Lecture 18: PID implies UFD

Tuesday, September 5, 2017 10:05 PM

<u>Theorem</u> If D is a PID, then D is a UFD.

In the previous lecture we proved the uniqueness part. Now we want to prove the existence part:

<u>Existence</u>. $\underline{a}$ can be written as a product of irreducibles if $a \neq 0$ and $a \notin D^\times$.

<u>Why should it be true?</u>. If a is irreducible, then we are done

. If not, $a = a_1 a_2$ where a_1 and a_2 are not units

. Continue this process for a_1 and a_2.

<u>Question</u>. Why does this process stops?

(For $\mathbb{Z}$, we can use the absolute value; and for $F[x]$, we can use the degree of polynomials to show this.)

<u>Proof of existence</u> (the general case: not part of the exam.)

$$A = \{a \in D \mid a \neq 0,\ a \notin D^\times,\ a \text{ cannot be written as a product of irreducibles}\}.$$

If A is empty, we are done. So suppose to the contrary that $a_0 \in A$. Hence, in particular, a_0 is not irreducible. So $a_0 = a_1 b_1$

for some $a_1, b_1 \in D \setminus D^\times$. Since D is an integral domain and $a_0 \neq 0$, we have a_1 and b_1 are non-zero. If $a_1, b_1 \notin A$, then that means a_1 and b_1 can be written as a product of irreducibles (as they are not either 0 or a unit). This implies $a_0 = a_1 b_1$ can be written as a product of irreducibles, which contradicts $a_0 \in A$. So either $a_1 \in A$ or $b_1 \in A$. Without loss of generality, we can and will assume $a_1 \in A$. By a similar argument inductively we can find a sequence $a_1, a_2, \dots$ of elements of D such that $\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots$ and

$$a_i = a_{i+1} b_{i+1} \quad \text{where } b_{i+1} \notin D^\times.$$

Now let $I = \bigcup_{i=0}^{\infty} \langle a_i \rangle$. Show that I is an ideal of D.

Since D is a PID, $\exists\, b \in D$ such that $I = \langle b \rangle$.

So $b \in \bigcup_{i=0}^{\infty} \langle a_i \rangle$, which means $\exists\, i_0$ such that $b \in \langle a_{i_0} \rangle$.

Therefore $\langle b \rangle \subseteq \langle a_{i_0} \rangle \Rightarrow \forall\, i \geq i_0$, $\langle a_i \rangle \subseteq \langle b \rangle \subseteq \langle a_{i_0} \rangle$ and $\langle a_{i_0} \rangle \subseteq \langle a_i \rangle$.

This implies $\langle a_i \rangle = \langle a_{i_0} \rangle$. Show that $\langle a_{i_0+1} \rangle = \langle a_{i_0} \rangle$ implies

Lecture 18: Existence; Alternative proof for F[x]

Thursday, September 7, 2017 2:13 PM

b_{i_0+1} is a unit which is a contradiction. ■

Here we present an alternative proof of the existence part when $D = F[x]$. (This proof is part of exam.)

• Any non-constant polynomial $f(x) \in F[x]$ can be written as a product of irreducible polynomials in $F[x]$.

<u>Proof.</u> We proceed by the strong induction on $\deg(f)$.

<u>Base of induction.</u> $\deg(f) = 1$.

Since F is a field, any degree 1 polynomial in $F[x]$ is irreducible. So $f(x)$ is irreducible; this implies that $f(x)$ is already written as a product of irreducible polynomial(s) with only one factor.

<u>The strong induction step</u>. Suppose any non-constant polynomial $g(x)$ of degree $< k$ is a product of irreducible polynomials. We have to show any polynomial $f(x)$ of degree k is a product of irreducible polynomials.

Lecture 18: Existence: case of F[x]

Thursday, September 7, 2017 2:24 PM

<u>Case 1.</u> $f(x)$ is irreducible.

In this case, $f(x)$ is already written as a product of irreducible polynomial(s), with only one factor.

<u>Case 2.</u> $f(x)$ is NOT irreducible.

In this case, as $f(x)$ is NOT a constant polynomial, we can write $f(x)$ as a product of two non-constant polynomials $g(x)$ and $h(x)$.

