

# A Report Study of Some Topics in Algebra

**Bashayer Fayed Al-qurashi**

Departement of Mathematical Sciences

Faculty of Applied Sciences

Umm AL-qura University, Saudi Arabia

This article is distributed under the Creative Commons by-nc-nd Attribution License.  
Copyright © 2020 Hikari Ltd.

## Abstract

The research project has described the Euclidean Domains (ED), the Principal Ideal Domain (PID) and the Unique Factorization Domain (UFD). We find that there exists a Principal Ideal Domain (PID) which is not an Euclidean Domain (ED). Every Principal Ideal Domain (PID) is a Unique Factorization Domain (UFD). On other hand, it is not true that every Unique Factorization Domain (UFD) is a PID. We use the concept of the norm. In the end of the report, we discuss tensor product of certain algebraic structures. We have tried to understand how the tensor product behaves with the present of dual spaces.

## 1 Introduction

This research will introduce the notion of further algebraic structures and prove the relationship between them. The research will describe the Euclidean Domain (ED) and the Principal Ideal Domain (PID). Moreover, we will talk about the Unique Factorization Domain (UFD) then we will provide the relationship between (ED), (PID) and (UFD). We give some counter example. At the end of the section, we will study some of the properties of the tensor product see

the ring  $R$  is the identity in tensor product operation on the category of  $R$ -modules. We prove that. We know that dual module  $M^*$  may or may not be the inverse of tensor product operation of modules.

## 2 Euclidean Domains

In this section, we shall study the Euclidean domain and give some examples.

In this section, the results are extracted from the references [2, 3].

**Definition 2.1.** A commutative ring with unity  $1 \neq 0$  and no zero divisors is called an integral domain.

We first define the notion of a norm on an integral domain.

**Definition 2.2.** A norm on the integral domain is defined as a function  $N : R \rightarrow \mathbb{Z}^+ \cup 0$  with  $N(0) = 0$ .

where  $R$  is an integral domain and  $\mathbb{Z}^+$  denote positive integer.

**Definition 2.3.**  $N$  is a positive norm if and only if  $N(a) > 0$  for  $a \neq 0$ .

It may be possible for the same integral domain  $R$  to possess several different norms because of that we can say a norm is fairly weak.

**Definition 2.4.** An integral domain  $R$  is said to be Euclidean domain if there exist 'd' norm non zero element of  $R$  to non-negative integer, such that

- $d(a) \leq d(a, b) \quad \forall a \neq 0 \in R.$

- Let  $a \in R, a \neq b \in R$  then there exist  $R$  such that

$$a = qb + r \quad \text{with } r = 0 \text{ or } d(r) < d(b).$$

**Definition 2.5.** Let  $R$  be an integral domain and  $a, b \in R$  with  $b \neq 0$ , the Euclidean algorithm of Euclidean consisting of repeatedly applying division

algorithm to  $a$  and  $b$  until we will get a remainder, as follows

$$\begin{aligned} a &= q_1b + r_1 \\ b &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_kr_k + r_{k+1} \\ r_k &= q_{k+1}r_{k+1}. \end{aligned}$$

By division algorithm, we know that  $N(r_1) > N(r_2) > \dots$ , and since  $N(r_i)$  is a nonnegative integer for each  $i$ , this sequence must eventually terminate with the last remainder equalling zero (else we would have an infinite decreasing sequence of non negative integers).

**Example 2.1.** In an Euclidean Domain there are some trivial examples as fields where any norm satisfies the defining condition (e.g.,  $N(a) = 0$  for all  $a$ ). This is because every  $a, b$  with  $b \neq 0$  we have  $a = qb + 0$ , where  $q = ab^{-1}$ .

**Example 2.2.** The ring of integers  $\mathbb{Z}$  is an Euclidean Domain with norm is given by the absolute value  $N(a) = |a|$ . A Division Algorithm in  $\mathbb{Z}$  is the familiar "long division" of elementary arithmetic and the existence of it is verified as follows: Let  $a$  and  $b$  be two nonzero integers, then suppose first that  $b > 0$ . The real line is divided by the half open intervals  $[nb, (n+1)b), n \in \mathbb{Z}$ , so  $a$  is in one of them. We can say that  $a \in [kb, (k+1)b)$ . For  $q = k$  we have  $a - qb = r \in [0, |b|)$  as needed. If  $b < 0$ , (so,  $-b > 0$ ), Accordingly, there is an integer  $q$  such that  $a = q(-b) + r$  with either  $r = 0$  or  $|r| < |-b|$ . Then to make it more formal we can use the induction on  $|a|$ .

