International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 05 May-2026 | Impact Factor: 3.5

"A brief study of Unique factorization domain in Integral Domain"

Dr. Amrish Kumar Srivastav
Assistant Professor
Department of Mathematics
Araria College, Araria
Email id – amrish112233@gmail.com

How to Cite this Article:

Srivastav, A. K. (2026). "A brief study of Unique factorization domain in Integral Domain". International Journal of Creative and Open Research in Engineering and Management, 02(05). https://doi.org/10.55041/ijcope.v2i5.561

https://doi.org/ 10.55041/ijcope.v2i5.561

Abstract

Unique Factorization Domains (UFDs) are integral domains where every non zero non unit element can be factored into irreducible elements in a manner that is unique, considering order and units. This idea extends the Fundamental Theorem of Arithmetic from integers to more abstract algebraic structures. This paper offers a comprehensive examination of UFDs within integral domains, covering definitions, equivalent characterizations, significant theorems, examples, counter examples and their connections to principal ideal domains and Euclidean domains. Additionally, applications in algebraic number theory and polynomial theory are explored.

Keywords: Integral domains, Euclidean, ideal domains

Introduction

In commutative algebra, factorization of elements into irreducible is a fundamental concept. While integers exhibit unique factorization into primes, this property does not always hold in general integral domains.
A Unique Factorization Domain (UFD) is an integral domain in which every nonzero nonunit element can be written uniquely (up to order and units) as a product of irreducible elements.
UFDs are especially important in: Algebraic number theory, where failure of unique factorization leads to the dvelopment of ideal theory. Polynomial theory, where polynomial rings over fields preserve unique factorization.

The study of factorization lies at the heart of number theory and algebra. In the integers, every number greater than 1 is in factors uniquely into primes. When extending arithmetic to general algebraic structures specifically integral domains this property may or may not persist.

An integral domain is a commutative ring with unity and no zero divisors. Within such domains, the question arises: When does unique factorization into irreducible hold? The answer leads to the notion of a Unique Factorization Domain (UFD), a fundamental structure in commutative algebra.

We know that every integer $n > 1$ can be uniquely expressed as product of primes and in a principal ideal domain an element is prime if and only if it is irreducible. Thus, we can say that integer $n > 1$, can be uniquely expressed as product of irreducible. The next question that arises is whether every integral domain has this property or not? It can be under stand by steps given below.

Factorization theory is a central topic in commutative algebra and number theory. The classical Fundamental Theorem of Arithmetic states that every integer greater than 1 can be uniquely expressed as a product of primes. Unique Factorization Domains generalize this property from the integers to more general algebraic structures called integral domains.

An integral domain is a commutative ring with identity and no zero divisors. In such structures, divisibility can be studied similarly to integers, but uniqueness of factorization may fail in general.

Definition:

An integral domain R is said to be a unique factorization domain (U.F.D) if,

1- Every non-zero, non-unit element of R can be expressed as a product of irreducible elements in R.

2- The factorization into irreducible is unique up to associates and the order in which the factors appear.

In other words, if $a = p_1{}^{n1}\ p_2{}^{n2} \dots p_r{}^{nr} = q_1{}^{m1}\ q_2{}^{m2} \dots p_s{}^{ms}$ be two factorizations of an element $a \in R$ as a product of irreducible, where no two $p_i\ 's$ are associates and no two $q_j\ 's$ are associates, then $r = s$ and each p_i is an associate of one and only one q_j .

Example1: Show that the ring $\mathbb{Z}$ of integers is a unique factorization domain (U.F.D).

Solution: Note that the only units in $\mathbb{Z}$ are ± 1

If $n \in \mathbb{Z}$ is non-zero and non-unit, then either $n > 0$ or $n < 0$

If $n > 0$.Then by fundamental theorem of arithmetic, can be uniquely expressed as $n = p_1{}^{k1}\ p_2{}^{k2}\ p_3{}^{k3} \dots p_m{}^{km}$ where $p_i\ 's$ are prime.

$$\Rightarrow n = (p_1 p_1 \dots p_1) \dots (p_m\ p_m \dots p_m)$$

Since $\mathbb{Z}$ is a P.I.D and we know that in a P.I.D, an element is prime iff it is irreducible.

