

A Study on Unique Factorization an Integral Domain

M.Phil.Scholar Suja Joseph

Department of Mathematics
Prist University, Thanjavu
Tamil Nadu,India

Dr.B.Senthil Kumar

Department of Mathematics
Prist University, Thanjavur
Tamil Nadu,India

Abstract – We take a broad view the notion of “unique factorization domain” in the spirit of “half-factorial domain”. We show that new generalization of UFD implies the now well known notion of half factorial domain. As a consequence, we discover that the one of the normal axioms for unique factorization domains is union scientiouslyred undant.That is, we interested in factoring numbers in integral domains so we have to scrutinize distribution, and so this post will begin with a fairly cursory look at the properties of distribution. Then we will introduce the crucial ideas of units and associates. (In the integers, ± 1 are units and $\pm n$, for any fixed n , are associates.)

Key words- UFD, Integral Domain, integer number etc.

I. INTRODUCTION

The notion of unique factorization is one that is central in the study of commutative algebra. A unique factorization domain (UFD) is an integral domain, R , where every nonzero non unit can be factored uniquely. More formally we record the following standard definition. Integral domains in general, but integral domains that are not unique factorization domains (UFDs) in particular. We interested in the outer ring of that diagram.

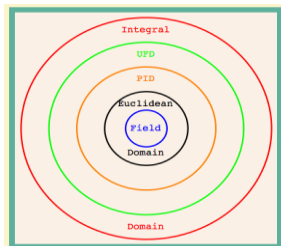


Fig.1 Ven Diagram of Integral Domain

Definition 1

Integral domain is irreducible over F field but reducible over ID Suppose that D is an integral domain and F is a field containing ID. If $g(x) \in ID[x]$ and $g(x)$ is irreducible over G but reducible over ID. This doesn't make sense to me, how can $ID \subseteq G$ and be irreducible in F but reducible in ID. The same polynomials in ID are in G , so any polynomial product representation of G is irreducible.

Example 1 We learning about Rings, commutative rings, IDs, UFDs, etc with each being a subset of the predecessor, and now we find an ID that is not a UFD

A certain integral domain is not a unique factorization domain We to prove the following: R is an ID and let F be its field of fractions. Suppose there exists a monic $p(x) \in R[x]$ such that $p(x) = a(x)b(x)$ where both a, b are monic and non constant polynomials of $F[x]$ but $a \notin R[x]$. Then I need to show that R is not a UFD.

Theorem 1 Let R be an integral domain. Every prime element is irreducible.

Proof. Let p be a prime element. We assume that p is reducible and we want to get a contradiction. This mean that we can write $p = ab$ where p is not associate to neither a , nor b . I notice that p/ab . Since p is a prime, this means that p/a or p/b . Without loss of generality I will assume that p/a . But now we have that p/a and also a/p . This means p and a are associate. Contradiction.

Example. 2 The converse is not true in general. As an example, consider the ring $z[\sqrt{-5}]$. The element 2 is irreducible in R . However,

$$2/6 = (1 + \sqrt{-5})i(1 - \sqrt{-5})i$$

But 2 dose not divide $[1 + \sqrt{-5}i]$ and dose not divide $[1 - \sqrt{-5}i]$. Hence 2 is not a prime.

Theorem 2 Let R be a domain in which every irreducible element is prime. Then the decomposition of an element as product of irreducible, if it exists, is unique. (Notice that this is not enough to conclude that R is a UFD, since the decomposition as product of irreducible may not exist.)

Proof Let's assume that we have two different decompositions where all p_i and q_j are irreducible. We want to prove that these two decompositions are the same, upto reordering and associates. Now we will proceed by induction on the maximum of n and m . For the base case, if $n = m = 1$, we have $P_1 = Q_1$ and we do not need to do anything.

Theorem 3 Let R an integral domain. Assume that x contains an element that is not 0, not a unit, and cannot be written as product of irreducible. Then there exists an infinite sequence

$$X_0, X_1, \dots, X_N \text{ of elements in } R \text{ such that } (X_0) \subset (X_1) \subset (X_2) \subset (X_3) \dots \text{ where all the inclusions are strict.}$$

Proof For elements in R , we know that x is a unit iff $(x) = R$. We know that x and y are associates. Iff $(x) = (y)$.

Moreover, if we can factor $x = yz$ non-trivially (so that y and z are neither units, nor associates to x), then $(x) \subset (y)$ and $(x) \subset (z)$. Pick an element $x \in R$ which is not zero, not a unit, and not the product of irreducible. Call $x_0 = x$. Since x is not a product of irreducible, in particular it is not irreducible, so we have a non-trivial factorization $x = yz$. At least one of y or z is also not a product of irreducible.

Whichever it is, call it x_1 . Repeat

Theorem 4. S is a saturated multiplicatively closed set.