**Example 2.3.** If  $F$  is a field, then the polynomial ring  $F[x]$  is an Euclidean Domain with a norm given by  $N(P(X)) = \text{the degree of } P(x)$ . The Division Algorithm for polynomials is simply "long division" of polynomials which may be familiar with polynomials with the real coefficients. The proof is very similar to that for  $\mathbb{Z}$ . In the order for a polynomial ring to be an Euclidean Domain the coefficients must come from a field since the division algorithm ultimately rests on being able to divide arbitrary nonzero coefficients.

### 3 Principal Ideal Domains (P.I.D.s)

In this section, we shall study the principal ideal domain and we shall study the ideal structure of a ring and we prove that every ED is a PID and give some examples. Additionally, we note that, it is not true that every PID is an ED.

In this section, the results is extract from the references [2, 5].

**Definition 3.1.** Let  $X$  be a subset of a ring  $R$ . Let  $\{A_i \mid i \in I\}$  be the family of all *[left]* ideals in  $R$  which contain  $X$ . Then  $\bigcap_{i \in I} A_i$  is called the *[left]* **ideal generated by  $X$** . This ideal is denoted  $\langle X \rangle$ . The elements of  $X$  are called **generators** of the ideal  $\langle X \rangle$ . If  $X = \{x_1, \dots, x_n\}$ , then the ideal  $\langle X \rangle$  is denoted by  $\langle x_1, x_2, \dots, x_n \rangle$  and said to be **finitely generated**. An ideal  $\langle x \rangle$  generated by a single element is called a **principal ideal**. A **principal ideal ring** is a ring in which every ideal is principal. A principal ideal ring which is an integral domain is called the **principal ideal domain**.

**Proposition 3.1.** Every Euclidean domain is PID.

*Proof.* Let  $R$  be ED and  $I \subseteq R$  be non zero ideal of  $R$ . Let  $a \in I, a \neq 0$  be an element of  $I$  such that  $d(a)$  is minimum in  $I$ . Consider  $I = \langle a \rangle$ , let  $b$  be an arbitray element of  $I$ .

$\because b \in I \subset R$  and  $R$  is ED.

$\therefore \exists q, r$  such that  $b = aq + r$  where either  $r = 0$  or  $d(r) < d(a)$ .

$\because b \in I$  and  $-aq \in I$ .

$\Rightarrow r = b - aq \in I$  from minimality of  $d(a)$  we have  $d(a) < d(r)$ .

Hence  $d(r) \not< d(a)$ .

$\Rightarrow r = 0$ .

$\Rightarrow b = aq$ .

Therefor  $I = \langle a \rangle \quad \because b$  is arbitray element of  $I$ .

Hence every ideal of  $R$  generated by singl element. □

**Proposition 3.2.** Every ideal in an Euclidean Domain is principal. More precisely, if  $I$  is any nonzero ideal in the Euclidean Domain  $R$  then  $I = \langle d \rangle$ , where  $d$  is any nonzero element of  $I$  with minimum norm.

*Proof.* If  $I$  is the zero ideal, there is nothing to prove. Otherwise let  $d$  be any nonzero element of  $I$  of minimum norm (such a  $d$  exists since the set  $\{N(a) \mid a \in 1\}$  has minimum element by the Well Ordering of  $\mathbb{Z}$ ). Clearly

$\langle d \rangle \subseteq I$  since  $d$  is in element of  $I$ . To show the reverse inclusion let  $a$  be any element of  $I$  and use the Division Algorithm to write  $a = qd + r$  with  $r = 0$  or  $N(r) < N(d)$ . Then  $r = a - qd$  and both  $a$  and  $qd$  are in  $I$ . So  $r$  also an element of  $I$ . By the minimality of the norm of  $d$ , we see that  $r$  must be 0. Thus  $a = qd \in \langle d \rangle$  showing  $I = \langle d \rangle$ .  $\square$

**Lemma 3.1.** Let  $\mathbf{R}$  be a ring,  $a \in R$ . The principal ideal  $\langle a \rangle$  consists of all elements of the form

$$ra + as + na + \sum_{i=1}^m r_i a s_i.$$

where  $r, s, r_i, s_i \in R; m \in N^*$ ; and  $n \in Z$ . The term "principal ideal ring" is sometimes used in the literature to denote what we have called a principal ideal domain.

