Principal Ideal Domains

P.I.D.

Definition A ring R is a principal ideal domain if

1/ R is an integral domain

2/ Every ideal of R is principal

$I \subset R$ ideal $\Rightarrow I = (a)$ for some $a \in I$

Proposition R Euclidean domain $\Rightarrow$ R a P.I.D.

R Euclidean domain $\Rightarrow$ R an integral domain

Let φ be a Euclidean function on R, $I \subset R$ an ideal.

$I = \{0_R\} \Rightarrow I = (0_R)$

$\varphi(m) \leq \varphi(n)$
$\forall n \in I \setminus \{0_R\}$

Assume $I \neq \{0_R\}$.

Choose $m \in I \setminus \{0_R\}$ such that $\varphi(m)$ is minimal.

Claim $I = (m)$.

$m \in I \Rightarrow (m) \subset I$

Assume $I \neq (m) \Rightarrow \exists\, b \in I \setminus \{0_R\}$ such that $m \nmid b$.

$\Rightarrow \exists\, q, r \in R$ such that $b = qm + r$, $r \neq 0_R$ and

$\varphi(r) < \varphi(m)$.

$b, m \in I \Rightarrow r = b - qm \in I$. Contradiction by minimality of $\varphi(m)$. Hence $I = (m)$ $\square$

field

Examples $\mathbb{Z}$, $F[x]$ are P.I.D.s

Definition Let R be an integral domain, $I_1, I_2, \ldots$ a nested sequence of ideals :

Ascending Chain of ideals

$$I_1 \subset I_2 \subset I_3 \cdots$$

We stay $\{I_i\}$ is **stationary** if $\exists\, N \in \mathbb{N}$ such that $I_n = I_N \;\; \forall\, n \geq N$.

A commutative ring satisfying this is called Noetherian

Theorem R a P.I.D $\Rightarrow$ Every ascending chain of ideals is stationary

Proof (Outline)

Ascending chain of ideals

$$I_1 \subset I_2 \subset I_3 \ldots \Rightarrow \bigcup_{i=1}^{\infty} I_i \text{ an ideal in } R$$

must be nested

R a P.I.D. $\Rightarrow \exists\, m \in \bigcup_{i=1}^{\infty} I_i$ such that $(m) = \bigcup_{i=1}^{\infty} I_i$

$\Rightarrow \exists\, N \in \mathbb{N}$ such that $m \in I_N$

$\Rightarrow (m) \subset I_N \subset \bigcup_{i=1}^{\infty} I_i \subset (m) \Rightarrow I_n = I_N \;\forall\, n \geq N$

$\square$

Theorem R a P.I.D. $\Rightarrow$ Every $a \neq 0_R$, $a \notin R^*$ admits an irreducible factorization

Proof

Crucial Observations: $(a) \subsetneq (b) \Leftrightarrow b \mid a$ and $a \nmid b$

$(a) = (b) \Leftrightarrow a = bu,\; u \in R^*$

Let $a \neq 0_R$ and $a \notin R^*$.

<u>Step 1</u> : Show a has an irreducible factor. $\overset{R^*}{\notin}$ $\notin R^*$

If a irreducible done. If not $a = b_1 a_1$

$$\Rightarrow \quad (a) \subsetneq (a_1)$$

$\overset{R^*}{\notin}$ $\notin R^*$

If a_1 irreducible done. If not $a_1 = b_2 a_2$

$$\Rightarrow \quad (a) \subsetneq (a_1) \subsetneq (a_2)$$

If a_2 irreducible done. If not repeat.

This process must terminate with an irreducible factor as every ascending chain of ideals is stationary.

<u>Step 2</u> Show a admits an irreducible factorization.

irreducible $\notin R^*$

If a irreducible done. If not $a = p_1 c_1$

$$\Rightarrow \quad (a) \subsetneq (c_1)$$

irreducible $\notin R^*$

If c_1 irreducible done. If not $c_1 = p_2 c_2$

$$\Rightarrow \quad (a) \subsetneq (c_1) \subsetneq (c_2)$$

Again this process must terminate with an irreducible c_n

$\Rightarrow \quad a = p_1 p_2 \cdots p_n c_n$ an irreducible factorization. $\square$

<u>Definition</u> Let R be an integral domain. We say $p \in R$ is prime if

1/ $p \neq 0_R$

2/ $p \notin R^*$

3/ $p \mid ab \Rightarrow p \mid a$ or $p \mid b \quad \forall a, b \in R$

Example

Euclid's Lemma

$p \in \mathbb{Z}$ irreducible $\Rightarrow$ $p \in \mathbb{Z}$ prime ← new definition

Remark $p \in R$ prime $\Leftrightarrow$ $p \neq 0_R$ and $(p) \subset R$ a prime ideal

Proposition p prime $\Rightarrow$ p irreducible.

