# 20250123 MATH4302 NOTE 1[1]

**Author:** Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
**Email:** u3612704@connect.hku.hk;
**Phone:** +852 5693 2134; +86 19921823546;

# Contents

# 1 Introduction

This note aims to prove the following relation:

**Euclidean Domain $\subseteq$ Principal Ideal Domain $\subsetneq$ Unique Factorization Domain**

Actually we may prove the following as well:

**Euclidean Domain $\not\supseteq$ Principal Ideal Domain**

However, the proof is not simple, so we don't include it here. We list the definitions of nonzero commutative ring with unity, integral domain and field.

**Definition 1.1.** (**Nonzero Commutative Ring with Unity**)
Let $R$ be a set with two operations $(r, s) \mapsto r + s, (r, s) \mapsto rs$. If:
(1) $\forall r, s \in R, r + s = s + r$.
(2) $\forall r, s, t \in R, (r + s) + t = r + (s + t)$.
(3) $\exists 0 \neq 1, \forall r \in R, 0 + r = r$.
(4) $\forall r \in R, \exists s \in R, s + r = 0$.
(5) $\forall r, s \in R, rs = sr$.
(6) $\forall r, s, t \in R, (rs)t = r(st)$.
(7) $\exists 1 \neq 0, \forall r \in R, 1r = r$.
(8) $\forall \lambda \in R, \forall r, s \in R, \lambda(r + s) = \lambda r + \lambda s$.
Then $R$ is a nonzero commutative ring with unity.

**Definition 1.2.** (**Zero Divisor and Integral Domain**)
Let $R$ be a nonzero commutative ring with unity.
If $r \neq 0$ and $\exists s \neq 0, rs = 0$, then $r$ is a zero divisor.
If every $r \neq 0$ is not a zero divisor, then $R$ is an integral domain.

**Definition 1.3.** (**Unit and Field**)
Let $R$ be a nonzero commutative ring with unity.
If $r \neq 0$ and $\exists s \neq 0, rs = 1$, then $r$ is a unit.
If every $r \neq 0$ is a unit, then $R$ is a field.

# 2 Principal Ideal Domain

**Definition 2.1.** (**Maximal Ideal**)
Let $R$ be a nonzero commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of $R$.
If there is no ideal strictly between $\mathfrak{p}$ and $R$, then $\mathfrak{p}$ is maximal.

**Proposition 2.2.** $\mathfrak{p}$ is maximal iff $R/\mathfrak{p}$ is a field.

*Proof.* We may divide our proof into two parts.
**"if" direction:** Assume that $R/\mathfrak{p}$ is a field.
As $R/\mathfrak{p}$ is a nonzero commutative ring with unity, $\mathfrak{p}$ is proper.
As $\forall a \notin \mathfrak{p}$, $xa \equiv 1 (\text{mod } \mathfrak{p})$ has a solution, $\langle a \rangle + \mathfrak{p} = R$, so $\mathfrak{p}$ is maximal.
**"only if" direction:** Assume that $\mathfrak{p}$ is maximal.
As $\mathfrak{p}$ is proper, $R/\mathfrak{p}$ is a nonzero commutative ring with unity.
As $\forall a \notin \mathfrak{p}, \langle a \rangle + \mathfrak{p} = R$, $xa \equiv 1 (\text{mod } \mathfrak{p})$ has a solution, so $R/\mathfrak{p}$ is a field.
Quod. Erat. Demonstrandum. $\square$

**Definition 2.3.** (**Prime Ideal**)
Let $R$ be a nonzero commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of $R$.
If $\mathfrak{p}^c$ is closed under multiplication, then $\mathfrak{p}$ is prime.

**Proposition 2.4.** $\mathfrak{p}$ is prime iff $R/\mathfrak{p}$ is an integral domain.

*Proof.* We may divide our proof into two parts.
**"if" direction:** Assume that $R/\mathfrak{p}$ is an integral domain.
As $R/\mathfrak{p}$ is a nonzero commutative ring with unity, $\mathfrak{p}$ is proper.
As $\forall a, b \notin \mathfrak{p}, ab \not\equiv 0 (\text{mod } \mathfrak{p})$, $ab \notin \mathfrak{p}$, so $\mathfrak{p}$ is prime.
**"only if" direction:** Assume that $\mathfrak{p}$ is prime.
As $\mathfrak{p}$ is proper, $R/\mathfrak{p}$ is a nonzero commutative ring with unity.
As $\forall a, b \notin \mathfrak{p}, ab \notin \mathfrak{p}$, $ab \not\equiv 0 (\text{mod } \mathfrak{p})$, so $R/\mathfrak{p}$ is an integral domain.
Quod. Erat. Demonstrandum. $\square$