*Proof.* So  $I$  is a left ideal and, similarly, a right ideal. With  $r = s = 0, n = 1, m = 1, r_1 = 0$  we see that  $a \in I$ . Now let  $I'$  be any ideal containing  $a$ . Then  $ra \in I$  and  $r_i a \in I'$  since  $I'$  is a left ideal. So  $as$  and  $r_i a s_i \in I'$  since  $I'$  is a right ideal. Next,  $na \in I'$  since  $I'$  is a subring of  $\mathbf{R}$  (and so is closed under addition). So  $ra + as + na + \sum_{i=1}^m r_i a s_i \in I'$  and  $I \subseteq I'$ . That is a subset of any ideal containing  $a$ , so  $I = \langle a \rangle$ .  $\square$

**Lemma 3.2.** Let  $\mathbf{R}$  be a ring,  $a \in R$ . If  $\mathbf{R}$  has an identity (unity), then

$$\langle a \rangle = \left\{ \sum_{i=1}^n r_i a s_i \mid r_i, s_i \in R; n \in N^* \right\}.$$

*Proof.* If  $\mathbf{R}$  has an identity  $1_R$ , then we write  $ra = ra1_R = r_{m+3} a s_{m+3}$  and so any element of  $\langle a \rangle$  is of the form

$$ra + as + na + \sum_{i=1}^m r_i a s_i = \sum_{i=1}^{m+3} r_i a s_i.$$

$\square$

**Lemma 3.3.** Let  $\mathbf{R}$  be a ring,  $a \in R$ . If  $a$  is in the center of  $R$ , then  $\langle a \rangle = \{ra + na \mid r \in R, n \in Z\}$ .

*Proof.* If  $a$  is in the center of  $\mathbf{R}$  then any element of  $\langle a \rangle$  is of the form

$$ra + as + na + \sum_{i=1}^m r_i a s_i = ra + as + na + \sum_{i=1}^m r_i s_i a$$

$$= \left( r + s + \sum_{i=1}^m r_i s_i \right) + a + na = r'a + na \quad \text{where } r' = r + s + \sum_{i=1}^m r_i s_i.$$

□

**Lemma 3.4.** Let  $\mathbf{R}$  be a ring,  $a \in R$ . If  $R$  has an identity and  $a$  is in the center of  $R$ , then  $Ra = \langle a \rangle = aR$ .

*Proof.* By 3.3,

$$\langle a \rangle = \{ra + na \mid r \in R, n \in \mathbb{Z}\} = \{ra + (n1_R)a \mid r \in R, n \in \mathbb{Z}\}.$$

$$\langle a \rangle = \{ra + na \mid r \in R, n \in \mathbb{Z}\} = \{ra + (n1_R)a \mid r \in R, n \in \mathbb{Z}\}.$$

With  $a$  in the center of  $R$ ,  $r'a = ar'$  and so  $\langle a \rangle = aR$  as well. □

**Lemma 3.5.** Let  $\mathbf{R}$  be a ring,  $a \in R$  and  $X \subset R$ . If  $R$  has identity and  $X$  is in the center of  $R$ , then the ideal  $\langle X \rangle$  consists of all finite sums  $r_1a_1 + \dots + r_na_n$  ( $n \in \mathbb{N}^*$ ;  $r_i \in R$ ;  $a_i \in X$ ).

*Proof.* Let  $R$  have an identity and let  $X$  be in the center of  $R$ . Let  $I$  be an ideal containing  $X$  and let  $a_i \in X$ . Since  $I$  is an ideal containing  $a_i$ , then  $I$  must contain  $\langle a_i \rangle$  (the "smallest" ideal containing  $a_i$ ) and by (v) contains  $Ra_i = \{ra_i \mid r \in R\}$ . Since  $I$  is an ideal, then it is a subring of  $R$  and so contains all  $r_1a_1 + r_2a_2 + \dots + r_na_n$ . Let  $I' = \{r_1a_1 + r_2a_2 + \dots + r_na_n \mid r_i \in R, a_i \in X\}$ , so  $I' \subseteq I$ . For  $r \in R$  and  $r_1a_1 + r_2a_2 + \dots + r_na_n \in I'$  we have  $r(r_1a_1 + r_2a_2 + \dots + r_na_n) = (rr_1)a_1 + (rr_2)a_2 + \dots + (rr_n)a_n \in I'$  so  $I'$  is a left (and since each  $a_i$  is in the center of  $R$ , also a right) ideal of  $R$ . We have now that  $I'$  is an ideal of  $R$  which is a subset of any ideal containing  $X$ . Therefore,  $I' = \langle X \rangle$ . □

**Proposition 3.3.** The ring of integers  $\mathbb{Z}$  is a PID.

*Proof.* Let  $I \triangleleft \mathbb{Z}$ . If  $I = 0$ , then  $I = \langle 0 \rangle$ , so  $I$  is a principal ideal. If  $I \neq 0$  then let  $a$  be the smallest integer such that  $a > 0$  and  $a \in I$ . We will show that  $I = \langle a \rangle$ .

Since  $a \in I$  we have  $\langle a \rangle \subseteq I$ . Conversely, if  $b \in I$  then we have  $b = qa + r$  for some  $q, r \in \mathbb{Z}$ ,  $0 \leq r < a$ . This gives  $r = b - qa$  so,  $r \in I$ . Since  $a$  is the smallest positive element of  $I$ , this implies that  $r = 0$ . Therefore  $b = qa$ , and so  $b \in \langle a \rangle$ . □

**Proposition 3.4.** If  $\mathbb{F}$  is a field then  $\mathbb{F}$  is a PID.

*Proof.* Let  $I \subset F$  be a non-trivial ideal.