Proof

Assume p reducible $\Rightarrow$ $p = ab$, $a, b \notin R^*$

$b \notin R^* \Rightarrow p \nmid a$

$a \notin R^* \Rightarrow p \nmid b$

However $p \mid ab$. $\Rightarrow$ p not prime. $\square$

Theorem If R is a P.I.D.

$p \in R$ irreducible $\Leftrightarrow$ $p \in R$ prime

Proof

Assume $p \in R$ irreducible $\Rightarrow$ $p \neq 0_R$ and $p \notin R^*$

Claim (p) is maximal. ← R must be a P.I.D.

$p \notin R^* \Rightarrow (p) \subset R$ is a proper ideal.

Assume $J \subset R$ is an ideal $(p) \subset J \subset R$.

R a P.I.D. $\Rightarrow$ $J = (m)$ for some $m \in J$

$(p) \subset (m) \Rightarrow p = cm \Rightarrow c \in R^*$ or $m \in R^*$

$$\left.\begin{array}{lll} c \in R^* & \Rightarrow & (p) = (m) \\ m \in R^* & \Rightarrow & (m) = R \end{array}\right\} \Rightarrow (p) \subset R \text{ maximal}$$

$(p) \subset R$ maximal $\Rightarrow$ $R/(p)$ field $\Rightarrow$ $R/(p)$ integral domain

$\Rightarrow$ $(p) \subset R$ prime ideal

$p \neq 0_R$ $\Rightarrow$ $p \in R$ prime $\square$

<u>Theorem</u> Let R be a ring. If

1/ R an integral domain

2/ Every $a \neq 0_R$, $a \notin R^*$ admits an irreducible factorization

3/ $p \in R$ irreducible $\Leftrightarrow$ $p \in R$ prime

then R is a UFD

actually equivalent to being a UFD

<u>Proof</u>

We need to prove that $3/ \Rightarrow$ uniqueness of irreducible factorizations.

Let $c = a_1 \dots a_n = b_1 \dots b_m$

irreducible factorizations of c

WLOG assume $n \leq m$

a_1 irreducible $\Rightarrow$ a_1 prime.

$a_1 \mid b_1 \dots b_m \Rightarrow a_1 \mid b_1$ after reordering

$a_1 = b_1 c_1$. a_1 irreducible, $b_1 \notin R^* \Rightarrow c_1 \in R^*$

$\Rightarrow$ a_1 and b_1 are associated

C.L.

$\Rightarrow$ $c_1 a_2 \dots a_n = b_2 \dots b_m$

Repeat with a_2 and b_2. ← after reorder

Repeat until we have

If $n < m$ we would eventually have

$$\underbrace{c_1 \cdots c_n}_{\in R^*} = b_{n+1} \cdots b_m \Rightarrow b_{n+1} \in R^*$$

Contradiction. Hence $n = m$ and, after reordering, a_i associated to b_i for all $i \in \{1, \ldots n\}$

$\square$

<u>Theorem</u> R a P.I.D. $\Rightarrow$ R a U.F.D.

<u>Proof</u>

1/ R a P.I.D. $\Rightarrow$ R integral domain

2/ R a P.I.D. $\Rightarrow$ $a \neq 0_R$, $a \notin R^*$ admits an irreducible factorization

3/ R a P.I.D. $\Rightarrow$ $p \in R$ irreducible $\Leftrightarrow$ $p \in R$ prime

$\square$

<u>Theorem</u> R a Euclidean domain $\Rightarrow$ R a UFD.

<u>Proof</u>

R a Euclidean domain $\Rightarrow$ R a P.I.D. $\Rightarrow$ R a U.F.D.

$\square$