Lecture 05: Irreducibility criteria

Friday, January 19, 2018 8:12 AM

In the previous lecture we proved that

$$D \text{ is a UFD} \Leftrightarrow D[x] \text{ is a UFD}.$$

So by induction we have

$$D \text{ is a UFD} \Leftrightarrow D[x_1, \ldots, x_n] \text{ is a UFD}.$$

We also proved that:

D: UFD and F: field of fractions of D;

$f(x) \in D[x]$ primitive. Then

$$f(x) \text{ is irreducible in } D[x] \Leftrightarrow f(x) \text{ is irred. in } F[x].$$

Cor. Suppose $f(x)$ cannot be written as a prod. of two poly. of deg. $<$ deg f in $(D/\mathfrak{m})[x]$. Then f is irred. in $F[x]$.

Pf. If not, $f(x) = f_1(x) f_2(x)$ for some $f_i(x) \in F[x] \setminus F$.

$$\Rightarrow \exists\, c_i \in F^{\times} \text{ s.t. } f(x) = \overbrace{\underbrace{(c_1 f_1(x))}_{\text{in } D[x]}}^{F_1(x)} \overbrace{\underbrace{(c_2 f_2(x))}_{\text{in } D[x]}}^{F_2(x)}$$

$\Rightarrow f(x) \equiv \overline{F}_1(x) \overline{F}_2(x) \bmod \mathfrak{m}$ which contradicts our assumption.

Lecture 05: Irreducibility criteria

Friday, January 19, 2018 8:20 AM

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

Solution. Let's consider $\mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[x]$.

$$p(x,y) \longmapsto p(x,0)$$

Then, by the 1^{st} isomor. theorem, $\mathbb{Q}[x,y]/\langle y\rangle \simeq \mathbb{Q}[x]$.

And $f(x) := x^3+xy+y^2+x+1$ is mapped to x^3+x+1.

Claim. x^3+x+1 is irred. in $\mathbb{Q}[x]$.

Pf. If not, it should have a factor of deg. 1; this implies x^3+x+1 has a rational root r/s. By an exercise you know that $r \mid 1$ and $s \mid 1$. So $r/s = \pm 1$. But $(\pm 1)^3 + (\pm 1) + 1 \neq 0$.

Hence by the above claim and the previous corollary we are done. ∎

Thm (Eisenstein's criterion) Suppose D is an integral domain, $\mathfrak{p} \in \operatorname{Spec}(D)$, $a_{n-1}, \ldots, a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is irreducible in $D[x]$.

Lecture 05: Irreducibility criteria

Friday, January 19, 2018 8:35 AM

Pf. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is not irreducible.

Since it is monic, $f(x) = f_1(x) f_2(x)$ and $\deg f_i < \deg f$.

$\Rightarrow f(x) \equiv f_1(x) f_2(x) \pmod{\mathfrak{p}}$

$\Rightarrow x^n \equiv f_1(x) f_2(x) \pmod{\mathfrak{p}}$

$\Rightarrow f_1(0)$ and $f_2(0) \in \mathfrak{p}$.

$\Rightarrow a_0 = f_1(0) f_2(0) \in \mathfrak{p}^2$ which is a contradiction. ∎

Ex. $x^{p-1} + \cdots + x + 1 = 0$ is irred. in $\mathbb{Q}[x]$ if p is a prime.

Pf. $f(x) = \dfrac{x^p - 1}{x - 1} \Rightarrow f(x+1) = \dfrac{(x+1)^p - 1}{x}$

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

It satisfies the Eisenstein criterion's condition. ∎

Ex. $x^n + p \in \mathbb{Z}[i][x]$ is irred. if p is an odd prime.

Pf. Suppose $a + ib$ is an irred. factor of p. Then

$a^2 + b^2 \mid p^2 \Rightarrow$ either $a^2 + b^2 = p^2$ or $a^2 + b^2 = p$.

In the first case, $a + ib \sim p$. In the second case

Lecture 05: Irreducibility criteria

Friday, January 19, 2018 8:46 AM

$p=(a+ib)(a-ib)$ and $(a+ib)^2 \nmid p$ (why ?)

So one can use the Eisenstein crieterion. ■

Hint: . If $a^2+b^2=p$, then $a\pm ib$ are irreducible;

. Show $a+ib \sim a-ib$, implies $p=2$.

Next we prove an extremely important theorem:

Theorem. Suppose A is a unital commutative ring. If A is Noethenian, then $A[x]$ is Noetherian.

Corollary. A finitely generated k-algebra A where k is a field is Noethenian.

