# Lecture 19: Noetherian and ideals

Thursday, December 6, 2018 8:55 AM

<u>Proposition</u>. $A$ is Noetherian $\Leftrightarrow$ any ideal is finitely generated.

<u>Pf.</u> ($\Rightarrow$) Suppose to the contrary that $\exists\, \mathfrak{a} \triangleleft A$ which is not f.g..

We will define recursively a sequence $a_0, a_1, \dots \in \mathfrak{a}$ s.t.

(*) $\langle a_0 \rangle \subsetneq \langle a_0, a_1 \rangle \subsetneq \cdots$. Let $a_0 \in \mathfrak{a}$; and suppose we have already found $a_0, \dots, a_n$ that satisfy the above property. Since $\mathfrak{a}$ is NOT f.g., $\exists\, a_{n+1} \in \mathfrak{a} \setminus \langle a_0, \dots, a_n \rangle$, which satisfies (*).

(*) contradicts the fact that a Noetherian ring has a.c.c. (ascending chain condition).

($\Leftarrow$) We show that $A$ satisfies the a.c.c. Suppose $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$ is a chain of ideals of $A$. Then as we have proved earlier $\bigcup_{i=0}^{\infty} \mathfrak{a}_i \triangleleft A$. So $\exists\, a_1, \dots, a_n \in A$ s.t.

$$\langle a_1, \dots, a_n \rangle = \bigcup_{i=0}^{\infty} \mathfrak{a}_i .$$

Hence $\exists\, i_j$ s.t. $a_j \in \mathfrak{a}_{i_j}$; let $m := \max\{i_1, \dots, i_n\}$. Then $\mathfrak{a}_{i_j} \subseteq \mathfrak{a}_m$ for any $j$, which implies $a_1, \dots, a_n \in \mathfrak{a}_m$. Therefore $\langle a_1, \dots, a_n \rangle \subseteq \mathfrak{a}_m$; and so $\bigcup_{i=0}^{\infty} \mathfrak{a}_i \subseteq \mathfrak{a}_m$. Thus for $i \geq m$

# Lecture 19: Noetherian and product of irreducibles

Friday, December 7, 2018 9:18 AM

$$\left.\begin{cases} \mathfrak{a}_i \subseteq \bigcup_{j=0}^{\infty} \mathfrak{a}_j \subseteq \mathfrak{a}_m \\ \mathfrak{a}_m \subseteq \mathfrak{a}_i \end{cases}\right\} \Rightarrow \forall\, i \geq m,\ \mathfrak{a}_i = \mathfrak{a}_m. \qquad \blacksquare$$

<u>Proposition</u>. Suppose $D$ is a Noetherian integral domain. Then any $a \in D \setminus (\{0\} \cup D^\times)$ can be written as a product of irreducibles.

<u>Pf.</u> Let $\Sigma := \left\{ \langle a \rangle \;\middle|\; \begin{array}{l} a \in D \setminus (\{0\} \cup D^\times) \\ a \text{ cannot be written as a} \\ \text{product of irreducibles} \end{array} \right\}$. We want to show that $\Sigma = \emptyset$. Suppose to the contrary that $\Sigma \neq \emptyset$.

Since $D$ is Noetherian, $\Sigma$ has a maximal element. So $\exists\, a_0 \in D$ s.t.

- ① $a_0 \notin \{0\} \cup D^\times$; ② $a_0$ cannot be written as a prod. of irreducibles; and ③ $\langle a_0 \rangle$ is maximal in $\Sigma$.

By ②, $a_0$ is not irreducible; and so by ①, $\exists\, b, c \in D \setminus (\{0\} \cup D^\times)$ s.t. $a = bc$; therefore

$$\left.\begin{cases} \langle a \rangle \subseteq \langle b \rangle \text{ and } \langle a \rangle \subseteq \langle c \rangle \\ a \not\sim b \text{ and } a \not\sim c \end{cases}\right\} \Rightarrow \begin{cases} \langle a \rangle \subsetneq \langle b \rangle, \\ \langle a \rangle \subsetneq \langle c \rangle. \end{cases}$$

Hence $\langle b \rangle, \langle c \rangle \notin \Sigma$. As $b, c \notin \{0\} \cup D^\times$, we deduce that $b$ and $c$ can be written as a product of irreducibles. Therefore

# Lecture 19: Irreducible, Prime, and uniqueness

Friday, December 7, 2018 9:34 AM

$\exists\, p_1, \ldots, p_n, q_1, \ldots, q_m \in D$ that are irreducible in $D$ and

$b = p_1 \cdot \ldots \cdot p_n$ and $c = q_1 \cdot \ldots \cdot q_m$, which implies

$a = bc = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$; and so $a$ can be written as

a product of irreducibles which is a contradiction. $\blacksquare$

<u>Proposition</u>. Suppose $D$ is an integral domain, where any

$a \in D \setminus (\{0\} \cup D^\times)$ can be written as a product of irreducibles

