Lecture 02: An integral domain that is not UFD

Wednesday, January 10, 2018 12:31 AM

Ex. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Pf. In a UFD any irreducible element is prime. So it is enough to find an irreducible element which is not prime.

Claim 1. 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Pf of claim 1. Suppose $3=(a_1+\sqrt{-5}\,b_1)(a_2+\sqrt{-5}\,b_2)$ and $a_i, b_i \in \mathbb{Z}$

$\Rightarrow 9=(a_1^2+5b_1^2)(a_2^2+5b_2^2)$

$\Rightarrow$ either $a_1^2+5b_1^2=a_2^2+5b_2^2=3$ or $\exists i,\ a_i^2+5b_i^2=1$.

Notice that, if $b_1 \neq 0$, then $a_1^2+5b_1^2 \geq 5$; and 3 is not a perfect square. Hence $\forall a_1, b_1 \in \mathbb{Z}$, $a_1^2+5b_1^2 \neq 3$. Therefore $\exists i,\ a_i^2+5b_i^2=1$, which implies $(a_i+\sqrt{-5}\,b_i)(a_i-\sqrt{-5}\,b_i)=1$

$\Rightarrow a_i+\sqrt{-5}\,b_i \in \mathbb{Z}[\sqrt{-5}]^{\times}$; and the claim follows.

Claim 2. $3 \mid (1+\sqrt{-5})(1-\sqrt{-5})$; this is clear.

Claim 3. $3 \nmid 1\pm\sqrt{-5}$.

Pf of claim 3. If not, $\exists a, b \in \mathbb{Z}$, $3(a+\sqrt{-5}\,b)=1\pm\sqrt{-5}$
$\Rightarrow 3a=1$ and $3b=1$ (here we are using the fact that $\sqrt{-5}\notin\mathbb{Q}$); which is a contradiction.

Lecture 02: Ring of polynomials

Wednesday, January 10, 2018 10:39 AM

Hence 3 is not prime. Therefore $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $\blacksquare$

Next we would like to show $\mathbb{Z}[x]$ is a UFD, but it is not a PID.

It will be done in many steps:

Proposition. $R[x]$ is a PID $\Leftrightarrow$ R is a field.

Thm. $R[x]$ is a UFD $\Leftrightarrow$ R is a UFD.

Clearly the above Prop. and Thm imply that $\mathbb{Z}[x]$ is a UFD and it is not a PID.

To prove the above proposition we start with the following lemma:

Lemma. Suppose A is a unital commutative ring and $\mathfrak{a} \trianglelefteq A$.

Let $\phi_{\mathfrak{a}} : A[x] \to (A/\mathfrak{a})[x]$, $\phi_{\mathfrak{a}}(\sum_{i=0}^{\infty} a_i x^i) = \sum_{i=0}^{\infty} (a_i + \mathfrak{a}) x^i$.

Then $\phi_{\mathfrak{a}}$ is an onto ring homomorphism, and

$$\ker \phi_{\mathfrak{a}} = \mathfrak{a}[x] := \{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathfrak{a},\ a_i = 0 \text{ except for finitely many } i \}.$$

Pf. (Exercise)

Cor. In the above setting, $A[x]/\mathfrak{a}[x] \simeq (A/\mathfrak{a})[x]$. (Pf. Use 1^{st} iso. thm.)

Lecture 02: Ring of polynomials

Wednesday, January 10, 2018 10:51 AM

<u>Cor.</u> $\mathfrak{p} \in \mathrm{Spec}(A) \Leftrightarrow \mathfrak{p}[x] \in \mathrm{Spec}(A[x])$.

<u>Pf.</u> $\mathfrak{p} \in \mathrm{Spec}(A) \Leftrightarrow A/\mathfrak{p}$ is an integral domain

$\Leftrightarrow (A/\mathfrak{p})[x]$ is an integral domain

by the previous corollary.

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

$\Leftrightarrow \mathfrak{p}[x] \in \mathrm{Spec}(A)$. ∎

<u>Pf of proposition.</u> ($\Leftarrow$) R: field $\Rightarrow$ we have long division in $R[x]$

$\Rightarrow R[x]$ is a Euclidean domain $\Rightarrow R[x]$ is a PID.

($\Rightarrow$) Suppose $a \in R \setminus \{0\}$. We have to show $a \in R^{\times}$; this is equivalent to saying $\langle a \rangle = R$. Suppose to the contrary that $\langle a \rangle$ is a proper ideal. So there is a maximal ideal $\mathfrak{m}$ s.t. $\langle a \rangle \subseteq \mathfrak{m}$. Hence $\mathfrak{m} \in \mathrm{Spec}(R)$; and by the previous corollary $\mathfrak{m}[x] \in \mathrm{Spec}(R[x])$.

Since $R[x]$ is a PID, $\mathrm{Spec}(R[x]) = \mathrm{Max}(R[x]) \cup \{0\}$.

As $a \neq 0$ and $a \in \mathfrak{m}[x]$, we deduce that $\mathfrak{m}[x] \in \mathrm{Max}(R[x])$.

Therefore $R[x]/\mathfrak{m}[x]$ is a field. On the other hand,

Lecture 02: gcd

Wednesday, January 10, 2018 11:18 AM

$R[x]/\mathfrak{m}[x] \simeq (R/\mathfrak{m})[x]$; and $((R/\mathfrak{m})[x])^\times = (R/\mathfrak{m})^\times$ as $R/\mathfrak{m}$ is a field. So $(R/\mathfrak{m})[x]$ cannot be a field, which gives us a contradiction. ■

To prove the mentioned theorem, we start with the definition of greatest common divisor of elements of a ring.

<u>Def</u>. • Suppose $\underset{\neq 0}{a}, b \in D$; we say $a|b$ if $\exists\, c \in D$ s.t. $b = ac$.

• We say d is a greatest common divisor of $\overset{\#0}{a_1}, \ldots, a_n$ if (1) $\forall i$, $d | a_i$, (2) if $d' | a_i$ for any i, then $d' | d$.

<u>Lemma</u>. Suppose D is an integral domain;

(a) d is a gcd of $a_1, \ldots, a_n$ if and only if $\langle d \rangle$ is the <u>minimum</u> principal ideal which contains $\langle a_1, \ldots, a_n \rangle$.

(b) If d_1 and d_2 are two gcd's of $a_1, \ldots, a_n$, then $\langle d_1 \rangle = \langle d_2 \rangle$ (and so $d_1 \sim d_2$).

<u>Pf.</u> (a). $d | a_i \Rightarrow a_i \in \langle d \rangle \Rightarrow \langle a_1, \ldots, a_n \rangle \subseteq \langle d \rangle$.

• If $\langle a_1, \ldots, a_n \rangle \subseteq \langle d' \rangle$, then $d' | a_i$ $\underline{\forall i}$.

Hence $d' | d$, which implies $\langle d \rangle \subseteq \langle d' \rangle$.

Lecture 02: gcd

Friday, January 12, 2018 11:08 AM

(b) By part (a), $\langle d_1\rangle$ and $\langle d_2\rangle$ are the minimum principal ideal that contains $\langle a_1,\ldots,a_n\rangle$; and so $\langle d_1\rangle = \langle d_2\rangle$. As D is an integral domain, we deduce that $d_1 \sim d_2$. $\blacksquare$