PIDs and UFDs, II: A PID is a UFD

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday Jan 20 2025

& Thursday Jan 23, 2025

In this file: §1.2.3-1.2.4.

1. Definition of a UFD and two characterizing properties of a UFD;
2. A PID is a UFD.

Recall definition:

A non-zero non-unit a in an integral domain R is said to be irreducible if whenever $a = bc$, either b or c is a unit.

Definition. A unique factorization domain (UFD), or factorial ring, is an integral domain R such that

1. every non-zero non-unit $a \in R$ can be written as

$$a = p_1 p_2 \cdots p_r,$$

   where each p_i, for $i = 1, 2, \ldots, r$, is irreducible (but not necessarily pair-wise distinct);

2. if $a = q_1 q_2 \cdots q_s$ is another such factorization, then $r = s$ and after a permutation of the indices, p_i and q_i are associates for each $i = 1, 2, \ldots, r$.

Observation. If R is a UFD, we have a well-defined function

$$l : R\backslash\{0\} \longrightarrow \mathbb{N},$$

where $l(a) = 0$ if a is a unit, and $l(a) = r$ if a is a non-unit and is a product of r irreducible factors. Then

$$l(ab) = l(a) + l(b), \qquad a, b \in R\backslash\{0\}.$$

Terminology: If a in a UFD R is non-zero and non-unit, a factorization

$$a = p_1 p_2 \cdots p_n,$$

where each p_j is irreducible, is called a prime factorization, or a factirzation of a into primes, or a factirzation of a into irreducibles.

Fundamental Theorem of Arithmetic: The ring $\mathbb{Z}$ is a UFD.

Example: For $\mathbb{Z}$ and $n \neq \pm 1$, $l(n)$ is the number of prime factors counting multiplicity:

$$l(-2^3 7^2 (11)^5) = 3 + 2 + 5 = 10.$$

Next immediate goal: To prove that every PID is a UFD.

Two characterizing properties of a UFD:

Lemma. An element in a UFD is irreducible if and only if it is prime.

Proof. Let R be a UFD. Already know prime are irreducible.

- Let $a \in R$ be irreducible, and suppose that $a|bc$ for $b, c \in R\backslash\{0\}$.
  Need to show either $a|b$ or $a|c$
- Then $bc = ax$ for some $x \in R$.
- If b is a unit, then $a|c$, and if c is a unit, then $a|b$.
  $\Rightarrow c = a(xb^{-1})$
- Suppose that neither b nor c is a unit. Write

$$b = p_1 \cdots p_n, \qquad c = q_1 \cdots q_m, \qquad x = r_1 \cdots r_t$$

as products of irreducibles. Then

$$bc = p_1 \cdots p_n q_1 \cdots q_m = ax = ar_1 \cdots r_t.$$

- Uniqueness of the factorizations implies that a is an associate of some p_i's or some q_j. Thus $a|b$ or $a|c$.
- Conclusion: irreducible elements of R are prime.

Q.E.D.

Lemma. Let R be an integral domain. If there exists a non-zero non-unit $a \in R$ which is not the product of irreducible elements in R, then there exists a chain

$$aR \subset c_1 R \subset c_2 R \subset \cdots \subset c_n R \subset \cdots$$

of principal ideals in R with proper inclusion at each step.

Proof.

- As a is not irreducible, have $a = a_1 b_1$, neither a_1 nor b_1 is a unit. So

$$aR \subset a_1 R, \quad aR \subset b_1 R, \quad \text{and} \quad aR \neq a_1 R, \quad aR \neq b_1 R.$$

- Either a_1 or b_1 is not irreducible. Say a_1 is not irreducible. Then can write $a_1 = a_2 b_2$, where neither a_2 nor b_2 is a unit, so

$$a_1 R \subset a_2 R, \quad a_1 R \subset b_2 R, \quad \text{and} \quad a_1 R \neq a_2 R, \quad a_1 R \neq b_2 R.$$

- Now $a = a_2 b_2 b_1$, and at least one of the three elements a_2, b_2, b_1 is not irreducible. Proceeding this way, we get the desired chain

$$aR \subset c_1 R \subset c_2 R \subset \cdots \subset c_n R \subset \cdots .$$

Cor: If R has ACCPI, then every non-zero non unit $a \in R$ is a product of irreducibles.

Q.E.D.

Definition. An integral domain is said to satisfy the ascending chain condition for principal ideals (ACCPI) if for every increasing sequence

$$I_1 \subset I_2 \cdots \subset I_n \subset \cdots$$

of principal ideals there exists m such that $I_n = I_m$ for all $n \geq m$.

Theorem. An integral domain R is a UFD if and only if it satisfies the ACCPI and every irreducible element in R is prime.

Proof. Assume R is a UFD. Already know every irreducible of R is prime.

- Need to show that R has ACCPI. Thus assume that

  $$a_1R \subset a_2R \subset \cdots \subset a_nR \subset \cdots$$

  is an increasing sequence of principal ideals in R.
- If $a_j = 0$ for every j, nothing to prove, so assume otherwise. Let $j \geq 1$ be the smallest j such that $a_j \neq 0$. Then $(l(a_j),\ l(a_{j+1}), \ldots)$ decreases so there is some m s.t. $l(a_n) = l(a_m)$ for all $n \geq m$.
- Since $a_n | a_m$ for every $n \geq m$, a_n and a_m are associates for all $n \geq m$, i.e., $a_nR = a_mR$ for all $n \geq m$. Thus R has ACCPI.

Proof cont'd: Assume R has ACCPI and every irreducible of R is prime.

- Let $a \in R$ be non-zero and non-unit. By Lemma above, a has a factorization into irreducibles. Let $m(a)$ be the smallest positive integer such that a is a product of $m(a)$ irreducibles. with multiplicity
- If $m(a) = 1$, then a is irreducible, and uniqueness is clear.
- Assume that $m = m(a) > 1$ and that uniqueness of factorization holds for any $b \in R$, $b \neq 0$, with $m(b) < m$.
- Let $a = p_1 \cdots p_m = q_1 \cdots q_n$ be two factorizations into irreducibles.
- Since every irreducible of R is prime, p_m is prime.
- As $p_m | q_1 \cdots q_n$, p_m divides q_j for some $1 \leq j \leq n$.
- By re-ordering the elements, we may assume that $j = n$, so $q_n = x p_m$ for some $x \in R$. As q_n is irreducible and p_m is not a unit, x must be a unit, so p_m and q_n are associates.
- Let $b = (x^{-1} p_1) p_2 \cdots p_{m-1} = q_1 \cdots q_{n-1}$. Then $m(b) \leq m - 1$. By induction assumption, $n - 1 = m - 1$ and that, re-order the elements $q_1, \ldots, q_{n-1}$ if necessary, $x^{-1} p_1$ and q_1 are associates and p_j and q_j are associates for $j \geq 2$.

Q.E.D.

Theorem. A PID is a UFD.

Proof. A PID has the two characterizing properties of a UFD.

Q.E.D.

Example: We will show that if R is a UFD, so is $R[x]$.

Fact: Let R be an integral domain. Then $R[X]$ is a PID iff R is a field.

Example: The ring $\mathbb{Z}[x]$ is a UFD but not a PID.

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

as $\langle r, x \rangle$ can be used to test $\exists r^{-1}$