(The existence part of being a UFD holds). Then

$$D \text{ is a UFD} \iff \text{any irreducible is prime.}$$

<u>Pf.</u> ($\Rightarrow$) Suppose $p \in D$ is irreducible. So $p \notin \{0\} \cup D^\times$; hence

we only need to show $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

$p \mid ab \Rightarrow \exists\, c \in D$, $pc = ab$; by the existence part of being

a UFD, $\exists\, p_1, \ldots, p_n, q_1, \ldots, q_m, l_1, \ldots, l_k \in D$ irreducible

and $c = p_1 \cdot \ldots \cdot p_n$, $a = q_1 \cdot \ldots \cdot q_m$, $b = l_1 \cdot \ldots \cdot l_k$. So

$p \cdot p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m \cdot l_1 \cdot \ldots \cdot l_k$; by the uniqueness part of

being a UFD, $\exists\, i$, $p \sim q_i$ or $p \sim l_i$. By symmetry w.l.o.g.

# Lecture 19: UFD



we can and will assume $p \sim q_i$. That means $q_i = up$ for some $u \in D^\times$. Hence $a = q_1 \cdot \dots \cdot q_m = p\,(u q_1 \cdot \dots \cdot q_{i-1} \cdot q_{i+1} \cdot \dots \cdot q_m)$; and so $p \mid a$.

($\Leftarrow$) We have the existence part by assumption. So we focus on the uniquess part. Suppose $p_1, \dots, p_n, q_1, \dots, q_m$ are irreducible in $D$ and $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$. So $p_1 \mid p_1 \cdots p_n = q_1 \cdot \dots \cdot q_m$. As $p_1$ is irreducible, $p_1$ is prime. Therefore $p_1 \mid q_1 \cdot \dots \cdot q_m$ implies $p_1 \mid q_{i_1'}$ for some $i_1'$. Thus $q_{i_1'} = p_1 \cdot u$ for some $u \in D$. As $q_{i_1'}$ is irred. and $p_1$ is not a unit, we deduce that $u \in D^\times$. And so $p_1 \sim q_{i_1'}$; after cancelling $p_1$ we get $p_2 \cdot \dots \cdot p_n = u q_1 \cdot \dots \cdot q_{i_1'-1} q_{i_1'+1} \cdots q_m$ and we can finish the argument by induction on $n$. ∎

<u>Theorem</u>. A Noetherian integral domain is a UFD if and only if any irreducible is prime.

<u>Pf</u>. This is an immediate corollary of the previous propositions. ∎

# Lecture 19: PID implies UFD

Thursday, December 6, 2018 8:59 AM

<u>Theorem</u>. PID $\Rightarrow$ UFD.

<u>Pf</u>. • Suppose $D$ is a PID; then any ideal is principal, and so any ideal is f.g., which implies $D$ is Noetherian.

• In a PID, we have that $p$ is irreducible $\Leftrightarrow$ $p$ is prime.

Hence claim follows from the previous theorem. ∎

In general we would like to know if a given ring property can be passed on to the ring of polynomials:

$$A \text{ has property } * \Rightarrow A[x] \text{ has property } *.$$

For instance we have seen that, if $A$ is an integral domain, then $A[x]$ is an integral domain.

<u>Roughly geometrically means</u>: suppose $TV$ is the trivial line bundle over a variety $V$. What kind of properties of $V$ would be passed on to $TV$?

Next we see that being a PID is NOT one of those properties.

In fact we show a much stronger statement:

# Lecture 19: When is A[x] a PID? Spec of PID

Thursday, December 6, 2018  8:59 AM

<u>Theorem.</u> $A[x]$ is a PID $\Leftrightarrow$ $A$ is a field.

First we study $\mathrm{Spec}(D)$ when $D$ is a PID, and then prove the above theorem.

<u>Theorem</u>. Suppose $D$ is a PID. Then $\mathrm{Spec}\, D = \{0\} \cup \mathrm{Max}\, D$.

<u>Pf</u>.. For any unital commutative ring $D$, $\mathrm{Max}\, D \subseteq \mathrm{Spec}\, D$.

. For an integral domain, $0 \in \mathrm{Spec}\, D$.

