PIDs and UFDs, III: GCD in UFDs and The Chinese Remainder Theorem for PIDs

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday Jan 27, 2025

Thursday Feb 6, 2025

In this file: §1.2.5-1.2.6.

Monday Jan 27, 2025

1. Greatest common divisors in UFDs;
2. The Chinese Remainder Theorem for PIDs

Thursday Feb 6 2025

Greatest common divisors in UFDs

Definition. Given an integral domain R and a non-empty $B \subset R\backslash\{0\}$, a greatest common divisor (gcd) of B is an element $a \in R$ such that

1. $a|b$ for all $b \in B$;
2. If $a'|b$ for all $b \in B$, then $a'|a$.

Remarks.

- Definition does not guarantee greatest common divisors for a given $B \subset R\backslash\{0\}$ always exist;
- Greatest common divisors for a given $B \subset R\backslash\{0\}$, if exist, are unique only up to associates (exercise).
- For $\mathbb{Z}$, we always pick the positive number as the gcd.

An example of non-existence of gcd

Ex: $\mathbb{Z}[\sqrt{-5}] = \{ a + \sqrt{5}\, i b : a, b \in \mathbb{Z} \}$

$a = 9, \quad b = 6 + 3\sqrt{5} i$

$D(a) = \{ 3, \; 9, \; \cancel{1}, \; 2 \pm \sqrt{5} i \}$

$D(b) = \{ \cancel{1}, \; 3, \; 2 + \sqrt{5} i, \; b \}$

$D(a) \cap D(b) = \{ 3, \; 2 + \sqrt{5} i \}$

Recall that $\mathbb{Z}[\sqrt{5}]$ is not a UFD

Proposition. If R is a UFD, then gcd exist for any non-empty $B \subset R \backslash \{0\}$.

Proof. Let D be the set of all common divisors of B.

- $D \neq \emptyset$ because $1 \in D$;
- The map $D \to \mathbb{Z}$, $d \mapsto l(d)$, is bounded from above by $l(b_0)$ for any $b_0 \in B$;
- Let $a \in D$ be such that $l(a) = \max\{l(d) : d \in D\}$.
- We now prove that a is a gcd of B.
- Only need to show that for any $a' \in D$, one has $a' | a$.

Proof cont'd:

- Suppose not. Then there exists $a' \in D$ such that $a' \nmid a$.
- Then there exists a prime element $p \in R$ and positive integer m such that $p^m | a'$ and $p^m \nmid a$.
- Let $b \in B$. Then $p^m | a' | b$, so $p^m | b$.
- As $a | b$, have $b = ax$ for some $x \in R$. So $p^m | ax$.
- Since $p^m \nmid a$ and p is prime, we have $p | x$. Thus $ap | b$.
- Since $b \in B$ is arbitrary, we see that $ap \in D$.
- Since $l(ap) = l(a) + 1$, we get a contradiction to the definition of a.
- We conclude that a is a gcd of B.

Q.E.D.

An explicit way of finding a gcd: Let $B \subset R \backslash \{0\}$, non-empty.

- Let $P(B) = \{p \in R : \ p$ irreducible and is a common divisor of $B\}$.
- Consider $P'(B) = P(B)/R^\times$, i.e., elements counted up to associates.
- For each $p \in P'(B)$, let
$$m(p) = \max\{m \in \mathbb{Z}_{\geq 0} : \ p^m | b, \ \forall\, b \in B\}.$$
- Note that $|P'(B)| \leq l(b_0)$ for any $b_0 \in B$, so $P'(B)$ is a finite set.
- A gcd of B is given by
$$\prod_{p \in P'(B)} p^{m(p)}.$$

$2^3 5^2 11^9 13^7$ $\quad$ $7^2 5^3$

An example from $\mathbb{Z}$.

To continue on Thursday, Feb 6, 2025.

Definition: Two non-zero elements b_1 and b_2 in a UFD are said to be co-prime or relatively prime if $\gcd(b_1, b_2) = 1$.

Lemma. Assume that b_1 and b_2 are co-prime, and suppose that $a \in R$ is such that $b_1|a$ and $b_2|a$. Then $(b_1 b_2)|a$.

Proof. Write $a = b_1 x$ for $x \in R$, so $b_2|b_1 x$.

- Let p be any prime element such that $p|b_2$ and let m be the highest power such that $p^m|b_2$.
- Since b_1 does not contains any power of p in its prime factorization, we have $p^m|x$.
- Thus $b_2|x$, so $(b_1 b_2)|a$.

