Lecture 20: Finishing proof of Hilbert's basis theorem

Thursday, December 6, 2018 9:08 AM

<u>Theorem</u>. A: Noetherian $\Rightarrow$ $A[x]$: Noetherian.

<u>Pf.</u> (Cont.) Suppose $\mathfrak{a}$ is a non-zero ideal of $A[x]$. Let

$$\mathrm{ld}(\mathfrak{a}) := \{a \in A \mid \exists\, ax^n + \text{smaller deg. terms} \in \mathfrak{a},\ a \neq 0\} \cup \{0\} \text{ and}$$

$$\mathrm{ld}_m(\mathfrak{a}) := \{a \in A \mid \exists\, ax^m + \text{smaller deg. terms} \in \mathfrak{a},\ a \neq 0\} \cup \{0\}.$$

Then we proved $\mathrm{ld}(\mathfrak{a})$ and $\mathrm{ld}_m(\mathfrak{a})$ are ideals of A; and so they are finitely generated. Suppose

$\mathrm{ld}(\mathfrak{a}) = \langle a_1, \ldots, a_{m'} \rangle$, and $f_i(x) = a_i x^{n_i} + \text{smaller deg. terms} \in \mathfrak{a}$,

$\mathrm{ld}_m(\mathfrak{a}) = \langle b_{1m}, \ldots, b_{k_m m} \rangle$, and $g_{im}(x) = b_{im} x^m + \text{smaller deg. terms} \in \mathfrak{a}$.

Let

$$\mathfrak{a}' := \langle f_1, \ldots, f_{m'} \rangle + \left\langle g_{ij} \;\middle|\; \begin{array}{l} 1 \le j \le \max(n_1, \ldots, n_{m'}) - 1 \\ 1 \le i \le k_j \end{array} \right\rangle$$

<u>Claim</u>. $\mathfrak{a} = \mathfrak{a}'$.

<u>Pf of Claim</u>. Since $f_i, g_{ij} \in \mathfrak{a}$, $\mathfrak{a}' \subseteq \mathfrak{a}$. Next by strong induction on $\deg f$ we show that, if $f \in \mathfrak{a}$, then $f \in \mathfrak{a}'$.

<u>Case 1</u>. $\deg f \ge \max\{n_1, \ldots, n_{m'}\}$.

Suppose $f(x) = a x^n + \text{smaller deg. terms}$. Then $a \in \langle a_1, \ldots, a_{m'} \rangle$ and so $a = r_1 a_1 + \cdots + r_{m'} a_{m'}$ for some $r_1, \ldots, r_{m'} \in A$.

Lecture 20: Hilbert's basis theorem; p-valuation

Thursday, December 6, 2018 11:14 AM

And so $\underbrace{ax^n}_{\text{leading term of } f(x)} = (r_1 x^{n-n_1})(\underbrace{a_1 x^{n_1}}_{\text{leading term of } f_1(x)}) + \cdots + (r_{m'} x^{n-n_{m'}})(\underbrace{a_{m'} x^{n_{m'}}}_{\text{leading term of } f_{m'}(x)})$

$(n - n_i \geq 0)$

$$\Rightarrow \deg\left(f - \sum_{i=1}^{m'} r_i x^{n-n_i} f_i\right) < \deg f. \qquad (1)$$

$$\left.\begin{array}{l} \sum_{i=1}^{m'} r_i x^{n-n_i} f_i \in \mathfrak{a}' \subseteq \mathfrak{a} \\ f \in \mathfrak{a} \end{array}\right\} \Rightarrow f - \sum_{i=1}^{m'} r_i x^{n-n_i} f_i \in \mathfrak{a} \qquad (2)$$

(1) and (2) and the strong induction hypothesis imply

$$\left.\begin{array}{l} f - \sum_{i=1}^{m'} r_i x^{n-n_i} f_i \in \mathfrak{a}' \\ \sum_{i=1}^{m'} r_i x^{n-n_i} f_i \in \mathfrak{a}' \end{array}\right\} \Rightarrow f \in \mathfrak{a}'.$$

Case 2. $\deg f < \max\{n_1, \ldots, n_{m'}\}$.

Suppose $f(x) = a x^\ell +$ smaller deg. terms. Then $a \in \mathrm{ld}_\ell(\mathfrak{a})$.