Hence, n is uniquely expressed as product of irreducible elements.

If $n < 0$, then $n = -m$, for some $m > 0$

As in case of $n > 0$, m can be expressed uniquely as product of irreducible elements.

Let $m = q_1 q_2 \dots q_k$

Then, $n = -m = -q_1\, q_2 \dots\dots\dots\dots\dots q_k$

As $q_1 = (-1)\ (-q_1))$, where -1 is unit.

Therefore $-q_1$ and q_1 are associates and we know that associate of an irreducible is irreducible, so q_1 is irreducible.

Theorem 1: Every principal ideal domain is a unique factorization domain.

Proof: Let R be a principal ideal domain and $a_0 \in R$ be a non-zero, non-unit element of R.

1- We claim that a_0 can be written as a product of irreducible elements in R.

If a_0 is irreducible, then $a_0 = a_0$ and we get the result.

Suppose that a_0 is not irreducible.

Then as $_0$ is non-zero, non-unit element, therefore by Theorem if be a principal ideal domain and $a \in R$ is a non-zero, non-unit element then there exists an irreducible element p such that $p \mid a.$, there exists an irreducible element p_1 such that $p_1 \mid a_0$.

$\Rightarrow a_0 = p_1 a_1$, for some $a_1 \in R$.

$\Rightarrow < a_0 > \subseteq < a_1 >$

If a_1 is irreducible, then we have expressed a_0 as a product of irreducible elements in R.

If a_1 is not irreducible, then $a_1 \neq 0$

Then $a_0 =$ $_1$. a_1

$= p_1 . 0$

$= 0$, which is not true.

Also a_1 is non-unit, because if a_1 is unit then a_1 and $_1$ are associates and as p_1 is irreducible therefore a_1 is irreducible which is also not true.

Hence a_1 is a non-zero, non-unit element of R which is a principal ideal domain.

By theorem if R be a principal ideal domain and $a \in R$ is a non-zero, non-unit element, then there exists an irreducible element p such that $p \mid a$. There exists an irreducible element p_2 such that $_2 \mid a_1$.

$\Rightarrow a_1 = p_2 a_2$, for some $a_2 \in R$

$\Rightarrow < a_1 > \subseteq < a_2 >$

If a_2 is irreducible, then $a_0 = a_1 p_1$

$= p_2 a_2 p_1$

which is a finite product of irreducible elements and we are done.

If a_2 is not irreducible, then proceeding as above, it can be seen that a_2 is non-zero and non-unit in R.

Continuing like this we obtain an ascending chain of ideals

$< a_0 > \subseteq < a_1 > \subseteq < a_2 > \subseteq \cdots$

Then by theorem if R be a principal ideal domain and $A_1 \subset A_2 \subset \cdots$ be any strictly increasing chain of ideals in R. Then this chain of ideals must be of finite length, Therefore there exists an irreducible element $an \in R$ such that

$< a_0 > \subseteq < a_1 > \subseteq < a_2 > \subseteq \cdots \subseteq < a_n >$

and $a_0 = p_1 p_2 \ldots p_n a_n$ where $p_1, p_2, \ldots, p_n, an$ are irreducible elements in R.

Thus, Claim 1 holds.

2- Now we claim that the factorization is unique up to associated and the order in which they appear.

In order to prove this, we have to show that if $a \in R$ is non-zero, non-unit element and $a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ are two representations of a as product of irreducible then $m = n$ and each p_i is an associate of some q_j

We prove this by using induction on n.