Q.E.D.

Greatest common divisors in a PID.

主理想整环中最大公约数生成和理**想，**欧几里得整环中这个最大公约数及其生成方法还有求取的算法

In a PID, gcds have special properties.

Proposition. Let R be a PID, the gcds for a non-empty $B \subset R\backslash\{0\}$ are precisely the generators of the ideal I_B generated by B. In particular,

$$\gcd(B) = r_1 b_1 + \cdots + r_n b_n$$

for some $r_1, \ldots, r_n \in R$ and $b_1, \ldots, b_n \in B$.

Proof. Let $a \in R$ be a generator of the ideal I_B generated by B.

- For every $b \in B$, we have $b \in I_B = aR$, so $a|b$.
- $a \in I_B$ implies that $a = r_1 b_1 + \cdots + r_n b_n$ for some $r_i \in R$ and $b_i \in B$.
- If a' is a common divisor of B, then $a'|b_i$ for each i, so $a'|a$.
- We conclude the a is a gcd of B.

Q.E.D.

The fact that a gcd of B lies in I_B is not true for arbitrary UFDs:

Example: Let $R = \mathbb{Q}[x, y]$. Will show that R is a UFD. Have

$$\mathrm{gcd}(x, y) = 1,$$

but $R \neq xR + yR$.

$\gcd(x, y) = 1$

but $xR + yR \neq 1R$

§1.2.6: The Chinese Remainder Theorem.

The Chinese Remainder Theorem. Let $b_1, \ldots, b_n$ be positive integers and pairwise co-prime. Let $0 \leq r_i < b_i$ for $i = 1, \ldots, n$. Then the system

$$\begin{cases} x \equiv r_1 \pmod{b_1}, \\ \cdots \\ x \equiv r_n \pmod{b_n} \end{cases}$$

has a solution in $\mathbb{Z}$, and any two solutions x and x' satisfies

$$x - x' = 0 \equiv \pmod{b_1 b_2 \cdots b_n}.$$

Proof of the Chinese Remainder Theorem for $n = 2$:

- It follows from $\gcd(b_1, b_2) = 1$ that there exists $\alpha, \beta \in \mathbb{Z}$ such that $1 = \alpha b_1 + \beta b_2$.
- Then $r_1 - r_2 = (r_1 - r_2)\alpha b_1 + (r_1 - r_2)\beta b_2$, so have a solution

$$x = r_1 - (r_1 - r_2)\alpha b_1 = r_2 + (r_1 - r_2)\beta b_2.$$

$b_1 \mid a \quad a = k_1 b_1$

$b_2 \mid a \quad a = k_2 b_2$

- Suppose that x and x' are two solutions.
- Then $b_1|(x - x')$ and $b_2|(x - x')$.
- As b_1 and b_2 are co-prime, we have $b_1 b_2|(x - x')$.

$\lambda_1 b_1 + \lambda_2 b_2 = 1$

$k_1 = \lambda_1 k_1 b_1 + \lambda_2 k_1 b_2$

$= \lambda_1 k_2 b_2 + \lambda_2 k_1 b_2$

$= (\lambda_1 k_2 + \lambda_2 k_1) b_2$

Q.E.D.

Example:

The Chinese Remainder Theorem for PIDs.

Theorem. Let R be a PID, and let $q_1, q_2, \ldots, q_k$ be elements in R that are pair-wise co-prime, i.e. $\gcd(q_i, q_j) = 1$ for all $i \neq j$. Then the map

$$R/\langle q_1 q_2 \cdots q_k\rangle \longrightarrow (R/\langle q_1\rangle) \times (R/\langle q_2\rangle) \times \cdots \times (R/\langle q_k\rangle)$$

given by $r + \langle q_1 q_2 \cdots q_k\rangle \mapsto (r + \langle q_1\rangle,\ r + \langle q_2\rangle,\ \ldots,\ r + \langle q_k\rangle)$ is a ring isomorphism.

Proof. For $k = 2$ the proof is the same as for $\mathbb{Z}$. Genera case follows from the case of $k = 2$.

Corollary: Let $p_1, p_2, \ldots, p_k$ be distinct prime numbers, and let $n_1, n_2, \ldots, n_k$ be positive integers. Then

$$\mathbb{Z}/\langle p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\rangle \cong (\mathbb{Z}/\langle p_1^{n_1}\rangle) \times (\mathbb{Z}/\langle p_2^{n_2}\rangle) \times \cdots \times (\mathbb{Z}/\langle p_k^{n_k}\rangle).$$