. Suppose $\mathfrak{p} \in \mathrm{Spec}\, D \setminus \{0\}$. Since $D$ is a PID, $\mathfrak{p} = \langle p \rangle$.

$$\left.\begin{array}{l}\mathfrak{p} = \langle p \rangle \text{ prime} \\ p \neq 0\end{array}\right\} \Rightarrow \left.\begin{array}{l} p \text{ prime} \\ D \text{ PID}\end{array}\right\} \Rightarrow p \text{ irreducible}$$

$$\Rightarrow \langle p \rangle \text{ maximal among proper principal ideals}$$

$$D \text{ PID} \quad \Rightarrow \langle p \rangle \in \mathrm{Max}\, D. \quad \blacksquare$$

• For $\mathfrak{a} \triangleleft A$, $\pi_{\mathfrak{a}} : A[x] \to (A/\mathfrak{a})[x]$, $\pi_{\mathfrak{a}}(\sum_i a_i x^i) := \sum_i (a_i + \mathfrak{a}) x^i$

is an onto ring homomorphism, and

$\ker \pi_{\mathfrak{a}} = \{ \sum_i a_i x^i \mid a_i \in \mathfrak{a} \}$ is denoted by $\mathfrak{a}[x]$.

So $A[x]/\mathfrak{a}[x] \simeq (A/\mathfrak{a})[x]$.

# Lecture 19: When is A[x] a PID?

Friday, December 7, 2018 4:29 PM

<u>Cor.</u> $\mathfrak{p} \in \operatorname{Spec} A \Rightarrow \mathfrak{p}[x] \in \operatorname{Spec} A[x] \setminus \operatorname{Max} A[x]$.

<u>Pf.</u> . $\mathfrak{p} \in \operatorname{Spec} A \Rightarrow A/\mathfrak{p}$ is integral domain $\Rightarrow (A/\mathfrak{p})[x]$ is integral domain

$\Rightarrow A[x]/\mathfrak{p}[x]$ is integral domain

$\Rightarrow \mathfrak{p}[x] \in \operatorname{Spec} A[x]$.

. $A[x]/\mathfrak{p}[x] \simeq (A/\mathfrak{p})[x]$

$A/\mathfrak{p}$ : integral domain $\Rightarrow ((A/\mathfrak{p})[x])^\times = (A/\mathfrak{p})^\times$

$\Rightarrow (A/\mathfrak{p})[x]$ is NOT a field

$\Rightarrow \mathfrak{p}[x]$ is NOT maximal. ■

was not mentioned in class

<u>Cor.</u> If $A$ has a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals, $A[x]$ has a chain of prime ideals whose length is $\underline{1}$ more.

<u>Pf.</u> $\mathfrak{p}_0[x] \subsetneq \mathfrak{p}_1[x] \subsetneq \cdots \subsetneq \mathfrak{p}_n[x]$ is a chain of primes in $A[x]$; since $\mathfrak{p}_n[x]$ is NOT maximal, $\exists\, \mathfrak{m} \in \operatorname{Max} A[x]$ s.t. $\mathfrak{p}_n[x] \subsetneq \mathfrak{m}$; and claim follows. ■

In Math 200c, we define $\dim A :=$ sup. length of chain of primes, and show $\dim A[x] = \dim A + 1$. The above corollary shows the "easy" part $\dim A[x] \geq \dim A + 1$.

# Lecture 19: Hilbert's basis theorem

Thursday, December 6, 2018 9:08 AM

One of the important properties that can be passed to the ring of poly. from a ring is the Noetherian condition.

Theorem. $A$ is Noetherian $\Longleftrightarrow$ $A[x]$ is Noetherian.

Pf. The easy direction ($\Leftarrow$) was not given in class. Here is its one line proof: $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \Rightarrow \mathfrak{a}_1[x] \subsetneq \mathfrak{a}_2[x] \subsetneq \cdots$!

($\Rightarrow$) Informal part We have to show any ideal $\mathfrak{a}$ of $A[x]$ is f.g..

When $A$ is a field, we used long division to show any ideal is principal. So we need to come up with a generalization of long division. In the process of long division, at each step we multip. by a suitable monomial to get rid of the leading term, and get a smaller degree poly. and repeat this algorithm. In order to get rid of the leading term $ax^n$ we need to multi. the leading term $bx^m$ of the divisor by a monomial to match $ax^n$. That monomial is $\frac{a}{b}x^{n-m}$; so we need to have $a \in \langle b \rangle$ (and $n \geq m$). This condition is clear in a field. When $A$

# Lecture 19: Proof of Hilbert's basis theorem

Friday, December 7, 2018 5:02 PM

is not a field, we will follow a similar line of logic; so we have to be able to access the leading coeff.. Let

(formal)

$$\mathrm{ld}(\mathfrak{a}) := \{a \in A \mid \exists\ a x^n + \underbrace{\text{terms of smaller deg}} \in \mathfrak{a} \text{ for some } n \in \mathbb{Z}^{\geq 0}\} \cup \{0\}$$

<u>Claim</u>. $\mathrm{ld}(\mathfrak{a}) \trianglelefteq A$.