For $n = 1$, $a = p_1 p_2 \ldots p_m = q_1$ …(1)

As q_1 is irreducible, some pi must be unit. But each p_i being irreducible cannot be unit. Therefore, (1) holds only if $m = 1$

Thus, $a = p_1 = q1$ and $p_1 = 1 . q_1$

This implies that p_1 and q_1 are associates.

Hence the result holds for $n = 1$

Let the result be true for $n - 1$

As $a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$

$\Rightarrow p_1 p_2 \ldots p_m = q_1 (q_2 \ldots q_n)$.

$\Rightarrow q_1 \mid p_1 p_2 \ldots p_m$ …… (2)

As q_1 is irreducible in R which is a principal ideal domain and we know that in a principal ideal domain an element is prime if and only if it is irreducible.

Therefore q_1 is prime element.

(2) $\Rightarrow q_1 \mid p_i$ for some i

Since R is a commutative ring, we can assume without loss of generality that $i = 1$

$\Rightarrow q_1 \mid p_1$

$\Rightarrow p_1 = q_1u_1$ for some $u_1 \in R$
As p_1 is irreducible, therefore either q_1 is unit or u_1 is unit.
But q_1 being irreducible is non-unit therefore u_1 must be unit.
$\Rightarrow p_1$ and q_1 are associates.
As $p_1 p_2 \dots p_m = q_1(q_2 \dots q_n)$ and $p_1 = q_1u_1$
$\Rightarrow (q_1u_1)\, p_2 \dots p_m = q_1q_2 \dots q_n$
$\Rightarrow u_1 p_2 \dots p_m = q_2q_3 \dots q_n$
(as $q_1 \neq 0$ and cancellation law holds in an integral domain for non-zero elements).
$\Rightarrow p_2'p_3 \dots p_m = q_2q_3 \dots$, where $p_2' = u_1p_2$ is irreducible. …..… (3)
Because p_2 is irreducible, u_1 is unit which implies that p_2' and p_2 are associates and associate of an irreducible element is irreducible, therefore p_2' is irreducible.
In (3), we have two equal representations as a product of irreducible and one of the representation on R.H.S. contains $(n-1)$ elements.

Therefore, by induction hypothesis, on L.H.S. also we should have $(m-1)$ elements.

Therefore, $n-1 = m-1 \Rightarrow m = n$
Also we have seen above that p_1 and q_1 are associates.
Similarly, we can show that p_2 and q_2 are associates by considering
$p_1p_2 \dots p_m = q_2(q_1q_3 \dots q_n)$,and proceeding as above.
In this manner, we can see that each p_i is an associate of some .

Therefore, by Principle of mathematical induction result holds for every n. Hence, Claim 2 holds.

Thus, from Claim 1 and 2, it follows that R is a unique factorization domain.

Applications of Unique factorization domain

UFD properties are used in:

- Algebraic number theory
- Cryptography and Computation
- Polynomial factorization algorithms
- Computer algebra systems
- Error-correcting codes
- Algebraic Geometry - Coordinate rings of varieties often require factorization properties for structural analysis.

Conclusion

Unique Factorization Domains (UFDs) offer a significant extension of the concept of integer factorization to the realm of abstract algebraic structures. Established within integral domains, UFDs guarantee that each element can be uniquely decomposed into irreducible factors, thereby maintaining a crucial arithmetic framework. Although numerous significant rings qualify as UFDs, notable exceptions expose more profound algebraic insights that inspire the development of ideal theory and contemporary commutative algebra.

References:

- Abstract Algebra written by David S. Dummit, Richard M. Foote, ISBN: 978-0471433347, Pages: 253–280
- A First Course in Abstract Algebra written by John B. Fraleigh, ISBN: 978-0201763904, Pages: 243–265
- Algebra written by Michael Artin, ISBN: 978-0130047632, Pages: 199–220
- Topics in Algebra written by I.N. Herstein, ISBN: 978-8129702323, Pages: 140–160
- Introduction to Commutative Algebra written by M. F. Atiyah, I. G. Macdonald, ISBN: 978-0201407518, Pages: 1–20