Lecture 17: Principal ideals

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 \( \langle d \rangle \neq \emptyset, d^2, d^3, 1, d, d^2, \ldots \). Next we will see the connection between properties of \( d \) and \( \langle d \rangle \).

1. \( \langle d \rangle = D \iff d \in D^\times \)

   \[\text{Proof.} \quad (\implies) \quad \langle d \rangle = D \implies 1 \in \langle d \rangle \]

   \[\quad \implies \exists c \in D, \quad 1 = d \cdot c \]

   \[\quad \implies d \in D^\times \]

   \[\quad (\iff) \quad d \in D^\times \implies \exists c \in D, \quad 1 = d \cdot c \]

   \[\quad \implies \forall d' \in D, \quad d' = d(c \cdot d') \in \langle d \rangle \]

   \[\quad \implies D \subseteq \langle d \rangle \]

   \[\quad \implies D = \langle d \rangle . \]

2. \( b \mid a \iff a \in \langle b \rangle \iff \langle a \rangle \subseteq \langle b \rangle . \)
Lecture 17: Principal ideals

\[ a \mid b \Rightarrow \exists c \in D, \ b = ac \Rightarrow be\langle a \rangle \]

\[ be\langle a \rangle \Rightarrow \exists c \in D, \ b = ac \]

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

\[ \langle b \rangle \subseteq \langle a \rangle. \]

\[ \langle b \rangle \subseteq \langle a \rangle \Rightarrow b \cdot 1 \in \langle b \rangle \subseteq \langle a \rangle \]

\[ \Rightarrow b = ad \text{ for some } d \in D \]

\[ \Rightarrow a \mid b. \]

\[ \langle a \rangle = \langle b \rangle \iff \exists u \in D^*, \ a = bu. \]

\[ (\Rightarrow): \text{if } a = 0, \text{ then } \langle a \rangle = 0 \text{; and so } \langle b \rangle = 0. \]

\[ \text{Therefore } b = 0. \Rightarrow a = b = 0. \]

\[ \text{Suppose } a \neq 0. \quad \langle a \rangle = \langle b \rangle \Rightarrow \exists a = bc \text{ for some } c \in D \]

\[ b = ad \text{ for some } d \in D \]

\[ \Rightarrow a = bc = adc \Rightarrow a(1 - dc) = 0 \Rightarrow 1 - dc = 0 \]

\[ a \neq 0 \text{ no zero-divisor} \]

\[ \Rightarrow 1 = dc \Rightarrow ceD^* \text{ (and } a = bc). \]
Lecture 17: Principal ideals

Sunday, March 17, 2019 5:28 PM

\[(\Leftarrow) \quad a = bu \Rightarrow b \mid a \Rightarrow \langle a \rangle \subseteq \langle b \rangle\]

\[\begin{align*}
  & a = bu \Rightarrow b = au^{-1} \Rightarrow a \mid b \Rightarrow \langle b \rangle \subseteq \langle a \rangle \\
  & \text{if } u \in D^x \\
  & \therefore \langle a \rangle = \langle b \rangle
\end{align*}\]

\[\Rightarrow\]

Recall. Suppose \( D \) is a PID. Then \( d \) is irreducible in \( D \) \( \iff \) \( \langle d \rangle \) is a maximal ideal.

Def. Suppose \( D \) is an integral domain; \( p \in D \setminus (D^x \cup \{0\}) \)

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 \( D \) \( \iff \) \( \langle d \rangle \) is a prime ideal in \( D \).

\[\text{Pf. (} \Leftarrow \text{). } d \text{ is prime in } D \Rightarrow d \notin D^x \Rightarrow \langle d \rangle \neq D.\]

\[\Rightarrow ab \in \langle d \rangle \Rightarrow d \mid ab \Rightarrow d \mid a \text{ or } d \mid b\]

\[\Rightarrow ae \in \langle d \rangle \text{ or } be \in \langle d \rangle.\]

\[\text{Pf. (} \Rightarrow \text{). } \langle d \rangle \text{ is a prime ideal } \Rightarrow \langle d \rangle \neq D \Rightarrow d \notin D^x.\]
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 \text{ or } b \in \langle d \rangle

\Rightarrow d \mid a \text{ or } d \mid b.

(And by assumption \( d \neq 0 \).) \( \square \)

Summary. Suppose \( D \) is an integral domain.

\begin{enumerate}
  \item \( \langle d \rangle = D \iff d \in D^* \).
  \item \( d \mid d' \iff d' \in \langle d \rangle \iff \langle d' \rangle \subseteq \langle d \rangle \).
\end{enumerate}

Suppose \( D \) is a PID.

\begin{enumerate}
  \item \( \langle d \rangle \) is a maximal ideal \( \iff d \) is irreducible in \( D \).
  \item \( d \neq 0 \) and \( \langle d \rangle \) is a prime ideal \( \iff d \) is prime in \( D \).
\end{enumerate}

In particular, in a PID, irreducible \( \Rightarrow \) prime.