Since $f(x) = g(x)h(x)$ and $g(x), h(x)$ are not constant, we have $\deg g, \deg h < \deg f = k$.

So, by the strong induction hypothesis, $g(x)$ and $h(x)$ are products of irreducible polynomials; that means there are irreducible polynomials $p_1(x), \ldots, p_n(x)$ and $q_1(x), \ldots, q_m(x) \in F[x]$, such that $g(x) = p_1(x) \cdots p_n(x)$ and $h(x) = q_1(x) \cdots q_m(x)$. Thus $f(x) = g(x)h(x) = p_1(x) \cdots p_n(x) \cdot q_1(x) \cdots q_m(x)$, which means $f(x)$ can be written as a product of irreducible polynomials. ∎

Lecture 18: In a UFD irreducible implies PID

Sunday, March 17, 2019 6:34 PM

Remark. In the proof of the general case we showed that, if D is a PID and $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of D, then $I_{n_0} = I_{n_0+1} = \cdots$. We say a ring is Noetherian if it satisfies this property.

Next I want to give you an example of a ring that is not a UFD. The key to such examples is the following lemma:

Lemma. Suppose D is a UFD. Then if $d \in D$ is irred. in D, then d is prime in D.

Pf. • Since d is irreducible in D, $d \notin \{0\} \cup D^\times$.

• Suppose $d \mid ab$. So $\exists\, c \in D$ s.t. $dc = ab$.

$$a \in D^\times \Rightarrow \langle a \rangle = D \Rightarrow d \in \langle a \rangle \Rightarrow d \mid a$$

$$a = 0 \Rightarrow d \cdot 0 = 0 \Rightarrow d \mid a$$

Similarly, if $b \in D^\times \cup \{0\}$, then $d \mid b$.

• Next we assume $a, b \notin D^\times \cup \{0\}$. As $a \neq 0$ and $b \neq 0$, $ab \neq 0$. and so $c \neq 0$. Since D is a UFD, there are irreducibles

Lecture 18: In a UFD irreducible implies prime

Sunday, March 17, 2019 6:58 PM

p_i's, q_{r_j}'s, and l_k's s.t.

$$a = \prod p_i, \quad b = \prod q_{r_j}, \quad c = \prod l_k \text{ or } c \in D^\times.$$

Hence $d \cdot \underbrace{\prod l_k}_{\text{or a unit}} = \prod p_i \cdot \prod q_{r_j}$. By the uniquessness part of being a UFD, d should appear at the right hand side after multiplying by a unit; that means

$\exists i, u \in D^\times$, either $p_i = du$ or $q_{r_i} = du$.

If $p_i = du$, then $\left.\begin{array}{l} d \mid p_i \\ p_i \mid a \end{array}\right\} \Rightarrow d \mid a$

If $q_{r_i} = du$, then $\left.\begin{array}{l} d \mid q_{r_i} \\ q_{r_i} \mid b \end{array}\right\} \Rightarrow d \mid b$.

Overall we have $d \mid ab \Rightarrow d \mid a$ or $d \mid b$;

therefore d is prime. ∎

Next we use this property to show:

- $\mathbb{Z}[\sqrt{-10}]$ is not a UFD.

By the previous lemma it is enough to find an element that is irreducible but not prime.

The norm map $N: \mathbb{Z}[\sqrt{-10}] \to \mathbb{Z}^{\geq 0}$,

$$N(a+\sqrt{-10}\, b) = a^2 + 10\, b^2$$

is extremely useful for this type of problem.

Notice that, for $z \in \mathbb{C}$, $N(z) := |z|^2$; and so for z_1, z_2 we have $N(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_2|^2$

$$= N(z_1)\, N(z_2).$$

The first step in showing an element is irred. is to show that it is not a unit. So first we need to find $\mathbb{Z}[\sqrt{-10}]^\times$.

<u>Claim</u>. $\mathbb{Z}[\sqrt{-10}]^\times = \{\pm 1\}$.

