

A Note on Non-Unique Factorization Domains (UFD)

Dorel Mihet
 West University of Timisoara,
 Faculty of Mathematics and
 Computer Science
 Bv. V parvan 4, 300223
 Timisoara, Romania.
 Email: mihet@math.uvt.ro

In the paper ‘On GCD and LCM in Domains – A Conjecture of Gauss’ in *Resonance* [1], some elegant proofs for the fact that $\mathbb{Z}[\sqrt{-d}]$ ($d \geq 3$, square-free) is not a UFD are given. The aim of this note is to provide an alternative proof for this theorem.

1. Introduction

A unique factorization domain (UFD) is an integral domain in which every non-zero non-unit element can be written in a unique way, up to associates, as a product of irreducible elements. As in the case of the ring of rational integers, in a UFD every irreducible element is prime and any two elements have a greatest common divisor as well as a least common multiple.

It is well known that if d is a square-free rational integer, then the subring $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$ is a unique factorization domain only if d is 1 or 2. Some questions regarding this theorem are nicely discussed in [1]. Here we provide alternative proofs for some results in the above quoted paper of Khurana. For further information on the subject, the interested reader is referred to the recent papers [1,2].

2. Main Results

We give a simple proof of the fact that the element 2 in $\mathbb{Z}[\sqrt{-d}]$ ($d \geq 3$, square-free), although irreducible, is not prime. This proves that if $d \geq 3$ is a square-free integer, then $\mathbb{Z}[\sqrt{-d}]$ is not a UFD.

Proof. Let $u_1, v_1, u_2, v_2 \in \mathbb{Z}$ be such that

$$2 = (u_1 + iv_1\sqrt{d})(u_2 + iv_2\sqrt{d}).$$

Keywords

Factorization domains, unique factorization domains.



In a domain, an irreducible element need not be a prime, but a prime is always irreducible.

Then $N((u_1 + iv_1\sqrt{d})(u_2 + iv_2\sqrt{d})) = 4$, that is,

$$(u_1^2 + dv_1^2)(u_2^2 + dv_2^2) = 4.$$

If neither $u_1 + iv_1\sqrt{d}$ nor $u_2 + iv_2\sqrt{d}$ is a unit, then $u_1^2 + dv_1^2 \neq 1$ and $u_2^2 + dv_2^2 \neq 1$, that is, $u_1^2 + dv_1^2 = 2$. Thus we are led to a contradiction, by noting that $v_1 = 0 \Rightarrow u_1^2 = 2$ and $v_1 \neq 0 \Rightarrow u_1^2 + dv_1^2 \geq d > 2$.

Hence, 2 is irreducible in $\mathbb{Z}[\sqrt{-d}]$.

Let a be a rational integer such that a and d have the same parity. Then a^2 and d have the same parity; hence 2 divides

$$a^2 + d = (a + i\sqrt{d})(a - i\sqrt{d}).$$

On the other hand, since $\frac{a}{2} + \frac{1}{2}i\sqrt{d}$ and $\frac{a}{2} - \frac{1}{2}i\sqrt{d}$ are not in $\mathbb{Z}[\sqrt{-d}]$, 2 does not divide either of $a + i\sqrt{d}$ and $a - i\sqrt{d}$, concluding that 2 is not a prime in $\mathbb{Z}[\sqrt{-d}]$.

In the next proposition we identify pairs of elements in $\mathbb{Z}[\sqrt{-d}]$ which do not have a GCD (this also proves that $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ square-free, is not a UFD).

Proposition 2.1 *Let a be any rational integer such that $a \equiv d \pmod{2}$ and let $a^2 + d = 2q$. Then the elements $2q$ and $(a + i\sqrt{d})q$ do not have a GCD.*

Proof. Since 2 is an irreducible element in $\mathbb{Z}[\sqrt{-d}]$ and 2 does not divide $a + i\sqrt{d}$, every common divisor of 2 and $a + i\sqrt{d}$ is a unity of $\mathbb{Z}[\sqrt{-d}]$, that is

$$(2, a + i\sqrt{d}) = 1.$$

Now, if $(2q, (a + i\sqrt{d})q)$ did exist, then $(2q, (a + i\sqrt{d})q) = q$. Then, as $a + i\sqrt{d}$ divides both $a^2 + d = (a + i\sqrt{d})(a - i\sqrt{d})$ and $(a + i\sqrt{d})q$, it follows that $a + i\sqrt{d}$ divides $(2q, (a + i\sqrt{d})q) = q$. Therefore, there exist $u, v \in \mathbb{Z}$ such that

$$q = (a + i\sqrt{d})(u + iv\sqrt{d}).$$



This gives $au - vd = q$ and $u + av = 0$ (we note that q is a rational integer), which leads to $-v(a^2 + d) = q$, that is, $-2vq = q$, a contradiction. We conclude that $(2q, (a + i\sqrt{d})q)$ does not exist.

Remark 2.2 It has been proven in Theorem 2 [1], that if α, β are non-zero elements of an integral domain D , then $[\alpha, \beta]$ exists if and only if $(r\alpha, r\beta)$ exists for all $r \in D, r \neq 0$. From the above proposition it follows that in $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$, square-free, the elements 2 and $a + i\sqrt{d}$ with a and d of the same parity do not have a least common multiple (even if their GCD does exist).

Suggested Reading

- [1] D Khurana, On GCD and LCM in Domains – A Conjecture of Gauss, *Resonance*, Vol.8, No.6, pp.72–79, 2003.
- [2] V Peric, M Vukovic, Some examples of principal domain which is not Euclidean and some other counterexamples, *Novi Sad J. Math*, Vol.38, No. 1, pp.137–154, 2008.

