A NEW CHARACTERIZATION OF PRINCIPAL IDEAL DOMAINS

PHAM HONG NAM, NONG QUOC CHINH, LE THANH NHAN

College of Natural and Social Sciences
Thai Nguyen University

Abstract In this paper, we give a new characterization of principal ideal domains in term of the existence of a representation of the greatest common divisor of finitely many elements as a linear combination of these elements.

1 Introduction

Let D be a domain. The usual theory of unique factorization of an integer into a product of prime numbers has been developed for domains. A domain satisfies such a property of unique factorization is called a unique factorization domain (UFD for short). Recall that D is a *principal ideal domain* (PID for short) if any ideal of D is principal, i.e. it can be generated by an element. It is well known that any PID is a UFD, but the converse is not true. Therefore ones wish to find conditions for a UFD to be a PID.

It was shown that in a domain D, any maximal ideal is a prime ideal, and if D is a PID then any non zero prime ideal of D is maximal. An interesting characterization for a UFD to be a PID related to these terms was given by Gauss: D is a PID iff D is a UFD and any non zero prime ideal is maximal (see [A]).

We also know that for any elements $a_1, \ldots, a_n$ in a UFD which are not all zero, the greatest common divisor $\gcd(a_1, \ldots, a_n)$ of $a_1, \ldots, a_n$ exists, and if the UFD is a PID then $\gcd(a_1, \ldots, a_n)$ can be expressed as a linear combination of $a_1, \ldots, a_n$.

In this short paper, we prove the converse, that is a new characterization of a PID in term of the existence of a representation of the greatest common divisor of finitely many elements as a linear combination of these elements. This result is in some sense similar to the above work done by Gauss.

Main theorem. *Let D be a domain. Then D is a PID iff D is a UFD and for any elements $a_1, \ldots, a_n$ not all zero, their greatest common divisor $\gcd(a_1, \ldots, a_n)$ can be expressed as a linear combination of $a_1, \ldots, a_n$.*

2 Main result

Before proving the main result, we present the following lemma.

Lemma 2.1. *Let D be a UFD. Then the following statements are equivalent:*

(i) For any elements $a_1, \ldots, a_k$ of D which are not all zero, their greatest common divisor $\gcd(a_1, \ldots, a_k)$ is a linear combination of $a_1, \ldots, a_k$.

(ii) Every non zero prime ideal of D is maximal.

Proof. (i)⇒(ii). Let I be a non zero prime ideal of D. Assume that J is an ideal of D containing I such that $J \neq I$. Let $b \in J$ such that $b \notin I$. Since $I \neq 0$, there exists a non zero element $a \in I$. Since I is prime, $I \neq D$. Therefore a is not a unit. Because D is a UFD, there exists a factorization $a = p_1 \cdots p_k$, where p_i is irreducible for all $i = 1, \ldots, k$. Since I is a prime ideal and $a \in I$, there exists i such that $p_i \in I$. Since $b \notin I$, it follows that p_i is not a divisor of b. So the greatest common divisor of p_i and b is 1. By the hypothesis (i), there exists $q, r \in D$ such that $p_i q + br = 1$. Since $p_i \in I$, we have $p_i \in J$. As p_i and b are elements of J, it follows that $1 \in J$, i.e. $J = D$. Therefore I is a maximal ideal of D, and (ii) is proved.

Conversely, suppose that (ii) is true. Let $a_1, \ldots, a_n$ be any elements in D which are not all zero, and let d be a greatest common divisor of $a_1, \ldots, a_n$. We need to show that d is a linear combination of $a_1, \ldots, a_n$. The case $n = 1$ is nothing to do. Let $n = 2$. We first assume that $a_1, a_2 \in D$ are not both zero, and $\gcd(a_1, a_2) = d = 1$. Set