Pf. Suppose $A=k[a_1,\ldots,a_n]$. Then $k[x_1,\ldots,x_n] \longrightarrow A$, $x_i \longmapsto a_i$

is an onto ring homomorphism. Hence $A \simeq k[x_1,\ldots,x_n]/\mathfrak{a}$.

By the previous theorem, $k[x_1,\ldots,x_n]$ is Noeth.; Hence any of its quotients is Noeth. ■

(An ideal of R/I is of the form $\mathfrak{b}/I$ where $\mathfrak{b} \trianglelefteq R$ and $I \subseteq \mathfrak{b}$. So if R is Noeth., then $\mathfrak{b}$ is f.g.; therefore $\mathfrak{b}/I$ is f.g.)

Lecture 05: Beginning of proof of Hilbert's basis theorem

Friday, January 19, 2018 11:23 AM

<u>Pf.</u> Let $\mathfrak{a}$ be a non-zero ideal of $A[x]$. We'd like to show $\mathfrak{a}$ is f.g. (When A is a field, we use long division to show, any ideal of $A[x]$ is principal. The key idea of long division is cancelling out the leading term of $a_n x^n + \cdots$ by a multiple of $g(x)$, and then continue this process. And we could do it as $\underline{a_n}$ is in the ideal gen. by the leading coeff. of g. Now we'd like to follow a similar idea and get rid of leading term.)

Let $ld(\mathfrak{a}) := \{ \underbrace{a \in A \mid \exists \underset{a \neq 0}{a x^n + \cdots} \in \mathfrak{a}}_{\substack{\text{leading coeff. of} \\ \text{an element of } \mathfrak{a}}} ; \} \cup \{0\}$.

Then $ld(\mathfrak{a})$ is an ideal of A.

- $a, a' \in ld(\mathfrak{a}) \Rightarrow \left\{ \begin{array}{l} \exists\ a x^n + \cdots \in \mathfrak{a} \\ \exists\ a' x^m + \cdots \in \mathfrak{a} \end{array} \right\} \Rightarrow$

$$x^m (a x^n + \cdots) + x^n (a' x^m + \cdots) = (a + a') x^{m+n} + \cdots \in \mathfrak{a}$$

So either $a + a' = 0 \in ld(\mathfrak{a})$ or $a + a'$ is a leading coeff. of an elem. of $\mathfrak{a}$ $\Rightarrow$ in either case $a + a' \in ld(\mathfrak{a})$.

Lecture 05: Beginning of proof of Hilbert's basis theorem

Friday, January 19, 2018 11:37 AM

$$\left.\begin{array}{l} \cdot\ a \in \mathrm{ld}(\mathfrak{a}) \Rightarrow \exists\, ax^n + \cdots \in \mathfrak{a} \\ \ \ r \in A \end{array}\right\} \Rightarrow r(ax^n + \cdots) = (ra)x^n + \cdots \in \mathfrak{a}$$
$$\Rightarrow ra \in \mathrm{ld}(\mathfrak{a}).$$

. Since A is Noeth., $\exists\, a_1, \ldots, a_m \in A$ s.t. $\mathrm{ld}(\mathfrak{a}) = \langle a_1, \ldots, a_m \rangle$

. As $a_i \in \mathrm{ld}(\mathfrak{a})$, $\exists\ f_i(x) = a_i x^{n_i} + \cdots \in \mathfrak{a}$.

(We will use f_i's to clear leading terms till we get to a polynomial of deg $< \max\{n_i\}$; to access these polynomials we consider the following sets:)

For any $m \in \mathbb{Z}^+$, let

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

Then $\mathrm{ld}_m(\mathfrak{a})$ is an ideal of A.

$$\cdot\ a, a' \in \mathrm{ld}_m(\mathfrak{a}) \Rightarrow \left\{\begin{array}{l} ax^m + \cdots \in \mathfrak{a} \\ a'x^m + \cdots \in \mathfrak{a} \end{array}\right\} \Rightarrow (a+a')x^m + \cdots \in \mathfrak{a}$$
$$\Rightarrow a + a' \in \mathrm{ld}_m(\mathfrak{a})$$

$$\left.\begin{array}{l} \cdot\ a \in \mathrm{ld}_m(\mathfrak{a}) \\ \ \ r \in A \end{array}\right\} \Rightarrow \left.\begin{array}{l} ax^m + \cdots \in \mathfrak{a} \\ r \in A \end{array}\right\} \Rightarrow r(ax^m + \cdots) = (ra)x^m + \cdots \in \mathfrak{a}$$
$$\Rightarrow ra \in \mathrm{ld}_m(\mathfrak{a}).$$

(In the next lecture, we will continue.)