East-West J. of Mathematics: Vol. 10, No 2 (2008) pp. 149-152

NEW CHARACTERIZATIONS OF PRINCIPAL IDEAL DOMAINS

Nong Quoc Chinh and **Pham Hong Nam**

Thai Nguyen College of Sciences
Thai Nguyen, Vietnam
e-mail: nongquocchinh2002@hn.vnn.vn

Abstract

In this short paper, we prove that a domain is a principal ideal domain if and only if it is a unique factorization domain and all its prime ideal are principal. As a consequence, we characterize principal ideal domains in term of the existence of a presentation of the greatest common divisor of finitely many elements as a linear combination of these elements.

1. Introduction

Let R be a commutative ring. Recall that R is called *Noetherian* if the set of ideals of R satisfies the ascending chain condition, i.e. for any ascending chain

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

of ideals of R, there exists an integer n_0 such that $I_n = I_{n_0}$ for all $n \geq n_0$. It is known that R is Noetherian if and only if every ideal of R is finitely generated. Then I. S. Cohen gave an interesting characterization of Noetherian rings which states that R is Noetherian if and only if every prime ideal of R is finitely generated, cf. [1] (see also [3, Theorem 3.4]). This fact suggests us to think that to study a certain property on the set of all ideals of a ring, it may be enough to study this property on the set of all prime ideals.

Throughout this paper, let D be a domain. For the basic concepts and terminologies, we reffer to the book [2]. We say that D is a *principal ideal domain* if every ideal of D is principal, i.e. it can be generated by an element. D is called a *unique factorization domain* (UFD for short) if every non zero

Keywords: Principal ideal domains, unique factorization domains, prime ideals, greatest common divisors.
2000 AMS Mathematics Subject Classification: 13A05, 13C05.

element of D, which is not a unit, can be factorized into a product of irreducible elements and this factorization is uniquely determined up to a unit factor and an ordering of the irreducible factors. It is well known that if D is a principal ideal domain then D is a UFD, but the converse is not true. For example, the ring of polynomials in two variables with coefficients in a field is a UFD, but not a principal ideal domain.

The main result of this paper is the following theorem, which gives a new characterization of principal ideal domains. The motivation of this result comes from the above mentioned result by I. S. Cohen in [1].

Theorem 1.1 *Let D be a domain. Then D is a principal ideal domain if and only if D is a UFD and every prime ideal of D is principal.*

As a consequence of Theorem 1.1, we have other characterizations of principal ideal domains as follows. It should be mentioned that if D is a UFD then for any elements $a_1, \ldots, a_n$ of D which are not all zero, their greatest common divisor $\gcd(a_1, \ldots, a_n)$ exists. Moreover, if D is a principal ideal domain then $\gcd(a_1, \ldots, a_n)$ can be expressed as a linear combination of $a_1, \ldots, a_n$, i.e. there exist $x_1, \ldots, x_n \in D$ such that

$$\gcd(a_1, \ldots, a_n) = a_1x_1 + \ldots + a_nx_n.$$

Colloraly 1.2 *Let D be a UFD. The following statements are equivalent:*

(i) D is a pricipal ideal domain.

(ii) Every maximal ideal of D is a principal ideal.

(iii) For any elements $a_1, \ldots, a_n$ of D which are not all zero, their greatest common divisor $gcd(a_1, \ldots, a_n)$ exists and it is a linear combination of $a_1, \ldots, a_n$.

2. The Proofs

Proof of Theorem 1.1 One direction is clear. For the non trivial direction, assume that every prime ideal of D is principal. Let I be an ideal of D. If $I = (0)$ or $I = D$ then I is principal. Suppose that $I \neq (0)$ and $I \neq D$. Let $0 \neq a \in I$. As $I \neq R$, it follows that a is not a unit. Moreover, since D is a UFD, we have a factorization $a = p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$, where $k \geq 1$ is an integer and p_i's are distinct irreducible elements. Note that the $p_i^{s_i}$'s are uniquely determined up to a unit, so we call them the *components* of a. Also, the number k in the above factorization of a is uniquely determined. So, we can set $r(a) = k$, the number of distinct irreducible divisors of a. Set

