In the previous lecture we proved that

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

So by induction we have

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

We also proved that:

\[ D: \text{ UFD and } F: \text{ field of fractions of } D; \]

\[ \frac{f(x)}{g(x)} \in D[x] \text{ primitive. Then} \]

\[ f(x) \text{ is irreducible in } D[x] \iff f(x) \text{ is irr. in } F[x]. \]

Cor. Suppose \( f(x) \) cannot be written as a prod. of two
poly. of deg. < deg \( f \) in \( (D_{\text{fr}})[x] \). Then \( f \) is irr. in \( F[x] \).

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

\[ \Rightarrow \exists c_i \in F^* \text{ s.t. } f(x) = \frac{f_1(x)}{c_i} \cdot \frac{f_2(x)}{c_i} \]

\[ \text{in } D[x] \text{ in } D[x] \]

\[ \Rightarrow f(x) \equiv \overline{f_1(x)} \overline{f_2(x)} \text{ mod } \alpha \text{ which contradicts our assumption.} \]
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 $\mathbb{Q}[x,y] \rightarrow \mathbb{Q}[x]$.

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

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

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

Claim. $x^3+x+1$ is irreducible 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 $\eta_s$. By an exercise you know that $r \mid 1$ and $s \mid 1$. So $\eta_s = \pm 1$.

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, $\mathfrak{p} \in \text{Spec}(D)$, $a_{n-1}, \ldots, a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Then $x^n+a_{n-1}x^{n-1}+\ldots+a_0$ is irreducible in $D[x]$. 
Lecture 05: Irreducibility criteria

Friday, January 19, 2018  8:35 AM

pf. Suppose \( f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \) is not irreducible. Since it is monic, \( f(x) = f_1(x)f_2(x) \) and \( \deg f_1 < \deg f \).

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

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

\[ \Rightarrow f_1(0) \text{ and } f_2(0) \in \mathfrak{p} . \]

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

**Ex.** \( x^n + \ldots + x + 1 = 0 \) is irreducible in \( \mathbb{Q}[x] \) if \( \mathfrak{p} \) is a prime.

pf. \( f(x) = \frac{x^p-1}{x-1} \Rightarrow f(x+1) = \frac{(x+1)^p-1}{x} \]

\[ = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-1}x + \ldots \]

It satisfies the Eisenstein criterion’s condition.

**Ex.** \( x^n + p \in \mathbb{Z}[x] \) is irreducible if \( p \) is an odd prime.

pf. Suppose \( a + ib \) is an irreducible factor of \( p \). Then

\[ a^2 + b^2 \mid p^2 \Rightarrow \text{ either } a^2 + b^2 = p^2 \text{ or } a^2 + b^2 = p . \]

In the first case, \( a + ib \mid p \). 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 criterion.

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 Noetherian, then \( A[x] \) is Noetherian.

**Corollary.** A finitely generated \( k \)-algebra \( A \) where \( k \) is a field is Noetherian.

**Proof.** Suppose \( A = k[x_1, \ldots, x_n] \). Then \( k[x_1, \ldots, x_n] \to A \)

\[ x_i \mapsto a_i \]

is an onto ring homomorphism. Hence \( A \cong k[x_1, \ldots, x_n] / \mathfrak{m} \).

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 \( k/I \) where \( k \subseteq R \) and \( I \subseteq \mathfrak{m} \). So if \( R \) is Noeth., then \( k \) is \( \mathfrak{m} \); therefore \( k/I \) is \( \mathfrak{m} \).)
Lecture 05: Beginning of proof of Hilbert's basis theorem

Friday, January 19, 2018 11:23 AM

Pf. 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 \( a_nx^n \ldots \) by a multiple of \( g(x) \), and then continue this process. And we could do it as \( a_n \) 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 \( \text{ld}(\mathfrak{a}) := \{ a \in A \mid \exists \ a_nx^n \ldots \in \mathfrak{a} ; \ a \neq 0 \} \). \( \text{ld}(\mathfrak{a}) \) is an ideal of \( A \).

\[ a, a' \in \text{ld}(\mathfrak{a}) \implies \exists \ a_nx^n \ldots \in \mathfrak{a} \implies \exists \ a'x^m \ldots \in \mathfrak{a} \]

\[ x^m (a_nx^n \ldots) + x^n (a'x^m \ldots) = (a+a')x^{m+n} \ldots \in \mathfrak{a} \]

So either \( a+a'=0 \in \text{ld}(\mathfrak{a}) \) or \( a+a' \) is a leading coeff. of an elem. of \( \mathfrak{a} \) \( \implies \) in either case \( a+a' \in \text{ld}(\mathfrak{a}) \).
Lecture 05: Beginning of proof of Hilbert's basis theorem

Friday, January 19, 2018 11:37 AM

\[ ae \in \text{ld}(\mathcal{V}) \implies \exists \ ax^r + \ldots \in \mathcal{V} \implies r(ax^r + \ldots) = (ra)x^r + \ldots \in \mathcal{V} \]

\[ \therefore \text{ld}(\mathcal{V}) = \text{ra} \implies ra \in \text{ld}(\mathcal{V}). \]

Since \( A \) is Noetherian, \( \exists a_1, \ldots, a_m \in A \) s.t. \( \text{ld}(\mathcal{V}) = \langle a_1, \ldots, a_r \rangle \). As \( a_i \in \text{ld}(\mathcal{V}) \), \( \exists f_i : ax = a_i x^n + \ldots \in \mathcal{V} \).

(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

\[ \text{ld}_m(\mathcal{V}) := \{ a \in A \mid \exists ax^m + \ldots \in \mathcal{V} \} \mathcal{V} = U \mathcal{V}_o. \]

Then \( \text{ld}_m(\mathcal{V}) \) is an ideal of \( A \).

- \( a, a' \in \text{ld}_m(\mathcal{V}) \implies \exists ax^m + \ldots \in \mathcal{V} \implies (a+a')x^m + \ldots \in \mathcal{V} \implies a+a' \in \text{ld}_m(\mathcal{V}) \)

- \( a \in \text{ld}_m(\mathcal{V}) \implies \exists ax^m + \ldots \in \mathcal{V} \implies r(ax^m + \ldots) = (ra)x^m + \ldots \in \mathcal{V} \implies ra \in \text{ld}_m(\mathcal{V}) \).

(In the next lecture, we will continue.)