PIDs and UFDs, I: Two properties of PIDs

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday, Jan 20, 2025

Outline

In this file: §1.2.1-1.2.2.

1. Euclidean domains and PIDs;
2. Two properties of a PID;

§1.2.1: Euclidean domains and PIDs

Division Algorithm: Let R be an integral domain and let $f, g \in R[x]$.

- If the leading coefficient of g is a unit in R, then there exist unique $q, r \in R[x]$ with $\deg(r) < \deg(g)$ such that $f = qg + r$.

Proof. Exercise.

Example. Long divisions give

$$x^3 + 2x^2 - x + 5 = (x+2)(x^2+1) + (-2x+3),$$

$$x^2 + 3x - 1 = (\frac{1}{2}x + \frac{5}{4})(2x+1) - \frac{9}{4}.$$

$$\begin{array}{r} \frac{1}{2}x \\ 2x^2+1 \overline{)\ x^3+2x^2-x+5} \\ \underline{x^3+x} \\ 2x^2-2x+5 \end{array}$$

Euclidean domain

For UFD, replace v by the irreducible factor counter i

Definition. An Euclidean domain is a pair (D, v), where D is an integral domain, and $v : D\backslash\{0\} \to \mathbb{N}$ a map such that

1) $v(ab) \geq \max\{v(a), v(b)\}$ for all $a, b \in D\backslash\{0\}$;

2) for all $a \in D\backslash\{0\}$ and $b \in D$, there exist $q, r \in D$ such that $b = aq + r$, where either $r = 0$ or $r \neq 0$ and $v(r) < v(a)$.

Examples of Euclidean domains:

1. $\mathbb{Z}$: $\leftarrow v(n) = |n|$
2. $K[x]$ for any field K: $\leftarrow v(f) = \deg$.
3. $K[[x]]$ for any field K: $\leftarrow$

Principal Ideal Domains (PID).

Definition. An integral domain R is called a Principal Ideal Domain, or a PID, if every ideal I of R is principal, i.e. $I = aR$ for some $a \in R$.

Example: A field is a PID.

Lemma. Every Euclidean domain is a PID.

Proof. Tutorial.

Consequently,

1. $\mathbb{Z}$ is a PID;
2. $K[x]$ is a PID for any field K;
3. $K[[x]]$ is a PID for any field K.

$I \subset \mathbb{Z}$, let $n = \min\{|i| : i \in I\}$. Prove that $I = n\mathbb{Z}$

classify all ideals.

a local PID

We have

$$\textit{Fields} \subseteq \textit{Euclidean Domains} \subseteq \textit{PIDs} \subseteq \textit{UFDs}$$
$$\subseteq \textit{Integral Domains} \subseteq \textit{Commutative Rings with Identity}.$$

Exercise: The ring $R = \mathbb{Z}[x]$ is an integral domain but not a PID: the ideal $I = 2R + xR$ is not principal.

Why?

Suppose $I = aR$, with $a \in R$. Write $a = a_0 + a_1 x$ where $a_0 \in \mathbb{Z}$, $a_1 \in R$. Then $a_0 \in 2\mathbb{Z}$. If $a_0 \neq 0 \Rightarrow x \notin aR$ contradiction. So $a_0 = 0$. Then $2 \notin aR$, contradiction.

More examples of Euclidean domains and thus PIDs

1. The ring $\mathbb{Z}[\sqrt{-1}]$ of Gauss integers, defined as

$$\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} : \ m, n \in \mathbb{Z}\}$$

   is an integral domain with $v(m + n\sqrt{-1}) = m^2 + n^2$;

2. The subring $D = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}$ of $(\mathbb{R}, +, \cdot)$ is an Euclidean domain with $v(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Remark: You may read any book or online on the topic of rings quadratic integers, many of which are PIDs but not Euclidean domains.

(Complex roots of $x^2 + ax + b = 0$, where $a, b \in \mathbb{Z}$

§1.2.2: Two properties of PIDs

$a = u(u^{-1}a)$

Definition. Let R be an integral domain.

1. A non-unit $a \in R$ is said to be irreducible if whenever $a = bc$, either b or c is a unit.
2. A non-zero non-unit $a \in R$ is said to be prime if aR is a prime ideal, or, equivalently, if $b, c \in R$ and $a|bc$, then $a|b$ or $a|c$.