**Example 2.5.** As **Field** $\subseteq$ **Integral Domain**, **Maximal Ideal** $\subseteq$ **Prime Ideal**.

**Proposition 2.6.** $a$ is a unit in $R$ iff $1 \in \langle a, t \rangle$ in $R[\![t]\!]$.

*Proof.* We may divide our proof into two parts.
**"if" direction:** Assume that $1 \in \langle a, t \rangle$, i.e., $\exists x(t), y(t) \in R[\![t]\!], ax(t) + ty(t) = 1$.
The constant term projection is $\exists x_0 \in R, ax_0 = 1$, where $a, x_0 \neq 0$, so $a$ is a unit.
**"only if" direction:** Assume that $a$ is a unit, i.e., $\exists x_0 \in R, ax_0 = 1$.
Embed this into $R[\![t]\!]$, $\exists x_0, 0 \in R[\![t]\!], 1 = ax_0$, so $1 \in \langle a, t \rangle$.
Quod. Erat. Demonstrandum. $\square$

**Proposition 2.7.** $R$ is an integral domain iff $\langle t \rangle$ is prime in $R[\![t]\!]$.

*Proof.* We may divide our proof into two parts.
**"if" direction:** Assume that $\langle t \rangle$ is prime in $R[\![t]\!]$, i.e., $\forall a(t), b(t) \notin \langle t \rangle, a(t)b(t) \notin \langle t \rangle$.

The constant term projection is $\forall a_0, b_0 \neq 0, a_0 b_0 \neq 0$, so $R$ is an integral domain.
**"only if" direction:** Assume that $R$ is an integral domain, i.e., $\forall a_0, b_0 \neq 0, a_0 b_0 \neq 0$.
Embed this into $R[\![t]\!]$, $\forall a(t), b(t) \notin \langle t \rangle, a(t)b(t) \notin \langle t \rangle$, so $R$ is an integral domain.
Quod. Erat. Demonstrandum. $\square$

**Example 2.8.** In $\mathbb{Z}[t]$, **Maximal Ideal $\not\supseteq$ Prime Ideal**, as:
(1) $\langle t \rangle \subsetneq \langle 2, t \rangle \subsetneq \mathbb{Z}[t]$, so $\langle t \rangle$ is not maximal.
(2) $\mathbb{Z}$ is an integral domain, so $\langle t \rangle$ is prime.

**Definition 2.9.** (**Prime Element**)
Let $R$ be a nonzero commutative ring with unity, and $p$ be a nonzero nonunit element of $R$. If $\langle p \rangle$ is prime, then $p$ is prime.

**Definition 2.10.** (**Irreducible Element**)
Let $R$ be a nonzero commutative ring with unity, and $p$ be a nonzero nonunit element of $R$. If $p$ is not a product of nonunit elements, then $p$ is irreducible.

**Proposition 2.11.** In integral domain, **Prime Element $\subseteq$ Irreducible Element**.

*Proof.* For all prime element $p \in R$, assume that $p = ab$, where $a, b \in R$.
As $p|ab$, $p|a$ or $p|b$, so we may assume WLOG that $p|a$ with quotient $c$.
As $R$ is an integral domain, $bc = 1$, so this nonzero nonunit element $p$ is irreducible.
Quod. Erat. Demonstrandum. $\square$

**Example 2.12.** In $\mathbb{Z}_6$, **Prime Element $\not\subseteq$ Irreducible Element**, as:
(1) $\langle 2 \rangle^c = \mathbb{Z}_6^\times$ is closed under multiplication, so 2 is prime.
(2) $2 = 2 \cdot 4$, where $2, 4$ are nonunit, so 2 is reducible.

**Example 2.13.** In $\mathbb{Z}[\sqrt{-3}]$, **Prime Element $\not\supseteq$ Irreducible Element**, as:
(1) $\frac{1 \pm \sqrt{-3}}{2} \notin \mathbb{Z}[\sqrt{-3}]$ and $\frac{(1+\sqrt{-3})(1-\sqrt{-3})}{2} \in \mathbb{Z}[\sqrt{-3}]$, so 2 is not prime.
(2) $\overline{B}(0,2) \cap \mathbb{Z}[\sqrt{-3}] = \pm\{0, 1, \sqrt{-3}, 1+\sqrt{-3}, 1-\sqrt{-3}, 2\}$, so 2 is irreducible.