And so $a = r_1 b_{1\ell} + \cdots + r_{k_\ell} b_{k_\ell \ell}$. Therefore

$\deg\left(f - \sum_{i=1}^{k_\ell} r_i g_{i\ell}\right) < \deg f$. Since $g_{i\ell} \in \mathfrak{a}'$, one can finish the argument by a similar argument as in case 1. ■

Cor. If A is Noetherian, then $A[x_1, \ldots, x_n]$ is Noetherian.

Pf. By induction on n. □

Lecture 20: Finitely generated algebras

Thursday, December 6, 2018 11:27 AM

Cor. Suppose k is a field, and A is a finitely generated k-algebra; that means $\exists\, a_1,\dots,a_n \in A$ s.t. $A = k[a_1,\dots,a_n]$ where $k[a_1,\dots,a_n] = \{\sum_{i_1,\dots,i_n} c_{i_1,\dots,i_n} a_1^{i_1} a_2^{i_2}\cdots a_n^{i_n} \mid c_{i_1,\dots,i_n} \in k\}$ (it is the smallest subring of A that contains k as a subring and $a_1,\dots,a_n$ as elements). Then A is Noetherian.

Pf of Cor. Let $\phi: k[x_1,\dots,x_n] \to A$, $\phi(f) := f(a_1,\dots,a_n)$. Then ϕ is an onto ring homomorphism. Hence $A \simeq k[x_1,\dots,x_n]/I$ where $I = \ker\phi$. So it is enough to show any ideal of $k[x_1,\dots,x_n]/I$ is finitely generated. Any ideal of $k[x_1,\dots,x_n]/I$ is of the form $\mathfrak{a}/I$ where $I \subseteq \mathfrak{a}$ and $\mathfrak{a} \trianglelefteq k[x_1,\dots,x_n]$. Since k is a field, it is Noeth.. Hence by the previous cor., $k[x_1,\dots,x_n]$ is Noetherian. Therefore $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = \langle f_1,\dots,f_m\rangle$. Then $\mathfrak{a}/I = \langle f_1+I,\dots,f_m+I\rangle$ is f.g. ∎

Next we define p-valuations, g.c.d. in a UFD and Gauss's lemma, which enable us to show D:UFD $\Rightarrow D[x]$:UFD

Lecture 20: p-valuations

Thursday, December 6, 2018 11:48 AM

The last assertion will be proved in 200 B.

. For the rest of this lecture, we will assume D is a UFD.

Let $\mathcal{P} \subseteq D$ be such that, $\forall q \in D$ irreducible, $\exists!\, p \in \mathcal{P}$ s.t. $q \sim p$.

In $\mathbb{Z}$, since $\mathbb{Z}^{\times} = \{1, -1\}$, by working with positive integers we can pick a canonical representative from each class of associates, that is why g.c.d. or l.c.m. are defined to be <u>positive</u>. In an arbitrary UFD we cannot make such a canonical choice.

That is why we work with $[a] := aD^{\times}$ for $a \in D \setminus \{0\}$.

Notice that $a \sim b \Leftrightarrow [a] = [b]$;

($a \sim b \Rightarrow a = bu$ for some $u \in D^{\times} \Rightarrow aD^{\times} = buD^{\times} = bD^{\times}$

$[a] = [b] \Rightarrow a \in bD^{\times} \Rightarrow \exists\, u \in D^{\times},\ a = bu$.)

By the uniqueness of factorization into irreducibles,

$\forall a \in D \setminus \{0\}$, $\exists!\, v_p(a) \in \mathbb{Z}^{\geq 0}$ s.t. $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ for some $u \in D^{\times}$. Notice that from this definition we see

$v_p(a)$ is the <u>largest integer</u> s.t. $p^{v_p(a)} \mid a$.

