Lecture 03: Valuation

Wednesday, January 10, 2018 11:48 AM

Def. Suppose D is a UFD, and $p \in D$ is irreducible.

Then $\exists\, v_p : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}$, $\forall a \in D\setminus\{0\}$,

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

Notation. Let $\mathcal{P} \subseteq D$ be a subset consisting of irreducible elements s.t.

(1) $\forall\, p_1 \neq p_2 \in \mathcal{P}$, $\langle p_1 \rangle \neq \langle p_2 \rangle$ (2) $\forall\, p \in D$ that is irreducible there is $p' \in \mathcal{P}$ s.t. $\langle p \rangle = \langle p' \rangle$.

Remark. In $\mathbb{Z}$, there are only two units ± 1. In classical number theory we define primes to be positive; this way we choose a representative in a class of associates. The above notation $\mathcal{P}$ serves us the same way.

Since D is UFD (using the definition of $v_p(a)$), we get

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{where } u \in D^{\times}.$$

By the uniqueness of this decomposition we get that $v_p(a)$ is well-defined; and here are its basic properties.

(1) $v_p(ab) = v_p(a) + v_p(b)$ (2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

Lecture 03: Valuation

Wednesday, January 10, 2018 1:46 PM

and $v_p(a+b) = \min\{v_p(a), v_p(b)\}$ if $v_p(a) \neq v_p(b)$.

(Suppose $v_p(a) < v_p(b)$. Then $a+b = p^{v_p(a)}(\underbrace{a' + p^{v_p(b)-v_p(a)} b'}_{\text{not divis. by } p})$. So $\uparrow$.)

(3) $a \mid b \iff \forall p \in \mathcal{P}, \quad v_p(a) \leq v_p(b)$.

<u>Pf.</u> ($\Rightarrow$) $a \mid b \Rightarrow ac = b \Rightarrow v_p(ac) = v_p(b)$

$$\Rightarrow v_p(b) = v_p(a) + v_p(c) \geq v_p(a).$$

($\Leftarrow$) $\left.\begin{array}{l} a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \\ b = u' \prod_{p \in \mathcal{P}} p^{v_p(b)} \end{array}\right\} \Rightarrow a \cdot \underbrace{u' u^{-1} \cdot \prod_{p \in \mathcal{P}} p^{v_p(b)-v_p(a)}}_{\text{in } D} = b$

$\Rightarrow a \mid b$. ∎

(4). $a_1 \sim a_2 \iff \forall p \in \mathcal{P}, \ v_p(a_1) = v_p(a_2)$.

. $a \in D^\times \iff \forall p \in \mathcal{P}, \ v_p(a) = 0$.

Let $[a] := \{a' \in D \mid a \sim a'\} = aD^\times$. Then we can talk about $v_p([a])$.

(5) $\gcd(a_1, \ldots, a_m) = \left[\prod_{p \in \mathcal{P}} p^{\min_i \{v_p(a_i)\}}\right]$.

Equiva. $v_p(\gcd(a_1, \ldots, a_m)) = \min\{v_p(a_1), \ldots, v_p(a_m)\}$.

<u>Pf.</u> $v_p(\underbrace{\prod p^{\min\{v_p(a_i)\}}}_{d}) = \min\{v_p(a_i)\} \leq v_p(a_i) \Rightarrow d \mid a_i$.

Lecture 03: gcd

Wednesday, January 10, 2018 2:22 PM

If $d' \mid a_i$, then $\forall i$, $v_p(d') \le v_p(a_i)$. So $v_p(d') \le \min\{v_p(a_i)\}$
$= v_p(d)$.

So $d' \mid d$. $\blacksquare$

<u>Basic Properties of g.c.d.</u> D: UFD, $a_1, \ldots, a_m \in D$ at least one of them is not 0.

(1) $\forall c \in D^\times$, $\gcd(ca_1, \ldots, ca_m) = [c] \gcd(a_1, \ldots, a_m)$.

(2) Let $d := \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_i)\}}$, and suppose $a_i = d\, a_i'$.

Then $\gcd(a_1', \ldots, a_m') = [1]$.

