Lecture 01: Recall some results from 200a

Wednesday, January 9, 2019 6:26 PM

Towards the end of math 200a we mentioned that certain ring properties can be passed on to the ring of polynomials; for instance we proved Hilbert's basis theorem:

<u>Hilbert's basis theorem</u>. A is Noetherian $\Leftrightarrow$ $A[x]$ is Noetherian.

We pointed out that being a PID is not such a property; in fact we showed $A[x]$ is a PID $\Leftrightarrow$ A is a field.

Today we will prove:

<u>Theorem</u>. D is a UFD $\Leftrightarrow$ $D[x]$ is a UFD.

We will prove this in several steps. Let's recall that, if D is a UFD, for any irreducible element p, we can define the p-valuation; and we have

$$a = bu \text{ for some } u \in D^\times \Leftrightarrow aD^\times = bD^\times$$

$$\Leftrightarrow \forall \text{ irred. } p,\ v_p(a) = v_p(b).$$

We can define the g.c.d. of $a_1, \ldots, a_n$; and we explored its properties. For a polynomial $f(x) := a_0 + a_1 x + \cdots + a_n x^n \in D[x]$,

Lecture 01: Gauss lemma; it's important consequence

Wednesday, January 9, 2019 6:44 PM

we defined its content $c(f) := \gcd(a_0, \dots, a_n)$; and proved

Gauss's lemma. $c(f\,g) = c(f)\,c(g)$.

We said a polynomial is primitive if its content is $[1]$.

Using Gauss's lemma we proved:

Theorem. Suppose D is a UFD and F is its field of fractions. Suppose $f(x) \in D[x]$, $f(x) = f_1(x) \cdot \dots \cdot f_m(x)$ for some $f_i(x) \in F[x]$. Then $\exists\, a_i \in F$ s.t.

(1) $a_1 \cdots a_m = 1$ (2) $\bar{f}_i(x) := a_i f_i(x) \in D[x]$ for $1 \le i \le m$;

in particular $f(x) = \bar{f}_1(x) \cdot \bar{f}_2(x) \cdot \dots \cdot \bar{f}_n(x)$, $\bar{f}_i(x) \in D[x]$,

and $\deg f_i = \deg \bar{f}_i$.

Corollary. Suppose D is a UFD and F is a field of fractions. Suppose $f(x) \in D[x]$, $\deg f \ge 1$, and f is reducible in $F[x]$. Then $f(x)$ is reducible in $F[x]$.

For the rest of this lecture D is an integral domain and F is its field of fractions.

Lecture 01: Irreducibility and constant polynomials

Wednesday, January 9, 2019 6:57 PM

<u>Lemma</u>. Suppose $d \in D$. Then d is irreducible in D if and only if d is irreducible in $D[x]$.

<u>Pf.</u> ($\Rightarrow$) $\left.\begin{array}{l} d = f(x)\,g(x) \Rightarrow \deg d = \deg f + \deg g \\ d \in D \setminus \{0\} \end{array}\right\} \Rightarrow$

$0 = \deg f + \deg g \Rightarrow \deg f = \deg g = 0 \Rightarrow f, g \in D.$

$\left.\begin{array}{l} d \text{ is irreducible in } D \\ d = f \cdot g \\ f, g \in D \end{array}\right\} \Rightarrow f \in D^\times \text{ or } g \in D^\times$

$\Rightarrow f \in D[x]^\times$ or $g \in D[x]^\times$.

($\Leftarrow$) $\left.\begin{array}{l} d = a \cdot b \\ d \text{ irr. in } D[x] \end{array}\right\} \Rightarrow a \in D[x]^\times$ or $b \in D[x]^\times$

$\Rightarrow a \in D^\times$ or $b \in D^\times$. ■

<u>Lemma</u>. If $D[x]^\times$ is a UFD, then D is a UFD.

<u>Pf.</u> <u>Existence</u>. For $d \in D \setminus (D^\times \cup \{0\})$, we have that $d \in D[x] \setminus (D[x]^\times \cup \{0\})$; and so there are irred. $p_1, \ldots, p_m$ in $D[x]$ s.t. $d = p_1 \cdot \ldots \cdot p_m$. Comparing degrees of both sides we get $0 = \sum_{i=1}^{m} \deg p_i$; and so $\deg p_i = 0$ which means $p_i \in D \setminus \{0\}$. By the previous lemma we deduce that p_i's are irred. in D

Lecture 01: Being prime and constant polynomials

Friday, January 11, 2019 9:14 AM

<u>Uniqueness</u>. Suppose $p_1 \cdots p_m = q_1 \cdots q_\ell$, and p_i's and q_j's are irred. in D. Then by the previous lemma, p_i's and q_j's are irr. in $D[x]$. Since $D[x]$ is a UFD, p_i's and q_j's are the same up to reordering and multiplying by elements of $D[x]^\times = D^\times$ and claim follows. ∎

<u>Remark</u>. In lecture we gave an alternative argument:

<u>Recall</u>. Suppose in an integral domain D any element of $D \setminus (D^\times \cup \{0\})$ can be written as a prod. of irred. Then D is a UFD if and only if any irred. is prime.