**Definition 2.14.** (**Principal Ideal and Principal Ideal Ring**)
Let $R$ be a nonzero commutative ring with unity.
If an ideal $\mathfrak{a}$ is generated by some element $a$, then $\mathfrak{a}$ is principal.
If every ideal $\mathfrak{a}$ is principal, then $R$ is a principal ideal ring.

**Proposition 2.15.** In principal ideal ring, every irreducible element $p$ generates a maximal ideal $\mathfrak{p} = \langle p \rangle$.

*Proof.* For all ideal $\mathfrak{a} = \langle a \rangle$, assume that $\mathfrak{a} \supseteq \mathfrak{p}$.
As $a|p$, for some $b \in R$, $p = ab$.
As $p$ is irreducible, $a$ is a unit, $\mathfrak{a} = R$, or $b$ is a unit, $\mathfrak{a} = \mathfrak{p}$.
Hence, this proper ideal $\mathfrak{p}$ is maximal. Quod. Erat. Demonstrandum. □

**Example 2.16.** In $\mathbb{Z}[t]$, an irreducible element does not necessarily generate a maximal ideal, for the same reason given in **Example 2.8.**.

**Example 2.17.** In $\mathbb{Z}[t]$, a maximal ideal is not necessarily generated by an irreducible element, as:
(1) $\langle 2 \rangle$ is maximal in $\mathbb{Z}$, so $\langle 2, t \rangle$ is maximal in $\mathbb{Z}[t]$.
(2) $\forall a(t) \in \mathbb{Z}[t], a(t)|2 \implies a(t) \in \pm\{1, 2\}$, so $\langle 2, t \rangle$ is not principal.

**Definition 2.18.** (**Principal Ideal Domain**)
Let $R$ be an integral domain.
If $R$ is a principal ideal ring, then $R$ is a principal ideal domain.

**Example 2.19.** In principal ideal domain, the followings are equivalent:
(1) $\mathfrak{p}$ is a nonzero maximal ideal.
(2) $\mathfrak{p}$ is a nonzero prime ideal.
(3) $\mathfrak{p}$ is generated by a prime element $p$.
(4) $\mathfrak{p}$ is generated by an irreducible element $p$.

**Proposition 2.20.** In principal ideal ring, for all ascending chain of ideals:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

The chain stops increasing after some $\mathfrak{a}_m$:

$$\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$$

*Proof.* Define the following subset of $R$:

$$\mathfrak{a} = \bigcup_{n=1}^{+\infty} \mathfrak{a}_n$$

(1) $0 \in \mathfrak{a}_1, 0 \in \mathfrak{a}$.
(2) $\forall a_s \in \mathfrak{a}_s \subseteq \mathfrak{a}_{\mathrm{Max}\{s,t\}}, \forall a_t \in \mathfrak{a}_t \subseteq \mathfrak{a}_{\mathrm{Max}\{s,t\}}, a_s + a_t \in \mathfrak{a}_{\mathrm{Max}\{s,t\}} \subseteq \mathfrak{a}$.
(3) $\forall a_s \in \mathfrak{a}_s, -a_s \in \mathfrak{a}_s \subseteq \mathfrak{a}$.
(4) $\forall \lambda \in R, \forall a_s \in \mathfrak{a}_s, \lambda a_s \in \mathfrak{a}_s \subseteq \mathfrak{a}$.
As $R$ is a principal ideal ring, $\mathfrak{a}$ has a generator $a$.

This $a$ belongs to some $\mathfrak{a}_m$, so the chain stop increasing after this $\mathfrak{a}_m$.
Quod. Erat. Demonstrandum. $\square$

**Example 2.21.** In $\mathbb{R}^{\mathbb{N}}$, there exists a strictly increasing chain of ideals:

$$\langle \mathbf{e}_1 \rangle \subsetneq \langle \mathbf{e}_1, \mathbf{e}_2 \rangle \subsetneq \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle \subsetneq \cdots$$

# 3 Unique Factorization Domain, Euclidean Domain

**Definition 3.1.** (**Factorization Tree and Factorization Domain**)
Let $R$ be an integral domain. If a binary tree $T$ satisfies the following properties:
(1) When a node $a$ is reducible, then $a = a_1 a_2$, where $a_1, a_2$ are children of $a$.
(2) When a node $a$ is irreducible, then $a$ has no child.
Then $T$ is a factorization tree.
If every factorization tree is finite, then $R$ is a factorization domain.