Then if  $a \in I$  is nonzero, we have  $1 = a^{-1}a \in I$  where  $a^{-1}$  exist, since  $F$  is a field and  $a \neq 0$ .

Since  $1 \in I$ , for every element  $b \in F, b = b.1 \in I$ , so we have that  $I = F = \langle 1 \rangle$  if  $I \neq \{0\}$ .

In conclusion, the only ideals of a field  $F$  are  $\langle 0 \rangle = \{0\}$  and  $\langle 1 \rangle = F$  which are both principal ideals.  $\square$

**Proposition 3.5.** If  $\mathbb{F}$  is a field then the ring of polynomials  $\mathbb{F}[x]$  is a PID.

*Proof.* We know that  $F[x]$  is an integral domain. Let  $I$  be an ideal. Now if  $I = \{0\}$ , then  $I = \langle 0 \rangle$ , suppose  $I \neq \{0\}$ . Let  $g \in I$  be a nonzero polynomial of minimal degree.

Now, we claim that  $I = \langle g \rangle$ .

Suppose  $f \in I$ . Then by the division algorithm, there are nonzero polynomials  $q$  and  $r$  such that  $f = qg + r$  and either  $r = 0$  or  $\deg(r) < \deg(g)$ . Since  $f, g \in I, r = f - qg \in I$ . Since  $g$  is of minimal degree in  $I$ , we must have  $r = 0$ . Thus  $f = qg \in \langle g \rangle$ .

If  $I \neq \{0\}$  and  $f \in I$  is of minimal degree, then  $f$  is a minimal polynomial of  $I$  and  $I = \langle f \rangle$ .

So,  $F[x]$  is a PID.  $\square$

**Example 3.1.** Example 1 following proposition 1 showed that the quadratic integer ring  $\mathbb{Z}[\sqrt{-5}]$  is not a P.I.D., in fact the ideal  $\langle 3, 1 + \sqrt{-5} \rangle$  is a non principal ideal. It is possible for the product  $IJ$  of the two principals, for example the ideals  $\langle 3, 1 + \sqrt{-5} \rangle$  and  $\langle 3, 1 - \sqrt{-5} \rangle$  are both non principal and their product is the principal ideal generated by 3, i.e.,  $\langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle = \langle 3 \rangle$ .

**Example 3.2.** Integers  $\mathbb{Z}$  are P.I.D.

**Example 3.3.** Polynomial ring  $\mathbb{Z}[x]$  are not a P.I.D because the ideal  $\langle x, 2 \rangle$  we will show  $\langle x, 2 \rangle$  is not principal.

Note that  $\langle x, 2 \rangle \neq \mathbb{Z}[x]$  because  $1 \notin \langle x, 2 \rangle$  because if it were then

$$1 = xf(x) + 2g(x) \quad \forall f(x), g(x) \in \mathbb{Z}[x].$$

But  $xf(x) + 2g(x)$  has even constant term.

Now, suppose  $\langle x, 2 \rangle = \langle p(x) \rangle$  for some  $p(x) \in Z[x]$  then, we must have  $x = p(x)f(x)$  and  $2 = p(x)g(x)$  for some  $f(x), g(x) \in Z[x]$ .

But the second implies that  $p(x)$  must be a constant polynomial as  $p(x) = -2, -1, 1 \text{ or } 2$  we can not have  $p(x) = \pm 1$  as then  $\langle p(x) \rangle = \mathbb{Z}[x]$  so  $p(x) = \pm 2$ , then  $x = \pm 2f(x)$ , a contradiction  $\pm 2f(x)$  has even coefficients.

**Example 3.4.** The ring  $\mathbb{Z}[x]$  is not an Euclidean domain with  $N(p(x)) = \deg p(x)$

There are not  $q(x), r(x) \in Z[x]$  such that either  $r(x) = 0$  or  $\deg r(x) < 1$  and  $x = 2q(x) + r(x)$ .