Next we proved the following lemma which gives us uniqueness.

<u>Lemma</u>. Suppose $p \in D$. Then p is prime in D if and only if p is prime in $D[x]$.

<u>Pf.</u> p is prime in $D \iff pD \in \operatorname{Spec}(D)$

$\iff (D/pD)[x] \simeq D[x]/pD[x]$ is an integral domain

$\iff pD[x] \in \operatorname{Spec}(D[x]) \iff p$ is prime in $D[x]$. ∎

Lecture 01: Irreducibility in D[x] and F[x]

Friday, January 11, 2019 9:41 AM

__Proposition__. Suppose D is a UFD and F is its field of fractions. Suppose $f(x) \in D[x]$ is primitive and $\deg f \geq 1$. Then $f(x)$ is irred. in $D[x]$ if and only if $f(x)$ is irred. in $F[x]$.

__Pf.__ ($\Rightarrow$) If not, then $\exists\, g, h \in F[x]$ s.t. $\deg g, \deg h \geq 1$ and $f(x) = g(x)h(x)$. And so $\exists\, c \in F^\times$ s.t. $c\, g(x) \in D[x]$ and $c^{-1} h(x) \in D[x]$, which implies f is not irred. in $D[x]$.

($\Leftarrow$) $\left.\begin{array}{l} \textcircled{1}\; f(x) = g(x)h(x) \text{ for some } g, h \in D[x] \\ f(x) \text{ irr. in } F[x] \end{array}\right\} \Rightarrow$ either $g(x) \in F[x]^\times$ or $h(x) \in F[x]^\times$

$\Rightarrow$ either $g(x) \in D \setminus \{0\}$ or $h(x) \in D \setminus \{0\}$ ②.

Since f is primitive, by ① and ② we deduce that either $g \in D^\times$ or $h \in D^\times$; and so f is irreducible in $D[x]$. ∎

__Pf of the main theorem__ (D: UFD $\Rightarrow D[x]$: UFD.)

__Existence__. Suppose $f(x) \in D[x] \setminus (D^\times \cup \{0\})$. If $\deg f = 0$, then $f \in D \setminus (D^\times \cup \{0\})$. Since D is a UFD, $f = p_1 \cdots p_m$ for some p_i's that are irred. in D. Hence p_i's are irred. in $D[x]$. Next we

Lecture 01: D UFD implies D[x] UFD

Friday, January 11, 2019 4:07 PM

assume $\deg f \geq 1$. Let $d \in D$ be s.t. $f(x) = d\,\overline{f}(x)$ where $\overline{f}(x)$ is primitive. Since D is a UFD, $\exists\, u \in D^{\times}$ and q_i's that are irred. in D s.t. $d = u q_1 \cdots q_\ell$. Let F be the field of fractions of D. Since $F[x]$ is a PID, it is a UFD. So $\exists\, p_i$'s that are irred. in $F[x]$ and $\overline{f}(x) = p_1(x) \cdots p_m(x)$. By a theorem that we proved in 200a, $\exists\, c_i \in F$ s.t. $\prod_{i=1}^{m} c_i = 1$ and $c_i p_i \in D[x]$.

$$\Rightarrow \overline{f}(x) = \underbrace{\overset{\overline{p}_1(x)}{(c_1 p_1(x))}}_{\text{in } D[x]} \cdot \underbrace{\overset{\overline{p}_2(x)}{(c_2 p_2(x))}}_{\text{in } D[x]} \cdot \ldots \cdot \underbrace{\overset{\overline{p}_m(x)}{(c_m p_m(x))}}_{\text{in } D[x]}$$

$\overline{f}$ is primitive

$\Rightarrow \overline{p}_i(x)$ is primitive (1)

$p_i(x)$ is irred. in $F[x] \Rightarrow \overline{p}_i(x) = c_i\, p_i(x)$ is irred. in $F[x]$ (2)

(1) and (2) and the previous proposition imply that $\overline{p}_i(x)$ is irred. in $D[x]$. And so

$$f(x) = u q_1 \cdots q_\ell \cdot \overline{p}_1 \cdots \overline{p}_m, \quad u \in D^{\times}, \ q_i\text{'s and } \overline{p}_j\text{'s are}$$

irred. in $D[x]$.

<u>Uniqueness</u>. Since we have already proved the existence, to get the

Lecture 01: D UFD implies D[x] UFD

Friday, January 11, 2019 4:32 PM

uniquess it is enough to show that any irred. $p \in D[x]$ is prime.