$$m = r(I) = \min\{r(a) \mid 0 \neq a \in I\}.$$

Then $m \geq 1$ and $r(a) \geq m$ for all $a \in I$. Moreover, there exists $b \in I$ with $r(b) = m$. Assume that $b = p_1^{j_1}p_2^{j_2}\ldots p_m^{j_m}$ where p_i is an irreducible element for all $i = 1, 2, \ldots, m$. For each p_i, let X_{p_i} be the set of all integer $s_i \geq 1$ such that $p_i^{s_i}$ appears as a component in an irreducible factorization of some element $a \in I$. For each i, let t_i be the least integer s_i in X_{p_i}. Let $d = p_1^{t_1} \dots p_m^{t_m}$. We will prove that $I = (d)$.

Firstly we show that $I \subseteq (d)$, i.e. d is a divisor of a for all $a \in I$. In fact, suppose that d is not a divisor of a for some $a \in I$, let $d' = \gcd(a, b)$. Since d' is a divisor of b, we have $r(d') \leqslant m$. From the definition of t_i, if p_i is a divisor of a then $p_i^{t_i}$ is also a divisor of a. Moreover, because d is not a divisor of a, there exists some $j \in \{1, \dots, m\}$ such that p_j is not a divisor of a. It implies that $r(d') < m$. We show that d' is a linear combination of a and b. In fact, since $d' = \gcd(a, b)$, there exist $a_1, a_2 \in D$ such that $a = d'.a_1$ and $b = d'.a_2$. So $\gcd(a_1, a_2) = 1$. Set

$$I_1 = \{a_1x + a_2y : x, y \in D\}.$$

Then I is an ideal of D. We claim that $I_1 = D$. In fact, suppose that $I_1 \neq D$. Then there exists a maximal ideal J of D containing I_1. Since J is maximal, $J \neq D$ and J is a prime ideal. By hypothesis, there exists $p \in D$ such that $J = (p)$. Since $a_1, a_2 \in I_1$, it follows $a_1, a_2 \in J = (p)$, i.e p is a common divisor of a_1 and a_2. Since $\gcd(a_1, a_2) = 1$, we get that p is a unit. Hence $J = D$, a contradiction and the claim is proved. Now, since $I_1 = D$, we get $1 \in I_1$ and hence $1 = a_1x + a_2y$ for some $x, y \in D$. Hence

$$d' = 1.d' = (a_1x + a_2y)d' = ax + by \in I$$

as $a, b \in I$. So $r(d') \geq m$, a contradiction. So d is a divisor of a for all $a \in I$.

Next we show that $(d) \subseteq I$, i.e. $d \in I$. For each $i \in \{1, 2, \dots, m\}$, there exists by the definition of t_i an element $b_i \in I$ such that

$$b_i = p_1^{s_1} \dots p_{i-1}^{s_{i-1}} p_i^{t_i} p_{i+1}^{s_{i+1}} \dots p_m^{s_m} y_i,$$

where p_j is not a divisor of y_i and $s_j \geq t_j$ for all $j \in \{1, \dots, m\}$. It is not difficult to check that

$$\gcd(b, b_1, b_2, \dots, b_m) = p_1^{t_1} \dots p_m^{t_m} = d.$$

Note that $b, b_1, b_2, \dots, b_m \in I$. Therefore, to prove $d \in I$, it is enough to show that d is a linear combination of $b, b_1, b_2, \dots, b_m$. Set $\gcd(b_1, b_2, \dots, b_m) = c$. Then $d = \gcd(b, c)$. By the same arguments as above, there exist $x_1, x_2 \in D$ such that $d = bx_1 + cx_2$. Therefore, we need only to prove that c is a linear combination of $b_1, b_2, \dots, b_m$. We prove this by induction on m. The case $m = 1$ is nothing to do. Let $m \geq 2$ and assume that the result is true for $m - 1$. Set $c_1 = \gcd(b_1, b_2, \dots, b_{m-1})$. Then $c = \gcd(c_1, b_m)$. By induction,