**Example 3.5.** Let  $R$  be the quadratic integer ring  $\mathbb{Z}[\sqrt{-5}]$ , let  $N$  be the associated field norm  $N(a + b\sqrt{-5}) = a^2 + 5b^2$  and consider the ideal  $I = \langle 3, 2 + \sqrt{-5} \rangle$  generated by 3 and  $2 + \sqrt{-5}$ . Suppose  $I = (a + b\sqrt{-5})$ ,  $a, b \in \mathbb{Z}$ , were principal, i.e.,  $3 = \alpha(a + b\sqrt{-5})$  and  $2 + \sqrt{-5} = \beta(a + b\sqrt{-5})$  for some  $\alpha, \beta \in R$ . Taking norms in the first equation gives  $9 = N(\alpha)(a^2 + 5b^2)$  and since  $a^2 + 5b^2$  is a positive integer it must be 1, 3, or 9. If the value is 9 then  $N(\alpha) = 1$  and  $\alpha = \pm 1$ , so  $(a + b\sqrt{-5}) = \pm 3$ , which is impossible by the second equation since the coefficients of  $2 + \sqrt{-5}$  are not divisible by 3. The value cannot be 3 since there are no integer solutions to  $a^2 + 5b^2 = 3$ . If the value is 1 then  $(a + b\sqrt{-5}) = \pm 1$  and the ideal  $I$  would be the entire ring  $R$ . But then 1 would be an element of  $I$ , so  $3\gamma + (2 + \sqrt{-5})\delta = 1$  for some  $\gamma, \delta \in R$ . Multiplying both sides by  $2 - \sqrt{-5}$  would then imply that  $2 - \sqrt{-5}$  is multiple of 3 in  $R$ , a contradiction. It follows that  $I$  is not a principal ideal and so  $R$  is not an Euclidean Domain (with respect to any norm).

**Remark 3.1.** It is not true that every PID is an Euclidean domain.

## 4 Unique Factorization Domains (U.F.D.s)

In this section, we shall study the unique factorization domain and we prove that every PID is a UFD and give some examples. Also, we note that it is not true that every UFD is a PID.

In this section, the results is extract from the references [2, 7].

**Definition 4.1.** Let  $R$  be a ring with an identity  $1_R$ . An element  $a \in R$  is called a unit if  $\exists b \in R$  s.t  $ab = 1_R = ba$ .



**Definition 4.2.** Let  $R$  be an integral domain, suppose  $r \in R$  is nonzero and not a unit. Then  $r$  is called irreducible in  $R$  if whenever  $r = ab$  with  $a, b \in R$ , at least one of  $a$  or  $b$  must be a unit in  $R$ . Otherwise  $r$  is said to be reducible.

**Definition 4.3.** An ideal  $I$  in a commutative ring  $R$  is called a **prime ideal** if it is a proper ideal, that is,  $I \neq R$ , and  $ab \in I$  implies  $a \in I$  or  $b \in I$ .

**Definition 4.4.** Let  $R$  be an integral domain, the nonzero element  $p \in R$  is called prime in  $R$  if the ideal  $\langle p \rangle$  generated by  $p$  is a prime ideal. In other words, a nonzero element  $p$  is prime if it is not a unit and whenever  $p \mid ab$  for any  $a, b \in R$ , then either  $p \mid a$  or  $p \mid b$ .

**Definition 4.5.** Let  $R$  be an integral domain, two element  $a$  and  $b$  of  $R$  differing by a unit are said to be associated with  $R$  (i.e.,  $a = ub$  for some unit  $u$  in  $R$ ).

**Definition 4.6.** A Unique Factorization Domains (U.F.D.) is an integral domain  $R$  in which every nonzero element  $r \in R$  which is not a unit has the following two properties:

$r$  can be written as a finite product of irreducibles  $p_i$  of  $R$  (not necessarily distinct):  $r = p_1 p_2 \dots p_n$ . The decomposition in (4.6) is unique up to associates. Remark: if  $r = q_1 q_2 \dots q_m$  is another factorization of  $r$  into irreducibles, then  $m = n$  and there are some renumbering of the factors so that  $p_i$  is associated with  $q_i$  for  $i = 1, 2, \dots, n$ .

**Example 4.1.** As we proved in the previous section, every principal ideal domain is a unique factorization domain: thus  $\mathbb{Z}, F[x]$  are unique factorization domains.

**Example 4.2.** The polynomial ring  $\mathbb{Z}[x]$  is a unique factorization domain, even though it is not a principal ideal domain.

**Example 4.3.** The ring  $\mathbb{Z}[\sqrt{-5}]$  is not a unique factorization domain because we can write  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$ . Note that each of  $1 \pm \sqrt{-5}, 2$  and  $3$  is irreducible in  $\mathbb{Z}[\sqrt{-5}]$  since their norms are 6, 4, and 9 respectively and there are no elements in  $\mathbb{Z}[\sqrt{-5}]$  of norm 2 or 3, and none of these elements are associated with one another. Thus, 6 has two inequivalent factorizations into irreducible in  $\mathbb{Z}[2i]$ .

**Example 4.4.** The ring  $\mathbb{Z}[2i]$  is not a unique factorization domain because we can write  $4 = 2 \cdot 2 = (2i) \cdot (2i)$ . Note that both 2 and  $2i$  are irreducible

since their norms are both 4 and there are no elements in  $\mathbb{Z}[2i]$  of norm 2, and 2 and  $2i$  are not associated since  $i \notin \mathbb{Z}[2i]$ . Thus, 4 has two inequivalent factorizations into irreducibles in  $\mathbb{Z}[2i]$ .