Lecture 20: p-valuations

Thursday, December 6, 2018 12:19 PM

Def. Suppose D is a UFD and p is irred. in D. Then the p-valuation v_p is defined as follows:

$$v_p : D \to \mathbb{Z}^{\geq 0} \cup \{\infty\}, \quad v_p(0) = \infty$$

$$v_p(a) = n \text{ if } p^n \mid a \text{ and } p^{n+1} \nmid a.$$

Notice If $p \sim p'$ are irreducible, then

$$p^n \mid a \Rightarrow a = p^n a' \Rightarrow a = (up')^n a'$$

$$\Rightarrow a = p'^n (u^n a') \Rightarrow p'^n \mid a$$

By symmetry, $p^n \mid a \Leftrightarrow p'^n \mid a$; and so $v_p(a) = v_{p'}(a)$, and we can talk about $v_{[p]}(a)$.

Basic Properties of p-valuations.

(0) $\forall a \in D \setminus \{0\}$, $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ for some $u \in D^\times$.

(1) $a \sim b \Longleftrightarrow$ for any irreducible p, $v_p(a) = v_p(b)$.

And so we can talk about $v_p([a])$.

(2) $a \mid b \Longleftrightarrow \forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$.

(3) $v_p(ab) = v_p(a) + v_p(b)$

(4) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$; and if $v_p(a) \neq v_p(b)$, equality holds.

Lecture 20: gcd in a UFD

Thursday, December 6, 2018 3:17 PM

Pf. It is almost identical to the proof of these claims over $\mathbb{Z}$, and they are rather easy. So we leave it as an exercise (proof by intimidation!)

Remark. The above properties imply the following is an exact sequence of monoids:

$$\begin{array}{ccccccccc} 1 \longrightarrow & D^\times & \longrightarrow & D\setminus\{0\} & \longrightarrow & \bigoplus_{p\in\mathcal{P}} \mathbb{Z}^{\geq 0} & \longrightarrow 0 \\ & u & \longmapsto & u, \quad a & \longmapsto & (v_p(a))_{p\in\mathcal{P}} & \end{array}$$

Def. Suppose D is a UFD; for $a_1,\ldots,a_m \in D\setminus\{0\}$, we let

$$\gcd(a_1,\ldots,a_n) := \Big[\prod_{p\in\mathcal{P}} p^{\min\{v_p(a_i)\}_{i=1}^m}\Big].$$

(So $v_p(\gcd(a_1,\ldots,a_n)) = \min(v_p(a_1),\ldots,v_p(a_n))$.)

Basic Properties of g.c.d.

(1) Suppose $\gcd(a_1,\ldots,a_n)=[d]$. Then $d\mid a_1,\ldots,d\mid a_n$ and $\gcd(a_1/d,\ldots,a_n/d)=[1]$.

(2) $\gcd(ca_1,\ldots,ca_n)=[c]\gcd(a_1,\ldots,a_n)$.

Pf. Exercise.

Lecture 20: Gauss's lemma, v.1 and v.2

Thursday, December 6, 2018 9:11 AM

Def ① Suppose D is a UFD. For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in D[x]$, we let $c(f) := \gcd(a_0, a_1, \ldots, a_n)$, and it is called the <u>content</u> of f.

② $f(x)$ is called <u>primitive</u> if $c(f) = [1]$.

<u>Gauss's lemma v.1</u>. f, g : primitive $\Rightarrow$ fg is primitive.

<u>Pf</u>. Suppose to the contrary that $v_p(c(fg)) \neq 0$ for some $p \in \mathcal{P}$. Let $\pi_p : D[x] \to (D/\langle p \rangle)[x]$, $\pi_p(\sum_i r_i x^i) = \sum \pi_p(r_i) x^i$.

Then $\pi_p(fg) = 0$ as $v_p(c(fg)) \neq 0$. On the other hand,

p irreducible $\Rightarrow$ p prime $\Rightarrow \langle p \rangle$ prime $\Rightarrow D/\langle p \rangle$ integral domain

$\Rightarrow (D/\langle p \rangle)[x]$ integral domain.

So $\pi_p(f)\, \pi_p(g) = 0$ implies either $\pi_p(f) = 0$ or $\pi_p(g) = 0$.

$\pi_p(f) = 0$ implies all the coeff. of f are multiples of p, which contradicts that f is primitive. ∎

<u>Gauss's lemma v.2</u>. $c(fg) = c(f)\, c(g)$.

