Lecture 17: Principal ideals

Sunday, March 17, 2019 5:04 PM

Suppose D is an integral domain. For any $d\in D$, we will denote the principal ideal dD by $\langle d\rangle$.

Warning. From the context you should find out that we are talking about the principal ideal and not the group generated by d. So $\langle d\rangle \neq \{\ldots, d^{-2}, d^{-1}, 1, d, d^2, \ldots\}$.

Next we will see the connection between properties of d and $\langle d\rangle$.

- $\langle d\rangle = D \Leftrightarrow d\in D^{\times}$

- Pf. $(\Rightarrow)$ $\langle d\rangle = D \Rightarrow 1\in\langle d\rangle$

$$\Rightarrow \exists c\in D,\ 1=d\cdot c$$
$$\Rightarrow d\in D^{\times}$$

$(\Leftarrow)$ $d\in D^{\times} \Rightarrow \exists c\in D,\ 1=dc$

$$\Rightarrow \forall d'\in D,\ d'=d(cd')\in\langle d\rangle$$
$$\Rightarrow D\subseteq\langle d\rangle$$
$$\Rightarrow D=\langle d\rangle.$$

- $b\mid a \Leftrightarrow a\in\langle b\rangle \Leftrightarrow \langle a\rangle\subseteq\langle b\rangle$.

Lecture 17: Principal ideals

Sunday, March 17, 2019 5:15 PM

Pf. $a|b \Rightarrow \exists c\in D,\ b=ac \Rightarrow b\in\langle a\rangle$

. $b\in\langle a\rangle \Rightarrow \exists c\in D,\ b=ac$

$\Rightarrow \forall d\in D,\ bd=(ac)d=a(cd)\in\langle a\rangle$

$\langle b\rangle\subseteq\langle a\rangle$.

. $\langle b\rangle\subseteq\langle a\rangle \Rightarrow b\cdot 1\in\langle b\rangle\subseteq\langle a\rangle$

$\Rightarrow b=ad$ for some $d\in D$

$\Rightarrow a|b$. ∎

• $\langle a\rangle=\langle b\rangle \Leftrightarrow \exists u\in D^{\times},\ a=bu$.

Pf. ($\Rightarrow$). If $a=0$, then $\langle a\rangle=\{0\}$; and so $\langle b\rangle=\{0\}$.

Therefore $b=0$. $\Rightarrow a=b=0$

. Suppose $a\neq 0$. $\langle a\rangle=\langle b\rangle \Rightarrow \begin{cases} a=bc \text{ for some } c\in D \\ b=ad \text{ for some } d\in D\end{cases}$

$\Rightarrow a=bc=adc \Rightarrow \left.\begin{array}{l} a(1-dc)=0 \\ a\neq 0 \\ \text{no zero-divisor}\end{array}\right\} \Rightarrow 1-dc=0$

$\Rightarrow 1=dc \Rightarrow c\in D^{\times}$ (and $a=bc$).

Lecture 17: Principal ideals

Sunday, March 17, 2019 5:28 PM

$(\Leftarrow)$ $a = bu \Rightarrow b \mid a \Rightarrow \langle a \rangle \subseteq \langle b \rangle$

$\left.\begin{array}{l} a = bu \\ u \in D^\times \end{array}\right\} \Rightarrow b = au^{-1} \Rightarrow a \mid b \Rightarrow \langle b \rangle \subseteq \langle a \rangle$

$\Rightarrow \langle a \rangle = \langle b \rangle$

$\blacksquare$

- **Recall**. Suppose D is a PID. Then

  d is irreducible in $D \Leftrightarrow \langle d \rangle$ is a maximal ideal.

Def. Suppose D is an integral domain; $p \in D \setminus (D^\times \cup \{0\})$ is called a prime element of D if

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

- Suppose D is an integral domain and $d \neq 0$. Then

  d is prime in $D \Leftrightarrow \langle d \rangle$ is a prime ideal in D.

Pf. $(\Rightarrow)$ $\cdot$ d is prime in $D \Rightarrow d \notin D^\times \Rightarrow \langle d \rangle \neq D$.