**Example 4.5.** The ring  $\mathbb{Z} + x\mathbb{Q}[x]$  of polynomials with rational coefficients and integral constant term is not a unique factorization domain because not every element has a factorization. Explicitly, the element  $x$  are not irreducible since  $x = 2 \cdot \frac{1}{2}x$  and neither 2 nor  $\frac{1}{2}x$  is a unit, but  $x$  cannot be written as a finite product of irreducible element: any such factorization would necessarily consist of a product of constants times and a rational multiple of  $x$ , but no rational multiple of  $x$  is irreducible in  $\mathbb{Z} + x\mathbb{Q}[x]$ .

**Theorem 4.1.** Every PID is a UFD.

*Proof.* Every non-zero non unit can be factored into a product of Irreducibles. It remains to show that such a factorization is unique.

Let,  $p_1 \dots p_m = q_1 \dots q_n$  be two factorizations of a given element into irreducibles. Without loss of generality say  $n \geq m$ .

Since  $p_1$  is irreducible, it is prime. Since  $p_1$  divides the product on the right, and easy introduction shows it divides one of the factors. Again without loss of generality, suppose it divides  $q_1$ .

Now  $q_1 = p_1 a_1$  implies  $a_1$  is a unit, since  $q_1$  is irreducible. Thus,  $p_1$  and  $q_1$  are associates. Replace  $q_1$  with  $p_1 a_1$  and cancel  $p_1$  off both sides, then

$$p_2 \dots p_m = a_1 q_2 \dots q_n.$$

Continuing in this fashion exhausts the  $p$  is, at which point the equation

$$1 = a_1 \dots a_m q_{m+1} \dots q_n.$$

It follows, that  $q_{m+1}, \dots, q_n$  are units, if they are really there. Since they are irreducible, they can not be units, so they are not there. This proves  $m = n$ , and the rearranging done during the proof proves the claim about associates.

□

**Remark 4.1.** It is not true that every UFD is a PID.

## 5 Tensor Product

In this section, we shall study the importance of tensor product and we study ED, PID and UFD on tensor product. Also, this article is over the integers  $Z$ .

In this section, the results is extract from the references [1, 4–6].

**Theorem 5.1.** Let  $I$  and  $J$  be two ideals in a  $PID$  of  $R$ . Determine

$$R/I \otimes_R R/J.$$

*Proof.* Given that  $R$  is a ring. Now we know that if  $I$  is an ideal of  $R$  then the tensor product of  $R/I \otimes_R M \cong M/IM$ , where  $M$  is a left  $R$ -module, then

$$\begin{aligned} \frac{R}{I} \otimes \frac{R}{J} &\cong \frac{R/J}{I(R/J)} \\ &\cong \frac{R/J}{\frac{I+J}{J}} \\ &\cong \frac{R}{I+J} \end{aligned} \quad \text{By isomorphic law.}$$

□

**Remark 5.1.**  $I \left( \frac{R}{J} \right) = \frac{(I+J)}{J}$ .

Now what we know by  $I \left( \frac{R}{J} \right)$ , it is nothing but an ideal of  $\left( \frac{R}{J} \right)$  which is spanned by  $I$ . it can write as  $\{ \sum i a_i c_i + J \}$  where  $a_i \in I$  and  $c_i \in R$ . (1)  
Because it is an quotient ring, now as  $I$  is ideal of  $\frac{R}{J}$  so it is ideal for  $R$  also equation 1 is nothing but ideal  $I$  itself and  $J$  also in  $R$ .

**Remark 5.2.**  $I+J$  is an ideal and  $R$  is  $PID$  then  $I+J$  generated by a single element.

**Lemma 5.1.** Let  $R$  be a commutative ring. Let  $I$  be an ideal of  $R$ . Suppose  $R/I$  is Noetherian and every ideal contained in  $I$  is finitely generated. Then  $R$  is Noetherian.

**Lemma 5.2.** Let  $R_1$  and  $R_2$  be two Noetherian rings, then  $R_1 \otimes_Z R_2$  is also Noetherian.

*Proof.* Let  $\psi : R_1 \otimes_Z R_2 \longrightarrow R_2$  be the projection. Let  $I$  be the kernel of  $\psi$ . It is easy to see that  $\psi$  and  $I$  satisfy the lemma. Therefore,  $R_1 \otimes_Z R_2$  is Noetherian. □

