# Lecture 22: Examples of Eisenstein's criterion

Friday, May 25, 2018 10:24 AM

In the previous lecture we proved Eisenstein's irreducibility criterion; let's see one example:

<u>Ex.</u> Prove that $f(x) = \frac{5}{2}x^6 - \frac{4}{3}x^3 + 7x - \frac{3}{11}$ is irreducible in $\mathbb{Q}[x]$.

<u>Pf.</u> We multiply by a common denominator in order to get a poly. with integer coeff. Notice that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $66 f(x)$ is irreducible in $\mathbb{Q}[x]$ as $66$ is a unit in $\mathbb{Q}[x]$.

$$66 f(x) = \underset{2\nmid}{33\times 5}\, x^6 - \underset{2|}{22\times 4}\, x^3 + \underset{2|}{66\times 7}\, x - \underset{\substack{2| \\ \text{and} \\ 4\nmid}}{6\times 3}$$

and so by Eisenstein's irreducibility criterion $66 f(x)$ is irreducible in $\mathbb{Q}[x]$. ∎

<u>Ex.</u> Suppose $p$ is a prime. Then $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$.

<u>Pf.</u> At the first glance, Eisenstein's criterion does not seem suitable

# Lecture 22: An application of Eisenstein's criterion

Friday, May 25, 2018 10:36 AM

for this problem. Let's have another look at the given polynomial:

$f(x) = x^{p-1} + \cdots + x + 1$. It looks like a "partial sum of a geometric series". So $f(x) = \dfrac{x^p - 1}{x-1}$ (Consider $(x-1)f(x)$

$= x f(x) - f(x) = (x^p + x^{p-1} + \cdots + x) - (x^{p-1} + \cdots + x + 1) = x^p - 1$.)

Hence $f(y+1) = \dfrac{(y+1)^p - 1}{y}$

$$= \frac{\left(y^p + \binom{p}{p-1} y^{p-1} + \cdots + \binom{p}{i} y^i + \cdots + \binom{p}{1} y + 1\right) - 1}{y}$$

$$= y^{p-1} + \binom{p}{p-1} y^{p-2} + \cdots + \binom{p}{i} y^{i-1} + \cdots + \binom{p}{2} y + p$$

$\forall\ 1 \le i \le p-1$, $p \mid \binom{p}{i}$ and $p^2 \nmid p$. Hence by Eisenstein's criterion

$f(y+1)$ is irreducible in $\mathbb{Q}[y]$. $(*)$

- If $f(x)$ is not irreducible in $\mathbb{Q}[x]$, then (as $\deg f = p-1 \ge 1$)

  $f(x) = g_1(x)\, g_2(x)$ for some $g_i(x) \in \mathbb{Q}[x]$ and $\deg g_i \ge 1$.

And so $f(y+1) = g_1(y+1)\, g_2(y+1)$ and $\deg_y g_i(y+1) = \deg_x g_i(x) \ge 1$,

which contradicts $(*)$. ∎

# Lecture 22: F[x] is a UFD.

Friday, May 25, 2018 10:50 AM

Before proving Eisenstein's criterion, we pointed out that any positive degree poly. in $F[x]$ can be written as a product of irreducibles in a unique way.

Def. An integral domain $D$ is called a Unique Factorization Domain (UFD) if any non-zero non-unit element can be written as a product of irreducible; and the irreducible factors are unique up to reordering and multiplying by a unit.

Ex. $\mathbb{Z}$ is a UFD; $6 = 2 \times 3 = (-3) \times (-2)$

reordering and multiplying by a unit

Theorem. PID $\Rightarrow$ UFD.

Pf. (Existence) Rough idea: for $d \in D$, non-zero and non-unit, we use the following steps:

- If $d$ is irreducible, we are done
- If not, $\exists\, d_1, d_1'$ non-zero, non-unit st. $d = d_1 d_1'$.
- Repeat this for $d_1$ and $d_1'$.

# Lecture 22: PID implies UFD; existence

Friday, May 25, 2018 11:03 AM

If this process ends, it means $d$ has been written as a product of irreducible. How can we show that this process ends?

Before proving the general case, let's consider $F[x]$ where $F$ is a field. In this case, a polynomial $f(x)$ of $\deg f = d$ cannot be written as a product of more than $d$ polynomials of positive degree. Hence this process ends after at most $\deg f$ steps.

Existence. Suppose to the contrary that this process does not end. So $\exists\, d_i, d_i'$: non-zero non-units s.t.

$$d = d_1 d_1', \quad d_1 = d_2 d_2', \quad d_2 = d_3 d_3', \quad \dots$$

$$\langle d \rangle \underset{\substack{\Updownarrow \\ d_1' \text{ is} \\ \text{not a} \\ \text{unit}}}{\subsetneq} \langle d_1 \rangle \underset{\substack{\Updownarrow \\ d_2' \text{ is} \\ \text{not a} \\ \text{unit}}}{\subsetneq} \langle d_2 \rangle \subsetneq \cdots .$$

(We will continue next time)