<u>Pf</u>. Suppose $c(f) = [c_f]$ and $c(g) = [c_g]$. By factoring out

Lecture 20: Gauss's lemma, v.2

Thursday, December 6, 2018 4:13 PM

c_f and c_g we get primitive polynomials $\bar{f}$ and $\bar{g}$;

$f(x) = c_f \bar{f}(x)$ and $g(x) = c_g \bar{g}(x)$. Then $f(x)g(x) = c_f c_g \bar{f}(x)\bar{g}(x)$.

By the first version of Gauss's lemma, $\bar{f}\cdot\bar{g}$ is primitive. Hence

$c(fg) = c(c_f c_g \bar{f}\bar{g}) = [c_f][c_g]\, c(\bar{f}\bar{g}) = c(f)\, c(g)$. ■

Recall. Suppose A is an integral domain; let

$F := \{[(a,b)] \mid a \in A,\ b \in A \setminus \{0\}\}$ where $(a,b) \sim (a',b')$

think about like $\frac{a}{b}$

if and only if $ab' = a'b$

$\left(\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b\right)$

$\sim$ is an equivalence relation, and F is a field with

$[(a,b)] + [(c,d)] := [(ad+bc, bd)]$ and $[(a,b)]\cdot[(c,d)] := [(ac,bd)]$.

F is called the field of fractions of A.

Theorem. Suppose D is a UFD and F is its field of fractions.

Suppose $f(x) \in D[x]$ and $f(x) = f_1(x)\cdot f_2(x)\cdot \cdots \cdot f_n(x)$ for

some $f_i(x) \in F[x]$. Then $\exists\, c_i \in F$ s.t.

(1) $c_1 \cdot c_2 \cdot \cdots \cdot c_n = 1$, (2) $c_i f_i(x) \in D[x]$;

and so

$$f(x) = \underbrace{(c_1 f_1(x))}_{\text{in } D[x]}\underbrace{(c_2 f_2(x))}_{\text{in } D[x]}\cdot \cdots \cdot \underbrace{(c_n f_n(x))}_{\text{in } D[x]}.$$

Lecture 20: Reducibility in D[x]

Thursday, December 6, 2018 4:57 PM

<u>Cor.</u> Suppose D is a UFD and F is its field of fractions.

Suppose $f(x) \in D[x]$ is reducible in $F[x]$ and $\deg f \geq 1$.

Then $f(x)$ is reducible in $D[x]$.

<u>Pf of theorem.</u> $\exists\, a_i \in D\setminus\{0\}$, $\hat{f}_i(x) := a_i f_i(x) \in D[x]$.

Let $[d_i] := c(\hat{f}_i)$; then $\hat{f}_i(x) = d_i\, \bar{f}_i(x)$ where $\bar{f}_i$

are primitive polynomials. So

$$\left(\prod_{i=1}^n a_i\right) f(x) = \prod_{i=1}^n a_i f_i(x) = \prod_{i=1}^n \hat{f}_i(x) = \prod_{i=1}^n d_i\, \bar{f}_i(x) \quad (1)$$

$$\Rightarrow c\left(\left(\prod_{i=1}^n a_i\right) f\right) = c\left(\prod_{i=1}^n d_i \cdot \prod_{i=1}^n \bar{f}_i\right)$$

$$\Rightarrow \left[\prod_{i=1}^n a_i\right] c(f) = \left[\prod_{i=1}^n d_i\right] \prod_{i=1}^n c(\bar{f}_i) \quad \text{(Gauss's lemma, v.2)}$$

$$= \left[\prod_{i=1}^n d_i\right]$$

$$\Rightarrow \prod_{i=1}^n a_i \,\Big|\, \prod_{i=1}^n d_i; \text{ say } \prod_{i=1}^n d_i = d \cdot \prod_{i=1}^n a_i. \quad (2)$$

(1) and (2) imply

$$f(x) = d \prod_{i=1}^n \bar{f}_i(x) = (d\, \bar{f}_1(x))(\bar{f}_2(x)) \cdot \ldots \cdot (\bar{f}_n(x)). \quad (3)$$

Notice that $\bar{f}_i(x) = \frac{a_i}{d_i} f_i(x)$; let $c_1 := d \cdot \frac{a_1}{d_1}, c_2 := \frac{a_2}{d_2}, \ldots, c_n := \frac{a_n}{d_n}$.

Then by (2) and (3) one can see that c_i's satisfy the desired conditions. ∎