $(\star)$ modulo p.

$(\star \bmod p)$ $\quad 0 = [a'](x) \cdot [b'](x)$

where $[a'] \in \mathbb{Z}_p[x]$ whose coefs are the mod p reductions of the coefs of a'.

But $\mathbb{Z}_p$ is a field so $\mathbb{Z}_p[x]$ is a domain, so

$(\star \bmod p) \Rightarrow$ At least one of $[a']$, $[b'] = 0$.

Say $[a'] = 0$. i.e. every coef of $a' \equiv 0 \bmod p$

i.e. $a'(x) = p \cdot a''(x)$ for some $a'' \in \mathbb{Z}[x]$.

$N := m \cdot n$

Review: We just proved that if $N f(x) = a'(x) b'(x) \in \mathbb{Z}[x]$

and $N = pN'$ then $p \mid$ one of a', b'

So $$N' f(x) = a''(x) \cdot b''(x) \in \mathbb{Z}[x].$$

where either $a'' = a'$, $b'' = \frac{b'}{p}$

or $a'' = \frac{a'}{p}$, $b'' = b'$

Now repeat the process. $\square$

Cor: For monic polys in $\mathbb{Z}[x]$

if $$\underbrace{\overset{f}{\overset{\shortparallel}{(x^q + \dots)}}}_{\in\, \mathbb{Z}[x]} = \overset{a}{\overset{\shortparallel}{(x^s + \dots)}}\ \overset{b}{\overset{\shortparallel}{(x^r + \dots)}}$$

is a factorization in $\mathbb{Q}[x]$,

then it is already a factorization in $\mathbb{Z}[x]$.

We know $\exists\ \underset{\in\, \mathbb{Z}[x]}{A, B}$ s.t. $f = AB$ and $A = \alpha a$, $B = \beta b$.

But look at leading coefs.

E.g.: Quick proof that $\sqrt{2}$ is irrat:

If $\sqrt{2} \in \mathbb{Q}$ then $x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ would be a factorization over $\mathbb{Q}$, hence over $\mathbb{Z}$.

So suffices to show that $\sqrt{2} \notin \mathbb{Z}$.

But if $n \in \mathbb{Z}$ and $|n| > 1$ then $|n^2| > 2$.

And $0, 1, -1$ also don't work.

Similarly, $\sqrt[3]{15}$ is irrat. If $\sqrt[3]{15} \in \mathbb{Q}$, then $\sqrt[3]{15} \in \mathbb{Z}$ by factoring $x^3 - 15$.

If $|x| \geq 3$ then $|x^3| \geq 27$ and so $x^3 \neq 15$

and $0^3 \neq 15$

$\pm 1^3 \neq 15$

$\pm 2^3 \neq 15$.

Cor: If $f = x^n + a_n x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ then any root of f is an integer dividing a_0.

Pf: If α is a root of f

then $f(x) = (x-\alpha)\cdot(x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0)$

both monic, and so monic $\in \mathbb{Z}[x]$.

$-\alpha \cdot b_0 = a_0$ in $\mathbb{Z}$.

both integers.

Eg: $f(x) = x^4 - 2x^2 + 8x + 1$

is irred over $\mathbb{Q}$.

Pf: If it factors, either (linear) $\times$ (cubic)

or (quad) $\times$ (quad).

(a) Since f monic, constant term is 1,

any root must be integer dividing 1.

$f(1) = 8$, $f(-1) = -8$. So no roots.

(b) If $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ $a, b, c, d \in \mathbb{Z}$

$a + c = 0$

$ac + b + d = -2$

$ad + bc = 8 \Rightarrow a + c = \pm 8$ oops!

$bd = 1. \Rightarrow b = d = \pm 1$

Thm [Eisenstein's criterion]:

If $p \in \mathbb{Z}$ is prime and

$f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$

s.t. $a_n \not\equiv 0 \pmod p$ but $a_i \equiv 0 \ (p)$ for $i<n$

and $a_0 \not\equiv 0 \pmod{p^2}$

Then f is irred in $\mathbb{Q}[x]$.

Pf: Enough to show it does not factor non constantly over $\mathbb{Z}$.

Suppose for contradiction that

$f(x) = (b_r x^r + \ldots + b_0)(c_s x^s + \ldots + c_0)$

Then $b_r c_s = a_n \not\equiv 0 \bmod p$, so $b_r, c_s \not\equiv 0 \ (p)$.

$b_0 c_0 = a_0 \equiv 0 \bmod p$

$\not\equiv 0 \bmod p^2.$

So one, but not both, of $b_0, c_0 \equiv 0 \ (p)$.

Say $c_0 \equiv 0 \ (p)$ and $b_0 \not\equiv 0 \ (p)$.

Let m be the smallest number so that $c_m \not\equiv 0 \ (p)$. (m exists because $c_s \not\equiv 0 \ (p)$.)

$m \neq 0$. $m \leq s$

$a_m = b_0 c_m + b_1 c_{m-1} + \dots + b_m c_0$

$c_{m-1}, c_{m-2}, \dots \equiv 0 \ (p)$,

find $a_m \not\equiv 0 \ (p)$. So $m = n$.

$s \geq m = n = \deg f$.

so factorization was trivial.

One of my favourite polynomials:

Let $n \in \mathbb{N}$. The n^{th} quantum integer

is $$qi_n(x) = [n]_x \in \mathbb{Z}[x]$$

$$\| $$

$$\frac{x^n - 1}{x - 1} = \underbrace{x^{n-1} + x^{n-2} + \dots + \overset{x}{\overset{\|}{x^1}} + \overset{1}{\overset{\|}{x^0}}}_{n \text{ terms, all coef} = 1.}$$

$$qi_n(1) = n.$$

Proposition: If p is prime, then $\Phi_p(x)$ is irred in $\mathbb{Q}[x]$.

Pf: Iff $\Phi_p(x) = a(x)\,b(x)$ $\quad \Phi_p(x+1) = a(x+1)b(x+1)$

So I'll actually prove $\Phi_p(x+1)$ is irred.

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x^1 + \cancel{\underbrace{\binom{p}{p}}_{=1}\underbrace{x^0}_{=1} - 1}}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \overbrace{\binom{p}{p-1}}^{= p}.$$

Because p is prime, $p \mid \binom{p}{i}$ for $0 < i < p$.

So Eisenstein's criterion applies. $\square$