Next we show its converse.

Proposition. Suppose \( D \) is a PID. Then

\[ d \in D \text{ is irreducible in } D \iff d \text{ is prime in } D. \]

\[ \text{Proof. (\( \Leftarrow \)) } d \in D \text{ irreducible } \Rightarrow d \neq 0 \text{ and } d \notin D^* \text{ and } \langle d \rangle \text{ is maximal} \]
\( \Rightarrow d \neq 0 \) and \( <d> \) is prime \( \Rightarrow d \) is prime.

\( \Leftarrow \). \( d \) is prime \( \Rightarrow d \neq 0 \) and \( d \notin D^x \).

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 \( c \in D \).

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

\( \Rightarrow a \left(1 - bc\right) = 0. \)

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

\( 1 - bc = 0 \Rightarrow bc = 1 \Rightarrow b \in D^x. \)

And so \( d = ab \Rightarrow b \in D^x \) or \( a \in D^x \), which implies \( d \) is irreducible in \( D \).

Next we show the uniqueness part of being a UFD for a PID.
Theorem. Suppose $D$ is a PID, $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible in $D$, and $p_1 \cdots p_n = q_1 \cdots q_m$. Then (1) $m = n$

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

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 two 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 $\frac{1}{2}x = \left(\frac{1}{2}\right)x$ and $\overset{\sim}{2x+2} = (2)\left(x+1\right)$

in $\mathbb{Q}[x]^\times$. 
Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019 6:05 PM

Proof. We prove it by induction on \( m \).

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

\[ q_1 = (p_1 \ldots p_n) \Rightarrow \text{either } p_1 \in D^x \text{ or } (p_1 \ldots p_n) \in D^x \]

As \( p_1 \) is irreducible in \( D \), \( p_1 \notin D^x \). Therefore \( p_2 \ldots p_n \in D^x \)

\[ \Rightarrow (\exists u \in D \text{ s.t. } u(p_2 \ldots p_n) = 1) \text{ or } n=1 \]

\[ \Rightarrow \text{either } 1 \notin \langle p_2 \rangle \text{ or } n=1 \Rightarrow n=1 \]

\[ p_2 \text{ is irreducible implies } 1 \notin \langle p_2 \rangle \]

\[ \Rightarrow q_1 = p_1. \]

The induction step.

\[ q_1 q_2 \ldots q_{m+1} = p_1 p_2 \ldots p_n \Rightarrow q_{m+1} \mid p_1 p_2 \ldots p_n. \]

\( q_{m+1} \) irreducible in \( D \) \( \Rightarrow q_{m+1} \) prime in \( D \)

\[ q_{m+1} \mid (p_1 \ldots p_{n-1}) p_n \Rightarrow q_{m+1} \mid p_1 \ldots p_{n-1} \text{ or } q_{m+1} \mid p_n \]

repeating

this argument

\[ q_{m+1} \mid p_1 \text{ or } q_{m+1} \mid p_2 \text{ or } \ldots \text{ or } q_{m+1} \mid p_n. \]
Lecture 17: Uniqueness part of being a UFD

Sunday, March 17, 2019  6:17 PM

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

\[ \Rightarrow \langle p_{i_{m+1}} \rangle \subseteq \langle q_{i_{m+1}} \rangle \]

\[ p_{i_{m+1}} : \text{irred. } \Rightarrow \langle p_{i_{m+1}} \rangle \text{ maximal ideal} \]

\[ q_{i_{m+1}} : \text{irred. } \Rightarrow \langle q_{i_{m+1}} \rangle \neq D \]

\[ \Rightarrow \exists u_{m+1} \in D^x, \ q_{i_{m+1}} = u_{m+1} \cdot p_{i_{m+1}}. \]

Therefore

\[ q_1 q_2 \cdots q_m u_{m+1} \cdot p_{i_{m+1}} = p_1 p_2 \cdots p_n. \]

By the cancellation law we get

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

Since \( p_1 \) is irreducible in \( D \) and \( u_{m+1}^{-1} \in D^x, \langle q_1 \rangle = \langle u_{m+1}^{-1} p_1 \rangle \) 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 \( i_1, \ldots, i_{m+1}, i_{m+2} \)) and \( u'_1, u'_2, \ldots, u'_m \in D^x \) such that

math103b-19-w Page 8
\[ q_1 = u_1' \left( u_{m+1}^{-1} p_{i_1} \right), \quad q_2 = u_2' p_{i_2}, \ldots, \quad q_m = u_m' p_{i_m}. \]

Notice that, since \( D^x \) is a group and \( u_1', u_{m+1} \in D^x \), \( u_1' u_{m+1}^{-1} \in D^x \). Let \( u_1 = u_1' u_{m+1} \). So \( q_j = u_j' p_{i_j} \) for \( 1 \leq j \leq m+1 \), and the claim follows. \( \square \)