Proof If $x, y \in S$ then we can write both x and y as product of primes, so xy can be also written as product of primes. This shows that S is a multiplicatively closed set.

Now, to prove that S is saturated we have to show that if $x \in S$, then every divisor of x is in S too. If we write $x = up_1 up_2 \dots up_n$ where u is a unit and the p_i 's are prime, then it can be shown by induction on n

$$\Rightarrow (A \cap X_i) \subseteq X_i$$

that every divisor of x is in S . I let you to do this proof by induction.

Now, we argue by contradiction assuming that there is a nonzero element $a \in R$ such that $a \notin S$, so the ideal generated by a , $\langle a \rangle$, is disjoint from S , i.e., $S \cap \langle a \rangle = \emptyset$, because if there were some $ra \in S$, then a would be in S (because $a | ra$ and S is saturated by the lemma above), contradicting our hypothesis that $a \notin S$.

Therefore the set $A = \{I \text{ non zero ideal of } R : I \cap S = \emptyset\}$ is non-empty and then by Zorn's Lemma A has a maximal element P such that P is not only an ideal, but in fact a prime ideal. By our general hypothesis P contains a prime element, let's say p , i.e., $p \in P$, but by the definition of S is clear that $p \in S$, so $p \in P \cap S$, which contradicts $P \cap S = \emptyset$.

This contradiction comes from our assumption that $a \notin S$. Hence every nonzero $a \in R$ belongs to S , i.e., $S = R \setminus \{0\}$ and this means that every nonzero, non unit element of R is expressible as a product of primes.

II. SUMMARY

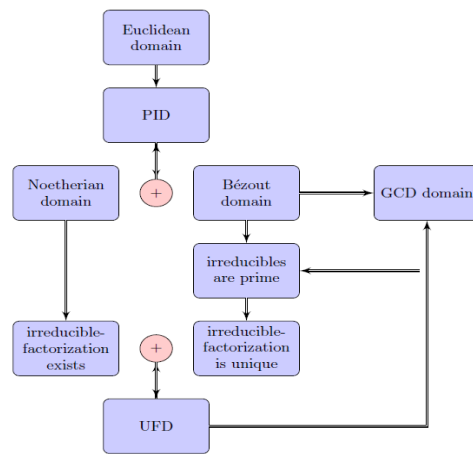


Fig.2 Function Diagram

III. MOTIVATION

We know that every integer number is the product of prime numbers in a unique way. Sort of. We just believed our kinder garden teacher when she told us, and we omitted the fact that it needed to be proven. We want to prove that this is true, that something similar is true in the ring of polynomials over a field. More generally, in which domains is this true? In which domains does this fail?

REFERENCES

- [1]. D.D. Anderson, D.F. Anderson and M. Zafrullah, Factorization in integral domains. *Journal of Pure and Applied Algebra* 69 (1990), 1-19.
- [2]. M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
- [3]. M. Auslander and D.A. Buchsbaum, Unique factorization in regular local rings. *Proc. Nat. Acad. Sci. U.S.A.* 45 1959 733{734.
- [4]. Baker, Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika* 13 (1966), 204-216; *ibid.* 14 (1967), 102-107; *ibid.* 14 1967 220{228.
- [5]. S. Borofsky, Factorization of polynomials. *Amer. Math. Monthly* 57, (1950), 317{320.
- [6]. Bouvier, Le groupe des classes de l'algebra d'une forme quadratique. *Publ. D'ep. Math. (Lyon)* 15 (1978), no. 3, 53{62.
- [7]. E.S. Barnes and H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms. I. *Acta Math.* 87, (1952). 259{323.
- [8]. D.A. Buchsbaum, Some remarks on factorization in power series rings. *J. Math. Mech.* 10 1961 749{753.
- [9]. E.D. Cashwell and C.J. Everett, The ring of number-theoretic functions. *Pacific J. Math.* 9 (1959) 975{985.

- [10]. D.A. Clark, A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* 83 (1994), no. 3-4, 327-330
- [11]. P.M. Cohn, Bézout rings and their subrings. *Proc. Cambridge Philos. Soc.* 64 (1968) 251-264
- [12]. P.M. Cohn, Unique factorization domains. *Amer. Math. Monthly* 80 (1973),
- [13]. D.A. Cox, Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.
- [14]. D. Eisenbud *Commutative algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics*, 150. Springer-Verlag, New York, 1995
- [15]. Euclid, The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III-IX. Vol. III: Books X-XIII and Appendix. Translated with introduction and commentary by Thomas L. Heath. 2nd ed. Dover Publications, Inc., New York, 1956.
- [16]. R.M. Fossum, The divisor class group of a Krull domain. *Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74*. Springer-Verlag, New York-Heidelberg, 1973