$\cdot$ $ab \in \langle d \rangle \Rightarrow d \mid ab \Rightarrow d \mid a$ or $d \mid b$

$\Rightarrow a \in \langle d \rangle$ or $b \in \langle d \rangle$.

$(\Leftarrow)$ $\cdot$ $\langle d \rangle$ is a prime ideal $\Rightarrow \langle d \rangle \neq D \Rightarrow d \notin D^\times$.

Lecture 17: Principal ideals

Sunday, March 17, 2019 5:38 PM

$d \mid ab \Rightarrow ab \in \langle d \rangle \Rightarrow a \in \langle d \rangle$ or $b \in \langle d \rangle$

$\Rightarrow d \mid a$ or $d \mid b$.

(and by assumption $d \neq 0$.) $\blacksquare$

<u>Summary</u>. Suppose D is an integral domain.

(a) $\langle d \rangle = D \Leftrightarrow d \in D^{\times}$.

(b) $d \mid d' \Leftrightarrow d' \in \langle d \rangle \Leftrightarrow \langle d' \rangle \subseteq \langle d \rangle$.

Suppose D is a PID.

(a) $\langle d \rangle$ is a maximal ideal $\Leftrightarrow d$ is irred. in D.

(b) $d \neq 0$ and $\langle d \rangle$ is a prime ideal $\Leftrightarrow d$ is prime in D.

In particular, in a PID, irreducible $\Rightarrow$ prime.

Next we show its converse.

<u>Proposition</u>. Suppose D is a PID. Then

$d \in D$ is irreducible in $D \Leftrightarrow d$ is prime in D.

<u>Pf</u>. ($\Rightarrow$) $d \in D$ irred. $\Rightarrow d \neq 0$ and $d \notin D^{\times}$ and $\langle d \rangle$ is maximal

Lecture 17: Prime, irreducible, PID

Sunday, March 17, 2019 5:50 PM

$\Rightarrow d \neq 0$ and $\langle d \rangle$ is prime $\Rightarrow d$ is prime.

($\Leftarrow$). d is prime $\Rightarrow d \neq 0$ and $d \notin D^{\times}$.

. Suppose $d = ab$. $\Rightarrow d \mid ab$

$\Rightarrow d \mid a$ or $d \mid b$

Without loss of generality we can and will assume $d \mid a$ (as the other case is similar). Hence $a = dc$ for some $c \in D$.

$\Rightarrow a = (ab)c = a(bc)$

$\Rightarrow a(1 - bc) = 0$.

Notice that $d \neq 0$ and $d = ab$; and so $a \neq 0$.

$1 - bc = 0 \Rightarrow bc = 1 \Rightarrow b \in D^{\times}$.

And so $d = ab \Rightarrow b \in D^{\times}$ or $a \in D^{\times}$, which implies d is irreducible in D. ∎

Next we show the uniqueness part of being a UFD for a PID.

Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019 5:57 PM

Theorem. Suppose D is a PID, $p_1, \dots, p_n, q_1, \dots, q_m$ are irreducible in D, and $p_1 \cdots p_n = q_1 \cdots q_m$. Then ① $m=n$

② $q_1 = u_1 p_{i_1}, q_2 = u_2 p_{i_2}, \dots, q_m = u_m p_{i_m}$ where $i_1, \dots, i_m$ is a permutation of $1, \dots, m$; and $u_i \in U(D)$.

Remark. Let's try to understand this claim by looking at an example: $x(x+1) = (2x+2)\left(\frac{x}{2}\right)$; here x, $\frac{x}{2}$, $x+1$, and $2x+2$ are irreducible in $\mathbb{Q}[x]$ and $\mathbb{Q}[x]$ is a PID.

We see that both sides have <u>two</u> irreducible factors, the irreducible factor corresponding to x is $\frac{x}{2}$ and the irreducible factor corresponding to $x+1$ is $2x+2$; and we have

$$\frac{1}{2}x = \underbrace{\left(\frac{1}{2}\right)}_{\text{in } \mathbb{Q}[x]^{\times}} x \quad \text{and}$$

$$2x+2 = \underbrace{(2)}_{\text{in } \mathbb{Q}[x]^{\times}} (x+1).$$

Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019 6:05 PM

Pf. We prove it by induction on m.