(<u>Remark</u>. In $\mathbb{Z}$, we have $\gcd(ca_1, \ldots, ca_m) = |c| \gcd(a_1, \ldots, a_m)$.

In general $[c]$ is need as there is no canonical choice a class of associates.)

<u>Pf</u>. (1) $v_p(\gcd(ca_1, \ldots, ca_m)) = \min_i \{v_p(ca_i)\}$

$$= \min_i \{v_p(c) + v_p(a_i)\}$$

$$= v_p(c) + \min_i \{v_p(a_i)\}$$

$$= v_p(c) + v_p(\gcd(a_1, \ldots, a_m))$$

$$= v_p([c] \gcd(a_1, \ldots, a_m)).$$

(2) $v_p(\gcd(a_1', \ldots a_m')) = \min\{v_p(a_i')\} = \min\{v_p(a_i) - v_p(d)\}$

$$= \min\{v_p(a_i)\} - v_p(d) = 0. \quad \blacksquare$$

Lecture 03: Content, primitive, and Gauss's lemma

Friday, January 12, 2018 11:48 AM

<u>Def.</u> D: UFD, $f(x)=\sum_{i=0}^{n} a_i x^i \in D[x]\setminus\{0\}$. Then the content $c(f)$ of $f(x)$ is $\gcd(a_0, a_1, \ldots, a_n)$.

<u>Basic properties</u> . • $c(af(x)) = [a]\, c(f)$

• $f(x) = c_f\, \bar{f}(x)$ s.t. $c(f)=[c_f]$ and $c(\bar{f})=[1]$.

<u>Def.</u> $f(x)\in D[x]$ is called <u>primitive</u> if $c(f)=[1]$.

<u>Lemma</u>. $f, g\in D[x]$ primitive $\Leftrightarrow$ fg is primitive.

<u>Pf.</u> $(\Rightarrow)$ Suppose to the contrary that the coeff. of fg have a common irreducible factor p. Consider

$$\phi: D[x]\to (D/\langle p\rangle)[x],\quad \phi\left(\sum a_i x^i\right) := \sum (a_i+\langle p\rangle)\, x^i .$$

Then $\phi(fg)=0$. And so $\phi(f)\,\phi(g)=0$. $(*)$

$\left.\begin{array}{l} p: \text{irred.} \\ D: \text{UFD} \end{array}\right\} \Rightarrow p: \text{prime} \Rightarrow \langle p\rangle \text{ prime} \Rightarrow D/\langle p\rangle$ integ. domain

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

So $(*)$ implies either $\phi(f)=0$ or $\phi(g)$. Hence either $v_p(c(f))\geq 1$ or $v_p(c(g))\geq 1$; this contradicts the assump. that f and g are primitive.

Lecture 03: Gauss's lemma

Thursday, January 11, 2018 9:54 PM

($\Leftarrow$) If not, $\exists p \in \mathcal{P}$ s.t. either $p \mid f(x)$ or $p \mid g(x)$. And so $p \mid f(x)g(x)$; and this contradi: the assumption that $f(x)g(x)$ is primitive. ∎

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

Pf. $f(x)\,g(x) = c_f\,\bar{f}(x)\,.\,c_g\,\bar{g}(x)$ s.t. $[c_f] = c(f)$, $\bar{f}$: primi.
$[c_g] = c(g)$, $\bar{g}$: 〃.

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

$$\Rightarrow c(fg) = [c_f\,c_g]\; c(\underbrace{\bar{f}\,\bar{g}}_{\text{primitive}}) = [c_f][c_g]\,[1]$$

$$= c(f)\,c(g).$$ ∎

Corollary (Sometimes this is known as Gauss's lemma)

D: UFD ; F: field of fractions. ; $f(x) \in D[x] \setminus D$.

(a) $f(x) = f_1(x)\,f_2(x)$ for some $f_i(x) \in F[x]$. $\Rightarrow$

$\exists c_1, c_2 \in F$ s.t. $c_1 c_2 = 1$ and $\tilde{f}_i(x) := c_i\,f_i(x) \in D[x]$

And so $f(x) = \tilde{f}_1(x)\,\tilde{f}_2(x)$ and $\deg f_i = \deg \tilde{f}_i$.