<u>Pf of Claim</u>. $z = a + \sqrt{-10}\, b \in \mathbb{Z}[\sqrt{-10}]^\times \Rightarrow$

$\exists\, z' \in \mathbb{Z}[\sqrt{-10}],\ z \cdot z' = 1 \Rightarrow$

$$N(z \cdot z') = N(1) \Rightarrow \underbrace{N(z)}_{\text{in } \mathbb{Z}^{\geq 0}} \cdot \underbrace{N(z')}_{\text{in } \mathbb{Z}^{\geq 0}} = 1$$

$\Rightarrow N(z) = 1 \Rightarrow a^2 + 10\, b^2 = 1$

Lecture 18: Showing a domain is not a UFD

Sunday, March 17, 2019 7:18 PM

. If $b \neq 0$, then $b^2 \geq 1$. Hence $a^2 + 10b^2 \geq 10$

$\Rightarrow a^2 + 10b^2 \neq 1$. Therefore $b = 0$; and so

$a^2 = 1$, which implies $a = \pm 1$. Overall we got

$b = 0$ and $a = \pm 1$, which implies

$z = a + \sqrt{-10}\, b = \pm 1$. ■

<u>Claim</u>. $\sqrt{-10}$ is irreducible in $\mathbb{Z}[\sqrt{-10}]$.

<u>Pf of claim</u>. By the previous claim, $\sqrt{-10} \notin \mathbb{Z}[\sqrt{-10}]^{\times}$.

$\sqrt{-10} = z \cdot \omega$ for $z, \omega \in \mathbb{Z}[\sqrt{-10}]$.

$$\Rightarrow \underbrace{N(\sqrt{-10})}_{10} = N(z \cdot \omega) = \underbrace{N(z)}_{\text{in } \mathbb{Z}^{\geq 0}} \cdot \underbrace{N(\omega)}_{\text{in } \mathbb{Z}^{\geq 0}}$$

$\Rightarrow$ either $N(z) = 1$ and $N(\omega) = 10$, or

$N(z) = 2$ and $N(\omega) = 5$, or

$N(z) = 5$ and $N(\omega) = 2$, or

$N(z) = 10$ and $N(\omega) = 1$.

If $N(z) = 1$, then by the previous argument $z = \pm 1$. Similarly

if $N(\omega) = 1$, then $\omega = \pm 1$. And so in these cases one of

Lecture 18: Showing a domain is not a UFD

Sunday, March 17, 2019 8:16 PM

the factors is a unit (as we desired). Hence it is enough to show $N(z') \neq 2$ for some $z' \in \mathbb{Z}[\sqrt{-10}]$.

Suppose to the contrary that $N(a+\sqrt{-10}\,b) = 2$ for some $a, b \in \mathbb{Z}$. If $b \neq 0$, then

$$b^2 \geq 1 \Rightarrow a^2 + 10b^2 \geq 10 \Rightarrow N(a+\sqrt{-10}\,b) \neq 2.$$

So $b=0$, which implies $a^2=2$. This is not possible as $\sqrt{2}$ is not an integer.

<u>Claim</u> $\sqrt{-10}$ is not prime in $\mathbb{Z}[\sqrt{-10}]$.

<u>Pf of claim</u>. $(\sqrt{-10}) \cdot (\sqrt{-10}) = 10 = (2)(5)$.

$$\Rightarrow \sqrt{-10} \mid (2)(5).$$

- $\sqrt{-10} \nmid 2$, $\sqrt{-10}\,(a+b\sqrt{-10}) = \sqrt{-10}\,a - 10b$
$$= 2$$
$$\Rightarrow -10b = 2$$
$$\Rightarrow b = \frac{1}{5} \in \mathbb{Z}$$ which is a contradiction.

- $\sqrt{-10} \nmid 5$, $\sqrt{-10}\,(a+b\sqrt{-10}) = \sqrt{-10}\,a - 10b = 5$
$$\Rightarrow -10b = 5 \Rightarrow b = -1/2 \in \mathbb{Z}$$ which

Lecture 18: Showing a domain is not a UFD

Sunday, March 17, 2019 8:27 PM

is a contradiction.

Since $\sqrt{-10}$ is irreducible and not prime, $\mathbb{Z}[\sqrt{-10}]$ is not a UFD.