Base of induction. $m=1$. Then $q_1 = p_1 \cdots p_n$. Since q_1 is irreducible, $n \neq 0$ (that means $q_1 \neq 1$.).

$q_1 = p_1 (p_2 \cdots p_n) \Rightarrow$ either $p_1 \in D^\times$ or $(p_2 \cdots p_n) \in D^\times$

As p_1 is irred. in D, $p_1 \notin D^\times$. Therefore $p_2 \cdots p_n \in D^\times$

$\Rightarrow (\exists u \in D \text{ s.t. } u \cdot p_2 \cdots p_n = 1)$ or $n=1$.

$$\left.\begin{array}{l} \Rightarrow \text{ either } 1 \in \langle p_2 \rangle \text{ or } n=1 \\ p_2 \text{ is irred implies } 1 \notin \langle p_2 \rangle \end{array}\right\} \Rightarrow n=1$$

$\Rightarrow q_1 = p_1$.

The induction step.

$q_1 q_2 \cdots q_{m+1} = p_1 \cdot p_2 \cdots p_n \Rightarrow q_{m+1} \mid p_1 \cdot p_2 \cdots p_n$.

q_{m+1} irred. in $D \Rightarrow q_{m+1}$ prime in D

$q_{m+1} \mid (p_1 \cdots p_{n-1}) p_n \Rightarrow q_{m+1} \mid p_1 \cdots p_{n-1}$ or $q_{m+1} \mid p_n$

$\xRightarrow[\text{this argument}]{\text{repeating}}$ $q_{m+1} \mid p_1$ or $q_{m+1} \mid p_2$ or $\cdots$ or $q_{m+1} \mid p_n$.

Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019 6:17 PM

$$\Rightarrow \exists\, i_{m+1} \text{ s.t. } q_{m+1} \mid p_{i_{m+1}}.$$

$$\left.\begin{array}{l} \Rightarrow \langle p_{i_{m+1}} \rangle \subseteq \langle q_{m+1} \rangle \\ p_{i_{m+1}} : \text{irred.} \Rightarrow \langle p_{i_{m+1}} \rangle \text{ maximal ideal} \\ q_{m+1} : \text{irred.} \Rightarrow \langle q_{m+1} \rangle \neq D \end{array}\right\} \Rightarrow \langle p_{i_{m+1}} \rangle = \langle q_{m+1} \rangle$$

$$\Rightarrow \exists\, u_{m+1} \in D^{\times},\ q_{m+1} = u_{m+1}\, p_{i_{m+1}}.$$

Therefore $\quad q_1 q_2 \cdots q_m \cdot u_{m+1} \cdot p_{i_{m+1}} = p_1 p_2 \cdots p_n.$

By the cancellation law we get

$$q_1 q_2 \cdots q_m = (u_{m+1}^{-1}\, p_1) \cdot p_2 \cdots p_{i_{m+1}-1} \cdot p_{i_{m+1}+1} \cdots p_n.$$

Since p_1 is irreducible in D and $u_{m+1}^{-1} \in D^{\times}$, $\langle p_1 \rangle = \langle u_{m+1}^{-1} p_1 \rangle$ is a maximal ideal of D; and so

$$u_{m+1}^{-1}\, p_1 \text{ is irreducible in } D.$$

Now by the induction hypothesis, $m = n-1$; and there are $i_1, \ldots, i_m$ (a reordering of $\{1, \ldots, n\} \setminus \{i_{m+1}\}$) and $u_1', u_2, \ldots, u_m \in D^{\times}$ such that

Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019 6:23 PM

$$q_{r_1} = u_1' (u_{m+1}^{-1} p_{i_1}), \quad q_{r_2} = u_2 p_{i_2}, \ldots, q_{r_m} = u_m p_{i_m}.$$

Notice that, since $D^\times$ is a group and $u_1', u_{m+1} \in D^\times$

$u_1' u_{m+1}^{-1} \in D^\times$. Let $u_1 = u_1' u_{m+1}'$. So $q_{r_j} = u_j p_{i_j}$

for $1 \leq j \leq m+1$; and the claim follows. ∎