(b) $f(x) = \prod_{i=1}^{m} f_i(x)$ for some $f_i \in F[x] \Rightarrow \exists c_i \in F$ s.t.
$\prod_{i=1}^{m} c_i = 1$ and $\tilde{f}_i(x) = c_i\,f_i(x) \in D[x]$.

Lecture 03: Gauss's lemma

Thursday, January 11, 2018 10:16 PM

The main point of this corollary is to relate reducibilty in $F[x]$ with reducibility in $D[x]$. Notice that $F[x]$ is a PID (and so UFD); and we would like to use this to say something about $D[x]$.

<u>Pf of corollary</u>. (a) Let a_i be the product of denom. of the coeffi. of f_i; and let $\overline{f}_i(x) := a_i f_i(x) \in D[x]$.

So $a_1 a_2 f(x) = \overline{f}_1(x) \overline{f}_2(x)$. Therefore

$[a_1 a_2] c(f) = c(a_1 a_2 f(x)) = c(\overline{f}_1 \overline{f}_2) = c(\overline{f}_1) c(\overline{f}_2)$. (I)

On the other hand, $\overline{f}_i(x) = c_{f_i} \hat{f}_i(x)$; where $[c_{f_i}] = c(f_i)$ and $\hat{f}_i \in D[x]$. Hence

$$a_1 a_2 f(x) = c_{f_1} \hat{f}_1(x) \, c_{f_2} \hat{f}_2(x)$$

$$= c_{f_1} c_{f_2} \hat{f}_1(x) \hat{f}_2(x) \qquad \text{(II)}$$

(I) $\Rightarrow$ $[a_1 a_2] c(f) = c(\overline{f}_1) c(\overline{f}_2) = [c_{f_1} c_{f_2}]$.

$\Rightarrow \exists d \in D, \; c_{f_1} c_{f_2} = a_1 a_2 d$. (III)

(II),(III) $\Rightarrow$ $a_1 a_2 f(x) = a_1 a_2 d \hat{f}_1(x) \hat{f}_2(x) \Rightarrow f(x) = d \hat{f}_1 \cdot \hat{f}_2$.

Lecture 03: Gauss's lemma

Friday, January 12, 2018 12:20 AM

So $f(x) = (\underbrace{d\, \hat{f}_1(x)}_{\text{in } D[x]})(\underbrace{\hat{f}_2(x)}_{\text{in } D[x]})$; $d\,\hat{f}_1(x)$ and $\hat{f}_2(x)$

are scalar (in $F^\times$) multiples of $f_1(x)$ and $f_2(x)$, respectively

$\left(f_i(x) = a_i^{-1} \bar{f}_i = a_i^{-1} c_{f_i} \hat{f}_i\right)$. Say $d\hat{f}_1(x) = c_1 f_1(x)$ and

$\hat{f}_2(x) = c_2 f_2(x)$. Then $f(x) = c_1 c_2 f(x)$ and so $c_1 c_2 = 1$.

(b) We use induction on m. Part (a) gives the case $m=2$.

$f(x) = \left(f_1(x) \cdots f_m(x)\right) f_{m+1}(x) \Rightarrow \exists\, c_{m+1}$ and $c' \in F$ s.t.

$(c' f_1(x)) f_2(x) \cdots f_m(x) \in D[x]$ and $c_{m+1} f_{m+1}(x) \in D[x]$ and $c_{m+1} c' = 1$.

By the induction hypoth. $\exists\, c_i' \in F$ s.t.

$\prod_{i=1}^{m} c_i' = 1$ and $c_1' c' f_1(x), c_2' f_2(x), \ldots, c_m' f_m(x) \in D[x]$.

Let $c_1 := c_1' c'$, $c_2 := c_2', \ldots, c_m := c_m'$, $c_{m+1} = c_{m+1}$. Then

$c_i f_i(x) \in D[x]$ and $\prod_{i=1}^{m+1} c_i f_i(x) = f(x)$; and so $\prod c_i = 1$.

■