Lecture 14 Feb 10, 2021

- Irreducible polys.

If F is a field, which polys in $F[x]$ are irreducible?

- depends on properties of F.

<u>Thm.</u> (remainder/factor thm).
If $f(x) \in F[x]$ (F a field) and $a \in F$, then

$$f = q(x-a) + r$$

where $r = f(a)$.

In particular $f(a) = 0$ iff $(x-a) \mid f$.

<u>Pf.</u> Apply long division to divide f by $(x-a)$, so $\deg r < 1$.

So $r \in F$ and $f(a) = q(a-a) + r$

so $r = f(a)$.

Cor. If $f \in F[x]$ with $\deg f \leq 3$ f nonzero, nonconstant
and f has no root in F, then
f is irreducible in $F[x]$.

Pf. If f is reducible, $f = gh$
with $\deg g, \deg h \geq 1$.
So g or h has degree 1; say
g does, so $g = (ax+b)$ $a, b \in F$.
$a \neq 0$.

$(ax+b) \mid f$, so
$(x + \frac{b}{a}) \mid f$.

So f has a root $(-\frac{b}{a})$ in F.

Prop (rational root thm)
Let R be a UFD with field of fractions K.
Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$.

If $f(\frac{r}{s})=0$ where $r,s\in R$ $s\neq 0$

then if $\gcd(r,s)=1$, we have

$r \mid a_0$ and $s \mid a_n$.

Pf. $f = a_n(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + \cdots + a_1(\frac{r}{s}) + a_0$

$=0$. Multiply by s^n -

$0 = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n$.

Notice $r \mid a_0 s^n$ and $\gcd(r,s)=1$

$\Rightarrow r \mid a_0$.

Also $s \mid a_n r^n$ so $s \mid a_n$.

Ex. $\frac{4}{11}x^3 + \frac{5}{11}x + 1 \in \mathbb{Q}[x]$.

does it have a root in $\mathbb{Q}$? Let $R=\mathbb{Z}$.

Consider $4x^3 + 5x + 11 \in \mathbb{Z}[x]$ instead.

Rational root thm says any root $\frac{r}{s}$

with $\gcd(r,s)=1$ has $r \mid 11$ and $s \mid 4$.

Check all possibilities - no roots.

So the polynomial is irr. over $\mathbb{Q}$.

Next: Eisenstein criterion.

<u>Prop.</u> Let R be a UFD, field of fractions K.
Suppose $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$.
Let $p \in R$ be prime s.t.
$p \nmid a_n$, $p \mid a_i$ $0 \le i \le n-1$, $p^2 \nmid a_0$.
Then f is irreducible over K.

<u>Pf.</u> Since p is prime in R, (p) is a prime ideal, so $\overline{R} = R/(p)$ is a domain.
We have the homomorphism

$$\phi : R[x] \longrightarrow \overline{R}[x]$$
$$g \longmapsto \overline{g}$$

Suppose $f = gh$ $\quad g, h \in F[x]$
$\deg g \ge 1$ $\quad \deg h \ge 1$.

Gauss's Lemma says we can adjust

g and h by constants in R to get $g, h \in R[x]$.

So now $\overline{f} = \overline{g}\,\overline{h}$

$$\overline{f} = \overline{a_n} x^n \qquad \overline{a_n} \neq 0.$$

in $\overline{R}[x]$ since $\overline{R}$ is a domain, we get $\overline{g} = \overline{b_\ell} x^\ell$ $\overline{h} = \overline{c_m} x^m$.

Since $\ell + m = n$, $\deg \overline{g} \geq 1$ $\deg \overline{h} \geq 1$.

So $\overline{b_0} = 0$ and $\overline{c_0} = 0$.

Here $g = b_\ell x^\ell + \cdots + \underline{b_0} \in R[x]$

$h = c_m x^m + \cdots + \underline{c_0} \in R[x]$.

$f = gh = \cdots\cdots + b_0 c_0$

So $b_0 c_0 = a_0$.

but $p \mid b_0$, $p \mid c_0 \Rightarrow p^2 \mid a_0$.

this is a contradiction.

Ex. $x^n + 4x + 2 \in \mathbb{Q}[x]$.

Apply Eisenstein with $p = 2$

$x^n + 4x + 2$ is irreducible over $\mathbb{Q}$ for any $n \geq 2$.

Ex. Let $f = x^3 + 5x^2y^2 + y$

$\in \mathbb{Q}[x,y] = (\mathbb{Q}[y])[x]$

take $R = \mathbb{Q}[y]$ as a UFD.

field of fractions is $\mathbb{Q}(y) = K$

Apply Eisenstein with $y \in \mathbb{Q}[y]$ which is prime.

$$f = 1\,x^3 + (5y^2)\,x^2 + y\,x^0.$$

So Eisenstein says f irreducible in $\mathbb{Q}(y)[x]$.

But then f is irreducible in $\mathbb{Q}[y][x]$
$= \mathbb{Q}[y,x]$. Since $\text{content}(f) = \gcd(1, 5y^2, y)$
$= 1$.

<u>Ex.</u> Fix prime $p \in \mathbb{Z}$ and consider

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$
$\in \mathbb{Q}[x]$.

We want to show irreducibility over $\mathbb{Q}$.

Notice $f = \dfrac{x^p - 1}{x - 1}$

i.e. $\underline{x^p} - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$

Take $g(x) = f(x+1)$

then $g(x) = f(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1}$

$$= \frac{(x+1)^p - 1}{x}$$

$$= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x}{x}$$

$$= \underline{x^{p-1}} + \underset{\substack{\shortparallel \\ p}}{\binom{p}{1}}x^{p-2} + \cdots + \underset{\substack{\shortparallel \\ \underline{p}}}{\binom{p}{p-1}}.$$

Eisenstein applies using the prime p. Since $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is a multiple of p for $i \neq 0$, $i \neq p$.

So g is irreducible over $\mathbb{Q}$.

So f is " " ".

<u>Prop.</u> (reduction mod p).

Let R be integral domain,

let $f \in R[x]$,

$f = a_n x^n + \cdots + a_0 \in R[x]$

Assume gcd $(a_0, \ldots, a_n) = 1$.

If $p \in R$ is prime with

$p \nmid a_n$

Then if $\bar{f} \in R/(p)[x]$ is

irreducible, so is f in $R[x]$.

Pf (omitted)

<u>Ex.</u> $f: x^4 + x + 1 \in \mathbb{Z}[x]$.

Let $p = 2$. Reduce mod p -

$\bar{f} = x^4 + x + 1 \in \mathbb{Z}/(2)[x]$.

Check - only irreducible in $\mathbb{Z}/(2)(x)$ of degree 2 are x^2+x+1.

and $(x^2+x+1)(x^2+x+1) = x^4+x^2+1 \neq \bar{f}$.

Also $\bar{f}$ has no roots in $\mathbb{Z}/(2)$.

So $\bar{f}$ is irreducible in $\mathbb{Z}/(2)(x]$.

f is irreducible in $\mathbb{Z}[x]$.

(also in $\mathbb{Q}[x]$).