Lecture 23: PID implies UFD

Friday, May 25, 2018 1:14 PM

Theorem. PID $\Rightarrow$ UFD.

Pf. Existence. We considered the following process:

- if d is irreducible, we are done
- If not, $d = d_1 d_1'$ and d_1, d_1' are non-zero, non-unit
- Repeat for d_1 and d_1'.

If this process stops, we are done. If not, $\exists\, d_i, d_i' \in D$ st. d_i, d_i' are non-zero non-units and

$d = d_1 d_1'$, $d_1 = d_2 d_2'$, $d_2 = d_3 d_3'$, ... Hence

$\langle d \rangle \underset{\substack{\uparrow \\ d_1' \text{ is not} \\ \text{a unit}}}{\subsetneq} \langle d_1 \rangle \subsetneq \langle d_2 \rangle \subsetneq \cdots$. Let $I := \bigcup_{i=1}^{\infty} \langle d_i \rangle$.

Claim. $I \trianglelefteq D$.

Pf of claim. We use ideal criterion; $x, y \in I$, $a \in D$,

$\Rightarrow x \in \langle d_i \rangle$ and $y \in \langle d_j \rangle$ for some $i, j \in \mathbb{Z}^+$. W.L.O.G let's assume $i \le j$. Hence $x, y \in \langle d_j \rangle$; and so $x - y \in \langle d_j \rangle \subseteq I$.

Hence $x - y \in I$. We also have $ax \in \langle d_i \rangle \subseteq I$; and claim follows.

Lecture 23: PID implies UFD

Friday, May 25, 2018 11:20 AM

Since D is a PID, $\exists\, d' \in D$, $I = \langle d' \rangle$.

Hence $\exists i$ s.t. $d' \in \langle d_i \rangle$, which implies $I = \langle d' \rangle \subseteq \langle d_i \rangle$

And so for any $i \leq j$, $I \subseteq \langle d_j \rangle \subseteq I$; and this

implies $\langle d_j \rangle = I$ if $i \leq j$; in particular

$\langle d_i \rangle = \langle d_{i+1} \rangle$ which is a contradiction. $\square$

Uniqueness. What does it mean?

Suppose p_i's and q_j's are irreducible, and

$p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m$. Then $m = n$, and

there is a reordering $i_1, \dots, i_n$ of $1, \dots, n$ and units u_j s.t.

$p_j = u_j \, q_{i_j}$ for any $1 \leq j \leq n$.

We proceed by induction on n.

$p_1 \cdot \dots \cdot p_n \in \langle p_n \rangle \Rightarrow q_1 \cdot \dots \cdot q_m \in \langle p_n \rangle$

$\left.\begin{array}{l} p_n : \text{irreducible} \\ D : \text{PID} \end{array}\right\} \Rightarrow \langle p_n \rangle : \text{maximal} \Rightarrow \langle p_n \rangle : \text{prime}$

for some i, $q_i \in \langle p_n \rangle$.

Lecture 23: PID implies UFD; uniqueness

Friday, May 25, 2018 11:30 AM

Hence $\langle q_i \rangle \subseteq \langle p_n \rangle$

q_i : irreducible, D : PID $\Rightarrow$ $\langle q_i \rangle$ is maximal

$\Rightarrow$ $\langle q_i \rangle = \langle p_n \rangle$ which implies $p_n = v_n q_i$ for some $v_n \in D^\times$.

And so $p_1 \cdots p_{n-1} p_n = q_1 \cdots q_m$ implies

$$p_1 \cdot \cdots \cdot p_{n-1} \cdot v_n q_i = q_1 \cdots q_{i-1} q_i q_{i+1} \cdots q_m .$$ Hence

$$p_1 \cdot \cdots \cdot p_{n-1} \cdot v_n = q_1 \cdot \cdots \cdot q_{i-1} q_{i+1} \cdots q_m$$

$p_1, p_2, \ldots, p_{n-2}, v_n p_{n-1}$ are irreducible in D; and so by the induction hypothesis $m-1 = n-1$ (which implies $n=m$); and $p_1, \ldots, p_{n-2}$, and $v_n p_{n-1}$ are the same as $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m$ up to reordering and multiplying by units; and claim follows. ∎

Next we go back to the study of zeros of a polynomial. We will show any poly. $p(x) \in F[x]$ has a zero in some field extension.

Lecture 23: Field extension

Wednesday, May 30, 2018 11:03 AM

<u>Theorem</u>. Suppose F is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then

(1) $\exists$ a field E and an injective ring homomorphism $i : F \hookrightarrow E$ s.t.

(1-a) for some $\alpha \in E$, $i(f)(\alpha) = 0$.

($f(x)$ has a zero in E.)

(1-b) $E = \{ i(a_0) + i(a_1)\alpha + \cdots + i(a_{n-1})\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in F \}$

where $n = \deg f$.

(2) If E' is a field and $i' : F \hookrightarrow E'$ is an injective ring homomorphism that satisfy (1-a) and (1-b), then $\exists\, \phi : E \xrightarrow{\simeq} E'$ s.t. $\phi(i(a)) = i'(a)$ for any $a \in F$.

$$\begin{tikzcd} & E \arrow[dd, dashed, "\phi"] \\ F \arrow[ur, hook, "i"] \arrow[dr, hook, "i'"'] \arrow[r, phantom, "\circlearrowleft"] & {} \\ & E' \end{tikzcd}$$

<u>Idea of pf.</u> Suppose E is a field, and $\alpha \in E$ is a zero of $f(x)$.

Then kernel of $\phi_\alpha : F[x] \to E$, $\phi_\alpha(p(x)) = p(\alpha)$ contains $f(x)$.

Since $f(x)$ is irreducible, we have seen that $\ker \phi_\alpha = \langle f(x) \rangle$, and

Lecture 23: Field extension

Wednesday, May 30, 2018 10:19 PM

$\mathrm{Im}\,\Phi_\alpha$ is a field; and $F[x]/\langle f(x)\rangle \xrightarrow{\sim} \mathrm{Im}\,\Phi_\alpha$. In particular,

$$p(x)+\langle f(x)\rangle \longmapsto p(\alpha)$$

$x+\langle f(x)\rangle \longmapsto \alpha$.

So it seems we are forced to think about $F[x]/\langle f(x)\rangle$.