**Remark 5.3.** Every Noetherian is P.I.D.

**Proposition 5.1.** Let  $R_1$  and  $R_2$  be two P.I.D, then  $R_1 \otimes_Z R_2$  is P.I.D.

*Proof.* Let  $I$  be an ideal of  $R_1 \otimes_Z R_2$ . By 5.2 of the lemma,  $I$  is finitely generated, let  $(a_1, b_1), \dots, (a_n, b_n)$  be generators of  $I$ , since  $R_1$  is a principal ideal ring,  $\exists c \in R$  such that  $cR_1$  is the ideal generated by  $a_1, \dots, a_n$  similarly  $\exists d \in R_2$  such that  $dR_2$  is the ideal generated by  $b_1, \dots, b_n$ . Since every element of  $I$  is of the form  $\sum_i (x_i, y_i)(a_i, b_i) = (\sum_i x_i a_i, \sum_i y_i b_i) = (c, d)$ . Hence  $R_1 \otimes_Z R_2$  is PID. □

**Proposition 5.2.** Let  $M$  be an  $R$ -module and  $R$  is an identity in tensor product. Then

$$R \otimes_R M \cong M.$$

*Proof.*  $\psi : R \times M \longrightarrow M$ .

$$\psi : (r, m) = rm \in M, \quad \forall r \in R, \forall m \in M.$$

We want to prove  $\psi$  is a middle linear map

•

$$\begin{aligned} \psi(r_1 + r_2, m) &= (r_1 + r_2)m \\ &= r_1m + r_2m \\ &= \psi(r_1, m) + \psi(r_2, m). \end{aligned}$$

•

$$\begin{aligned} \psi(r, m_1 + m_2) &= r(m_1 + m_2) \\ &= rm_1 + rm_2 \\ &= \psi(r, m_1) + \psi(r, m_2). \end{aligned}$$

•

$$\begin{aligned}
\psi(rr_1, m) &= (rr_1)m \\
&= r(r_1m) \\
&= \psi(r, r_1m).
\end{aligned}$$

$\therefore \psi$  is a middle linear map. Thus there exists a unique group homomorphism.

$$\phi : R \otimes M \longrightarrow M.$$

$$\phi(r \otimes m) = rm, \forall r \in R, \forall m \in M.$$

We want to prove  $\phi$  is isomorphism.

$$\text{Ker}\phi = \{r \otimes m \in R \otimes M : \phi(r \otimes m) = 0_m\}.$$

$$= \{r \otimes m \in R \otimes M : rm = 0_m\}.$$

But

$$\begin{aligned}
r \otimes m &= r \otimes m.1 \\
&= rm \otimes 1 \\
&= 0 \otimes 1 \\
&= 0
\end{aligned}$$

$$\therefore \text{Ker}\phi = 0.$$

$$\text{Let } y \in M \Rightarrow y = am = \phi(a \otimes m).$$

$\therefore \phi$  is injective and surjective.

$\phi$  is isomorphism.

$$R \otimes_R M \cong M.$$

□

**Remark 5.4.** The above result says that the ring  $R$  is the identity of the operation of tensor product in the category of  $R$ -modules.

**Proposition 5.3.** If  $M$  is finite dimensional module over  $R$  i.e.  $M$  has a basis then

$$M^* \otimes_R N \cong \text{Hom}_R(M, N).$$

*Proof.* Define bilinear map  $\phi : M^* \otimes_R N \longrightarrow \text{Hom}(M, N)$  by  $\phi(\varepsilon, n) : m \longmapsto \varepsilon(m)n$ , this bilinear map defines a linear map  $f : M^* \otimes_R N \cong \text{Hom}_R(M, N)$  by  $f(\varepsilon \otimes_R n) = \phi(\varepsilon, n)$ . (i)

Let  $\dim M = n, \{e_1, e_2, \dots, e_n\}$  is a basis of  $M$  then we define  $g : \text{Hom}_R(M, N) \longrightarrow M^* \otimes_R N$  by  $g(u) = \sum_{i=1}^n e_i^* \otimes u(e_i)$ . (ii)

Clearly,  $g$  is  $R$ -module homomorphism. Now, we shall show  $f$  and  $g$  all inverse to each other.

Let  $u : M \longrightarrow N$  such that  $u \in \text{Hom}_R(M, N)$

$$\begin{aligned}
 f(g(u))(m) &= f\left(\sum_{i=1}^n (e_i^* \otimes u(e_i))\right)(m) \\
 &= \sum_{i=1}^n f(e_i^* \otimes u(e_i))(m) \\
 &= \sum_{i=1}^n \phi(e_i^*, u(e_i))(m) \\
 &= \sum_{i=1}^n e_i^*(m)u(e_i) \\
 &= u\left(\sum_{i=1}^n e_i^*(m)e_i\right) \\
 &= u(m).
 \end{aligned}$$

.

Because  $m \in M \Rightarrow m = d_1e_1 + \dots d_ne_n = \sum_{i=1}^n d_ie_i \Rightarrow e_i^*(m) = d_i$ .