**Proposition 3.2.** Let $R$ be an integral domain.
$R$ is a factorization domain iff for all ascending chain of principal ideals:

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$$

The chain stops increasing after some $\langle a_m \rangle$:

$$\langle a_m \rangle = \langle a_{m+1} \rangle = \langle a_{m+2} \rangle = \cdots$$

*Proof.* It suffices to notice that a binary tree is finite iff every chain is finite.
Quod. Erat. Demonstrandum. $\square$

**Definition 3.3.** (**Unique Factorization Domain**)
Let $R$ be a factorization domain. If for all associated irreducible factorizations:

$$p_1 p_2 \cdots p_m \sim q_1 q_2 \cdots q_n$$

We have $m = n$, and for some $\sigma \in S_n$, $(p_1, p_2, \cdots, p_m) \sim \sigma * (q_1, q_2, \cdots, q_n)$, then $R$ is a unique factorization domain.

**Proposition 3.4.** Let $R$ be a factorization domain.
$R$ is a unique factorization domain iff every irreducible element is prime.

*Proof.* We may divide our proof into two parts.
**"if" direction:** Assume that every irreducible element is prime.

For all associated irreducible factorization:

$$p_1p_2\cdots p_m \sim q_1q_2\cdots q_n$$

(1) As $p_1$ is prime and $q_{\sigma(1)}$ is irreducible, $p_1, q_{\sigma(1)}$ are associated.
As $R$ is an integral domain, we may cancel $p_1, q_{\sigma(1)}$ and repeat the argument.
(2) According to well-ordering principle, this cancellation program terminates.
We end up with $m = n$, and for some $\sigma \in S_n$, $(p_1, p_2, \cdots, p_m) \sim \sigma * (q_1, q_2, \cdots, q_n)$.
**"only if" direction:** Assume that $R$ is a unique factorization domain.
For all irreducible element $p$, for all elements $a, b$, take the irreducible factorizations:

$$a = a_1a_2\cdots a_m \text{ and } b = b_1b_2\cdots b_n$$

As $R$ is a unique factorization domain:

$$p|ab \implies p|a_1a_2\cdots a_mb_1b_2\cdots b_n \implies p|\text{some } a_k \text{ or } p|\text{some } b_l \implies p|a \text{ or } p|b$$

Hence, $p$ is prime. Quod. Erat. Demonstrandum. □

**Example 3.5. Principal Ideal Domain $\subseteq$ Unique Factorization Domain**, as:
(1) In principal ideal domain, the ascending chain criterion for ideals holds.
(2) In principal ideal domain, every irreducible element is prime.

**Example 3.6. Principal Ideal Domain $\not\supseteq$ Unique Factorization Domain**, as:
(1) $\langle 2, t\rangle$ is not principal, so $\mathbb{Z}[t]$ is not a principal ideal domain.
(2) $\mathbb{Z}, \mathbb{Q}[t]$ are unique factorization domains, so does $\mathbb{Z}[t]$.

**Definition 3.7.** (**Euclidean Domain**)
Let $R$ be an integral domain.
If there is a monotone degeree function $\mathrm{Deg} : R \to \{-\infty, 0, 1, 2, \cdots\}$,
such that for all $a, b \in R$, with $b \neq 0$, for some $q, r \in R$:

$$a = qb + r \text{ and } \mathrm{Deg}(r) < \mathrm{Deg}(b)$$

**Proposition 3.8. Euclidean Domain $\subseteq$ Principal Ideal Domain**.

*Proof.* For all nonzero ideal $\mathfrak{b}$ of an Euclidean domain $R$,
there exists a nonzero element $b$ with smallest degree $\mathrm{Deg}(b) \geq 0$.
For all $a \in R$, $b$ must divide $a$, otherwise the remainder $r = a - qb \in \mathfrak{b}$,
having a smaller degree $\mathrm{Deg}(r) < \mathrm{Deg}(b)$, will contradict the definition of $b$.
This means $\mathfrak{b} = \langle b\rangle$ is principal, so $R$ is a principal ideal domain.
Quod. Erat. Demonstrandum. □

# References


[1] H. Ren, “Template for math notes,” 2021.