$$I = \{a_1 x + a_2 y \ : \ x, y \in D\}.$$

It is clear that I is a non zero ideal of D. We claim that $I = D$. Suppose that $I \neq D$, and we look for a contradiction. As $I \neq D$, there exists a maximal ideal J containing I. Since $I \neq 0$, we get $J \neq 0$. Therefore there exists $a \in J, a \neq 0$. Since J is maximal ideal of D, it follows that a is not a unit. Because D is unique factorization domain, a has a factorization $a = p_1^{s_1} \cdots p_k^{s_k}$, where p_i is irreducible, and $p_i, i = 1, \ldots, k$, are distinct. Note that the number k in the above factorization of a is unique determined. So, we can set $r(a) = k$. Since J is a maximal ideal, it is a prime ideal. So there exists i such that $p_i^{s_i} \in J$, and hence $p_i \in J$, i.e. there exists a irreducible element p in J. Hence $(p) \subseteq J$. Since p is irreducible and D is unique factorization domain, p is prime, and hence (p) is a non zero prime ideal. Therefore (p) is a maximal ideal by the assumption (ii). As $J \neq D$, it follows that $J = (p)$. Since $a_1, a_2 \in I$, we have $a_1, a_2 \in J = (p)$. Therefore p is a common divisor of a_1 and a_2. Since $\gcd(a_1, a_2) = 1$, we get that p is associated with 1, and hence $J = (p) = D$. This gives a contradiction since J is prime ideal. Therefore $I = D$ and the claim is proved. Now, since $I = D$, we get by the definition of I that $1 = a_1 x + a_2 y$ for some $x, y \in D$. For the case d is arbitrary, $d = (a_1, a_2)$, we write $a_1 = db_1, a_2 = db_2$. Then $\gcd(b_1, b_2) = 1$. So we get by the above fact that $1 = b_1 x + b_2 y$. Hence

$$d = db_1 x + db_2 y = a_1 x + a_2 y.$$

Let $n > 2$ and assume that the result is true for $n - 1$. Set $d' = \gcd(a_1, \ldots, a_{n-1})$. Then $d = \gcd(d', a_n)$. By the induction hypothesis,

$$d' = a_1x_1 + \ldots + a_{n-1}x_{n-1}$$

for some $x_1, \ldots, x_{n-1} \in D$. Since $d = \gcd(d', a_n)$, there exist $y, z \in D$ such that $d = d'y + a_nz$. Therefore

$$d = d'y + a_nz = a_1(x_1y) + \ldots + a_{n-1}(x_{n-1}y) + a_nz,$$

i.e. d is a linear combination of $a_1, \ldots, a_n$. □

As mentioned in the introduction, Gauss proved that a domain D is a principal ideal domain iff D is a UFD and each non zero prime ideal of D is maximal. Therefore, our main theorem follows immediately by the above lemma. However, we give here a direct, elementary and short proof for the main theorem.

Proof of main Theorem. We knew that if D is a PID then D is a UFD and for any elements $a_1, \ldots, a_n \in D$ not all zero, their greatest common divisor $\gcd(a_1, \ldots, a_n)$ is a linear combination of $a_1, \ldots, a_n$. Now we prove the converse. Let I be an ideal of D. If $I = \{0\}$ or $I = D$ then I is principal.

Assume that $I \neq D$ and $I \neq 0$. Let a be a non zero element of I. Because D is unique factorization domain, a has a factorization $a = p_1^{s_1} \cdots p_k^{s_k}$, where p_i is irreducible, and $p_i, i = 1, \ldots, k$, are distinct. Note that the number k in the above factorization of a is unique determined. So, we can set $r(a) = k$, the number of distinct prime divisors of a. Set

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

Then $r(a) \geq m$ for all $a \in I$ and there exists $b \in I$ with $r(b) = m \geq 1$. Assume $b = u_2{p_1}^{s_1} \ldots {p_m}^{s_m}$ where u_2 is a unit, p_i's are prime elements and $s_i \geq 1$ for all i. For each p_i, set X_{p_i} be the set of all integer $s_i \geq 1$ such that $p_i^{s_i}$ appears as a component in a prime factorization of some element $a \in I$. For each i, let t_i be the least integer s_i in X_{p_i}. Let $d = {p_1}^{t_1} \cdots {p_m}^{t_m}$. We show that 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 $d' = \gcd(a, b)$, then $r(d') < m$ and since d' is a linear combination of a and b, it follows that $d' \in I$, this gives a contradiction. Hence $I \subseteq (d)$. So, it is enough to show $d \in I$.

By the choice of $t_i, i = 1, \ldots, m$, there exists $a_i \in I$ such that

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

where p_i is not a divisor of y_i for all i, j, and $s_i \geq t_i$ for all i. Hence

$$\gcd(b, a_1, \ldots, a_m) = p_1^{t_1} \ldots p_m^{t_m} = d.$$

By the hypothesis, d is a linear combination of $b, a_1, \ldots, a_m \in I$, so $d \in I$. □

References

[1] Robert B. Ash. "Abstract Algebra", Springer-Verlag, 2000.