- If $\deg p = 0$, then $p \in D$.

$$\left.\begin{array}{l} p \in D \\ p \text{ irred. in } D[x] \end{array}\right\} \Rightarrow \left.\begin{array}{l} p \text{ irred. in } D \\ D \text{ UFD} \end{array}\right\} \Rightarrow p \text{ prime in } D$$

$$\Rightarrow p \text{ prime in } D[x].$$

- If $\deg p \geq 1$, then $p(x) = c \cdot \bar{p}(x)$ for some $c \in D$ and a primitive poly. $\bar{p}$. Since p is irred. and $\deg \bar{p} \geq 1$, c is a unit in $D[x]$; and so $c \in D^{\times}$. Thus $p(x)$ is primitive.

$$\left.\begin{array}{l} p: \text{primitive}, \deg p \geq 1 \\ p: \text{irred. in } D[x] \end{array}\right\} \Rightarrow \left.\begin{array}{l} p: \text{irred. in } F[x] \\ F[x] \text{ UFD} \end{array}\right\} \Rightarrow p: \text{prime in } F[x].$$

We need to show p is prime in $D[x]$. So suppose

$$\left.\begin{array}{l} p(x) \mid f(x) g(x) \ (\text{in } D[x]) \\ f, g \in D[x] \end{array}\right\} \Rightarrow \left.\begin{array}{l} p(x) \mid f(x) g(x) \ (\text{in } F[x]) \\ p: \text{prime in } F[x] \end{array}\right\} \Rightarrow$$

either $p \mid f$ (in $F[x]$) or $p \mid g$ (in $F[x]$). W.L.O.G let's assume $p \mid f$ in $F[x]$; that means $f(x) = p(x) q(x)$ for some $q(x) \in F[x]$. So $\exists a \in D \setminus \{0\}$ s.t. $a f(x) = p(x) \tilde{q}(x)$

where $\tilde{q}(x) \in D[x]$. By Gauss's lemma, $a\, c(f) = c(p)\, c(\tilde{q})$
$= c(\tilde{q})$.

$\Rightarrow \tilde{q} = a \cdot a' \cdot \bar{q}(x)$ for some $a' \in D \setminus \{0\}$ and $\bar{q}(x)$ is primitive.

$\Rightarrow a\, f(x) = p(x) \cdot a \cdot a' \cdot \bar{q}(x) \Rightarrow f(x) = p(x)\, \underbrace{(a' \bar{q}(x))}_{\text{in } D[x]}$

$\Rightarrow p(x) \mid f(x)$ in $D[x]$; and claim follows. $\blacksquare$

How can we say if a given polynomial is irreducible or not?

In general this is not an easy task.

<u>Proposition</u>. Suppose D is a UFD and F is its field of fractions. Suppose $f(x) \in D[x]$ is a polynomial of degree $n \geq 1$. Suppose $\mathfrak{a} \trianglelefteq D$ and $f(x)$ cannot be written as a product of two polynomials of degree $< n$ in $(D/\mathfrak{a})[x]$. Then $f(x)$ is irreducible in $F[x]$; moreover if $f(x)$ is primitive, then $f(x)$ is irreducible in $D[x]$.

<u>Pf</u>. Suppose to the contrary that $f(x) = g(x)\, h(x)$ for some $g, h \in F[x]$ with degree ≥ 1. By a result that we have

proved earlier, $\exists c \in F^{\times}$ s.t. $\bar{g}(x) = c\, g(x) \in D[x]$ and

$\bar{f}(x) = c^{-1} f(x) \in D[x]$. So $f(x) = \bar{g}(x) \cdot \bar{h}(x)$ and $\deg \bar{g} < n$,

$\deg \bar{h} < n$. Hence f can be written as a product of

two poly. of deg. $< n$ modulo $\mathfrak{a}$, which is a contrad.

The "moreover" part we have already proved

$\boxed{Q}$. Show that $x^3 + xy + y^2 + x + 1$ is irreducible in $\mathbb{Q}[x,y]$.

<u>Solution</u>. $f(x,y) \in \underbrace{\mathbb{Q}[x]}_{D}[y]$. Notice that D is a UFD,

and $\gcd(1, x, x^3+x+1) = 1$; and so $f(x,y)$ is primitive.

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

Therefore by the previous proposition it is enough to find

$\mathfrak{a} \trianglelefteq D$ s.t. f cannot be written as a product of two poly. of

degree $< \deg_y f = 2$ modulo $\mathfrak{a}$. Consider the evaluation map

at 0, $\mathbb{Q}[x] \longrightarrow \mathbb{Q}$; kernel of this map $\mathfrak{a} := \langle x \rangle$.

$$g(x) \longmapsto g(0)$$

Modulo $\mathfrak{a}$, f is mapped to y^2+1 which has no zero in $\mathbb{Q}$

and so $f(x,y)$ modulo $\mathfrak{P}$ cannot be written as a product of two poly. of deg. <2; claim follows. ∎

Going through the above argument we get the following generalization:

- $f(x,y) = \sum_{i=0}^{n} a_i(x)\, y^i \in \mathbb{Q}[x,y]$
- $n \geq 1$, $\gcd(a_0(x), \ldots, a_n(x)) = 1$
- $a_n(\alpha) \neq 0$ and $f(\alpha, y)$ is irred. in $\mathbb{Q}[y]$ for some $\alpha \in \mathbb{Q}$

$$\Downarrow$$

f is irreducible in $\mathbb{Q}[x,y]$.