Hence  $m = \sum_{i=1}^n e_i^*(m)e_i$ ; cosequently  $fg(u) = u$ .

Let  $\varepsilon \otimes n \in M^* \otimes_R N, g(f(\varepsilon \otimes n))$

$$\begin{aligned}
 &= g(\phi(\varepsilon, n)) \quad \text{by (i)} \\
 &= \sum_{i=1}^n e_i^* \otimes \phi(\varepsilon, n)(e_i) \quad \text{by (ii)} \\
 &= \sum_{i=1}^n e_i^* \otimes \varepsilon(e_i)(n) \\
 &= \sum_{i=1}^n \varepsilon(e_i)e_i^* \otimes n \\
 &= \varepsilon \otimes n.
 \end{aligned}$$

And so  $f$  and  $g$  are inverse of each others, hence  $f$  is an isomorphism, hence  $M^* \otimes_R N \cong \text{Hom}_R(M, N)$ .

□

**Remark 5.5.** In general the above proposition is not true i.e.  $M^* \otimes_R N \not\cong$

$Hom_R(M, N)$ .

**Proposition 5.4.** Let  $V$  and  $W$  be vector spaces over a field  $K$ . In case  $V$  is finite dimensional, the map

$$\Phi : W^* \otimes_K V \longrightarrow Hom_k(W, V).$$

$$\alpha \otimes v \{ \longmapsto W \longrightarrow V, w \longmapsto \alpha(w)v \}.$$

Is a monomorphism and its image is

$$Hom_k^{fin}(W, V) = \{ \varphi \in Hom_k(W, V) | \dim_K \varphi(W) < \infty \}.$$

The  $K$ -vector space of finite dimensional  $K$ -homomorphisms  $W \longrightarrow V$ .

*Proof.* The map  $w \longmapsto \varphi(w)v$  defines an element of  $Hom_k^{fin}(W, V)$ , whence  $\Phi$  is well-defined and its image is contained in  $Hom_k^{fin}(W, V)$ . Moreover,  $\Phi$  is a homomorphism.

Let  $x = \sum_{i=1}^n \alpha_i \otimes v_i \in W^* \otimes V$  with  $\Phi(x) = 0$ , i.e. with  $\sum_{i=1}^n \alpha_i(w)v_i = 0 \ \forall w \in W$ . Without loss of generality, we can assume that our representation of  $x$  satisfies that the  $v_i$  are linearly independent. In that case  $\sum_{i=1}^n \alpha_i(w)v_i = 0$  implies  $\alpha_i(w) = 0 \ \forall i$ . But since this is true for all  $w \in W$ , it follows that  $\alpha_i = 0 \ \forall i$ . But then,  $x = 0$ . Therefore,  $Ker \Phi = 0$ , whence  $\Phi$  is injective.

Now let  $\varphi \in Hom_k^{fin}(W, V)$ , and let  $(v_1, \dots, v_n)$  be a basis of  $\varphi(W)$ .

Let  $\pi_i : \varphi(W) \longrightarrow K$  be the projection with  $\pi_i(v_i) = 1$  and  $\pi_i(v_j) = 0$  for  $i \neq j$ . Set  $\alpha_i = \pi_i \circ \varphi$ . Then  $\varphi(w) = \sum_{i=1}^n \alpha_i(w)v_i \ \forall w \in W$  since  $v = \sum_{i=1}^n \pi_i(v)v_i \ \forall v \in \varphi(W)$ ; Therefore,  $\varphi = \Phi(\sum_{i=1}^n \alpha_i \otimes v_i)$ . Hence  $Hom_k^{fin}(W, V) \subseteq \Phi(W^* \otimes_K V)$  whence we have equality.  $\square$

**Remark 5.6.** It is not true in general that: the dual space is the inverse of the space under the operation of tensor product.

**Acknowledgements.** I would like to mention that this report is the output of my research project of my first course of algebra in my current study of Master degree at Umm Al-qura university(UQU). I would like to thank my teacher in that course Prof. Dr. Ahmad M. Alghamdi for his support and encouragements regarding this report.

## References

- [1] K. Conrad, *Tensor product*,  
<https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod.pdf>
- [2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, vol. 3, John Wiley & Sons, 2004.
- [3] J. R. Durbin, *Modern Algebra. An Introduction*, John Wiley & Sons, 2008.
- [4] F. Fontein, *Homomorphisms, tensor products and certain canonical maps*, <https://math.fontein.de/2010/01/29/homomorphisms-tensor-products-and-certain-canonical-maps/>
- [5] Th. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
- [6] J. Pakianathan, *Chain conditions*,  
<https://web.math.rochester.edu/people/faculty/jonpak/N13.pdf>
- [7] J. J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 1st edition, 2002.

**Received: August 18, 2020; Published: September 25, 2020**