$$c_1 = b_1x_1 + b_2x_2 + \dots + b_{m-1}x_{m-1}$$

for some $x_1, x_2, \dots, x_{m-1} \in D$. Since $c = \gcd(c_1, b_m)$, there exist $y, z \in D$ such that $c = c_1y + b_mz$. Therefore

$$c = b_1(x_1y) + b_2(x_2y) + \dots + b_{m-1}(x_{m-1}y) + b_mz$$

is a linear combination of $b_1, b_2, \dots, b_m$.Thus the theorem is completely proved.$\square$

Proof of Colloraly 1.2 $(i) \Rightarrow (ii)$ is trivial.
$(ii) \Rightarrow (iii)$. By induction on the number of elements, it is enough to prove (iii) for the case of two elements, i.e. if $a_1, a_2 \in D$ such that one of them is not zero then the greatest common divisor $d = \gcd(a_1, a_2)$ is a linear combination of a_1, a_2. Write $a_1 = db_1$ and $a_2 = db_2$, where $\gcd(b_1, b_2) = 1$. Set $I = \{b_1x + b_2y : x, y \in D\}$. If $I \neq D$ then I is contained in a maximal ideal of D, which is a principal ideal by (ii). Then we get a contradiction by the same arguments as in the proof of Theorem 1.1. It follows that $I = D$. Therefore $1 = b_1x + b_2y$ for some $x, y \in D$. Hence $d = a_1x + a_2y$ and the result follows.
$(iii) \Rightarrow (i)$. Let I be an ideal of D. If $I = (0)$ or $I = D$ then I is principal. So we can assume that $I \neq (0)$ and $I \neq D$. As in the proof of Theorem 1.1, we set

$$m = r(I) = \min\{r(a) \mid 0 \neq a \in I\},$$

where $r(a)$ is the number of distinct irreducible divisors of a. Note that $r(a) \geq m$ for all $a \in I$ and there exists $b \in I$ with $r(b) = m \geq 1$. Write $b = p_1^{j_1} p_2^{j_2} \dots p_m^{j_m}$ where p_i's are distinct irreducible divisors of b. For each $i = 1, \dots, m$, let X_{p_i} and t_i be defined as in the first paragraph of the proof of Theorem 1.1. Let $d = p_1^{t_1} \dots p_m^{t_m}$. We will prove that $I = (d)$. Let $a \in I$. Assume that d is not a divisor of a. Let $d' = \gcd(a, b)$. Then $r(d') < m$. By the assumption (iii), d' is a linear combination of a and b. As $a, b \in I$, we have $d' \in I$ and hence $r(d') \geq m$. This gives a contradiction. Therefore $a \in (d)$. Thus $I \subseteq (d)$. Conversely, By the definition of t_i for $i = 1, 2, \dots m$, there exists $b_i \in I$ such that

$$b_i = p_1^{s_1} \dots p_{i-1}^{s_{i-1}} p_i^{t_i} p_{i+1}^{s_{i+1}} \dots p_m^{s_m} y_i,$$

where p_j is not a divisor of y_i and $s_j \geq t_j$ for all j. It follows that

$$\gcd(b, b_1, b_2, \dots, b_m) = p_1^{t_1} \dots p_m^{t_m} = d.$$

By the hypothesis (iii), d is a linear combination of $b, b_1, b_2, \dots, b_m$. As $b, b_1, b_2, \dots, b_m \in I$, we get that $d \in I$. Thus $I = (d)$ as required. $\square$

Acknowledgment. The authors thank Professor Le Thanh Nhan for careful reading the manuscript and for many useful suggestions during preparation of this paper.

References

[1] I. S. Cohen, *Commutative rings with restricted minumum condition*, Duke Math. J., **17** (1950), 27-42.

[2] S. Lang, "Algebra", Springer, 2005 (Revised third edition).

[3] H. Matsumura, "Commutative ring theory", Cambridge University Press, 1986.