Counter ex: 2 in $\mathbb{Z}[\sqrt{6}]$

Lemma. Every prime element in an integral domain is irreducible.

Proof. Let $a \in R$ be prime, and assume that $a = bc$.

- One has $a|bc$, so $a|b$ or $a|c$.
- WOLG assume that $a|b$. Then $b = ax$ for some $x \in R$.
- Then $a = axc$ so $a(1 - xc) = 0$.
- Since R is an integral domain and $a \neq 0$, must have $1 = xc$, i.e., c is a unit.

Q.E.D.

First property of a PID

Proposition. If R is a PID and $p \in R$ is irreducible, then the ideal pR is maximal, so the quotient R/pR is a field.

Proof. Let R be a PID and let $p \in R$ be irreducible. Want to show that pR is maximal.

- Suppose that M is an ideal of R containing pR.
- Since R is a PID, $M = mR$ for some $m \in R$.
- Since $p \in pR \subset M$, $p = mx$ for some $x \in R$.
- Since p is irreducible, either m or x is a unit.
- If m is a unit, then $M = R$.
- If x is a unit, then $pR = mR = M$. Hence $M = R$ or pR.
- Thus pR is maximal, and R/pR is a field.

Q.E.D.

Another formulation of the first property.

Corollary: Let R be a principal ideal domain.

1. Prime elements in R are the same as irreducible elements;
2. A non-zero ideal I in R is prime if and only if it is maximal. ←

Proof. Direct consequence of previous Proposition and the definitions.

Definition. Let R be an integral domain. An irreducible element in $R[x]$ is called an irreducible polynomial over R.

$\Rightarrow F[x]$ is a PID

Theorem. If $f(x)$ is an irreducible polynomial over a field F, then $F[x]/\langle f(x)\rangle$ is a field containing F as a sub-field.

Proof. A direct consequence of the Proposition (first property of a PID).

Remarks: $F \hookrightarrow F[x]/\langle f(x)\rangle, \quad \lambda \mapsto \lambda + \langle f(x)\rangle$

- The Theorem is one of the most important ways of constructing a new field from an old one.
- The theorem raises the problem of classifying/understanding all irreducible polynomials over a field F. The problem is especially interesting if $F = \mathbb{Q}$ or if F is a finite field.

eg $F = \mathbb{Z}/p\mathbb{Z}$

$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$

An example of a non PID. $\{a+bi\sqrt{5} : a, b \in \mathbb{Z}\}$

Example. $\mathbb{Z}[\sqrt{-5}]$ is not a PID:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Thus $2|(1+\sqrt{-5})(1-\sqrt{-5})$.

- If $2|(1+\sqrt{-5})$, then $1+\sqrt{-5} = 2(a+b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$, so $2a = 1$, a cntradiction. Similarly, 2 does not divide $1-\sqrt{-5}$. Thus 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.
- Suppose $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}$. Then

$$4 = (a^2+5b^2)(c^2+5d^2),$$

这个5会让事情变容易

so either $a+b\sqrt{-5} = \pm 1$ or $c+d\sqrt{-5} = \pm 1$.

- Thus $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible.
- Conclusion: $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

A second property of PIDs.

Definition. An integral domain R is said to satisfy the ascending chain condition for ideals, or ACCI, if, for every increasing sequence

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots \tag{1}$$

of ideals in R, there exists $m \geq 1$ such that $I_n = I_m$ for all $n \geq 1$.

测度空间的上升序列之并不一定是测度空间，**原因在于无限运算**

Lemma. Every PID satisfies ACCI.

Proof. Let an increasing sequence of ideals be given as in (1).

- Consider $I = \cup_{n \geq 1} I_n$, which is an ideal of R.
- As R is a PID, there exists $a \in R$ such that $I = aR$.
- Since $a \in I$, there exists $m \geq 1$ such that $a \in I_m$.
- Then $I \subset I_m$ and thus $I = I_m$.
- It follows that $I_n = I_m$ for all $n \geq m$.

$I_m \subset I_n \subset I_m$

Q.E.D.