<u>Pf of Claim</u>. $a_1, a_2 \in \mathrm{ld}(\mathfrak{a}) \Rightarrow \exists\ f_i(x) = a_i x^{n_i} + \cdots \in \mathfrak{a}$

$$\Rightarrow x^{n_2} f_1(x) + x^{n_1} f_2(x) = (a_1 + a_2)\, x^{n_1+n_2} + \text{smaller deg terms} \in \mathfrak{a}$$

either $a_1 + a_2 = 0$ or $a_1 + a_2$ is the leading coeff. of an element of $\mathfrak{a}$.

So in either case $a_1 + a_2 \in \mathrm{ld}(\mathfrak{a})$.

- $a \in \mathrm{ld}(\mathfrak{a}) \Rightarrow \exists\ f(x) = a x^n + \cdots \in \mathfrak{a}$

$$\Rightarrow \forall r \in A,\quad r f(x) = (ra)\, x^n + \cdots \in \mathfrak{a}$$

$$\Rightarrow ra \in \mathrm{ld}(\mathfrak{a}). \qquad \blacksquare \text{ (Claim)}.$$

Since $A$ is Noetherian, $\exists\ a_1, \ldots, a_m \in A$ s.t.

$$\mathrm{ld}(\mathfrak{a}) = \langle a_1, \ldots, a_m \rangle.$$

And so $\exists\ f_i(x) = a_i x^{n_i} + \text{smaller deg. terms} \in \mathfrak{a}$.

(Informal) Next we try to see how much of $\mathfrak{a}$ can be generated

# Lecture 19: Proof of Hilbert's basis theorem

Friday, December 7, 2018 5:17 PM

by $f_1, \ldots, f_m$?"

So we pick $f \in \mathfrak{a}$; then $f(x) = a x^n + \cdots$. We want to use a linear combination of $f_i$'s to get rid of the leading term of $f$, and then repeat this algorithm:

$a \in ld(\mathfrak{a}) \Rightarrow \exists\, r_1, \ldots, r_m \in A,\ a = r_1 a_1 + \cdots + r_m a_m$; and

so $$\underbrace{a x^n}_{\substack{\text{leading}\\ \text{term of}\\ f(x)}} = (r_1 x^{n-n_1})\underbrace{(a_1 x^{n_1})}_{\substack{\text{leading}\\ \text{term of}\\ f_1(x)}} + \cdots + (r_m x^{n-n_m})\underbrace{(a_m x^{n_m})}_{\substack{\text{leading}\\ \text{term of}\\ f_m(x)}}$$

But this idea works only when $n \geq \max\{n_1, \ldots, n_m\}$. For $k < \max\{n_1, \ldots, n_m\}$ we need to focus on the leading coeff. of polynomials of degree $k$:

Formal:

$$ld_k(\mathfrak{a}) := \{a \in A \mid \exists\ \underset{a \neq 0}{a x^k} + \text{smaller deg. terms} \in \mathfrak{a}\} \cup \{0\}.$$

Claim. For any $k \in \mathbb{Z}^{\geq 0}$, $ld_k(\mathfrak{a}) \trianglelefteq A$.

Pf of Claim. $\bullet\ a_1, a_2 \in ld_k(\mathfrak{a}) \Rightarrow \exists\, f_i(x) = a_i x^k + \cdots \in \mathfrak{a}$

$\Rightarrow f_1(x) + f_2(x) = (a_1 + a_2) x^k + \cdots \in \mathfrak{a} \Rightarrow a_1 + a_2 \in ld_k(\mathfrak{a})$.

# Lecture 19: Proof of Hilbert's basis theorem

Saturday, December 8, 2018 12:06 AM

- $a \in ld_k(\mathfrak{A}) \Rightarrow \exists\, f(x) = ax^k + \cdots \in \mathfrak{A}$

$$\Rightarrow \forall r \in A,\ r f(x) = (ra)x^k + \cdots \in \mathfrak{A}$$

$$\Rightarrow ra \in ld_k(\mathfrak{A}). \qquad \blacksquare \text{ (claim)}$$

So $\exists\, b_{ik} \in A$ s.t. $ld_k(\mathfrak{A}) = \langle b_{1k}, \ldots, b_{\ell_k k} \rangle$ ; and

$\exists\, g_{ik}(x) = b_{ik} x^k + \cdots \in \mathfrak{A}$.

informal:

By a similar argument as before we can get rid of leading term of a poly. of deg. $k$ in $\mathfrak{A}$ using an $A$-linear combin. of $g_{1k}, \ldots, g_{\ell_k k}$. And so we get

$$\mathfrak{A} = \left\langle f_1, \ldots, f_m, g_{ij} ;\ \begin{matrix} 1 \le j < \max\{n_1, \ldots, n_m\} \\ 1 \le i \le \ell_j \end{matrix} \right\rangle \qquad \square$$

A complete version of a formal proof (modulo the results that $ld(\mathfrak{A}), ld_k(\mathfrak{A}) \trianglelefteq A$) is given in the lecture note of lecture 20.