ISSN No:-2456-2165

Unique Factorization for Ideals in the Ring $Z[\sqrt{-5}]$

Abdirahman O. Alin[1]
[1] Senior Lecturer at Pure Mathematics Courses in Many Universities in Somalia, MQ-Somalia

Abstract:- The fundamental theorem of arithmetic says that any integer greater than 2 can be written uniquely as a product of primes. For the ring $Z[\sqrt{-5}]$, although unique factorization holds for ideals, unique factorization fails for elements. We investigate both elements and ideals of$Z[\sqrt{-5}]$. For elements, we examine irreducibility (the analog of primality) in $Z[\sqrt{-5}]$ and look at how often and how badly unique factorization fails. For ideals, we examine irreducibility again and a proof for unique factorization.

Keywords: *Factorization; Ideals; Irreducibility; Rings; Prime*.

I. INTRODUCTION

Algebraic number theory is a branch of number theory that uses the techniques of abstract algebra to study the integers, rational numbers, and their generalizations. Number-theoretic questions are expressed in terms of properties of algebraic objects such as algebraic number fields and their rings of integers, finite fields, and function fields [1]. These properties, such as whether a ring admits unique factorization, the behavior of ideals, and the Galois groups of fields, can resolve questions of primary importance in number theory, like the existence of solutions to Diophantine equations. An important property of the ring of integers is that it satisfies the fundamental theorem of arithmetic, that every (positive) integer has a factorization into a product of prime numbers, and this factorization is unique up to the ordering of the factors [2]. Many rings of integers in algebraic number fields do not admit unique factorization. There is an algebraic obstruction called the ideal class group [3]. When the ideal class group is trivial, the ring is a Unique Factorization Domain. When it is not, there is a distinction between a prime element and an irreducible element [4]. An irreducible element x is an element such that if$x = yz$, then either y or z is a unit. These are the elements that cannot be factored any further.Every element in O admits a factorization into irreducible elements, but it may admit more than one. This is because, while all prime elements are irreducible, some irreducible elements may not be prime. For example, consider the ring $Z\sqrt{-5}$.In this ring, the numbers $3,2+\sqrt{-5}$ and $2-\sqrt{-5}$ are irreducible. This means that the number 9 has two factorization into irreducible elements [2].

We intend continue the exposiion on the failure of unique prime factorization in the ring $Z[\sqrt{-5}$. For ideals, we examine irreducibility and we intend to give a proof for unique factorization.

II. DEFINITIONS

In order to study $Z[\sqrt{-5}$, we must first understand some of the ideas in basic abstract algebra. We will use Z for the set of integers, Q for the set of rational numbers, and C for the set of complex numbers.

- *A Ring:*

A ring is a non empty set with two binary operations, addition and multiplication such that for all x, y, z in the ring[5]:

- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- there exists an additive, 0, such that $x + 0 = x$
- $x(yz) = (xy)z$
- there exists an additive inverse, $-x$, such that $x + -x = 0$
- $x(y + z) = xy + xz$

Moreover, a ring is called commutative if, in addition to (1) and (6) $xy = yx$ for all x, y in the ring

- *Ideal:*

An ideal I of a ring R is a principal ideal if there exists $a \in R$,such that $I = (a) = a.r$[6] where $r \in R$

- *A Unit:*

A unit is a nonzero element x of a commutative ring such that there is nonzero element in the ring with $xy = 1$.

➢ *A Field:*
A field is a commutative ring with identity in which every nonzero element is a unit.

➢ *A Subgroup:*
Let R be a ring. A left ideal I of R is a subset of R such that $(I,+)$ is a subgroup of $(R,+)$ and if $r \in R, \alpha \in I \Rightarrow r\alpha \in I$. Similarly a right ideal J of R is a subset of R such that $(J,+)$ is a subgroup of $(R,+)$ and if $r \in R, \alpha \Rightarrow \in J$..

- *Proposition:*

For $a, b \in Z$, the following statements are equivalent:

✓ $a + b\sqrt{-5}$ is reducible
✓ $a - b\sqrt{-5}$ is reducible
✓ $-a + b\sqrt{-5}$ is reducible and also
✓ $-a - b\sqrt{-5}$ Is reducible.

- *Proof:*

Assume $a + b\sqrt{-5}$ is reducible. Then there exists $m, n, s, t \in Z$ such that $+b\sqrt{-5} = (m + n\sqrt{-5})(s + t\sqrt{-5})$. This means $a = ms - 5nt$ and $b = mt - ns$. Then

$$-a - b\sqrt{-5} = -(-ms - 5nt) - (mt + ns)\sqrt{-5} = (m + n\sqrt{-5})(-s - t\sqrt{-5}),$$
$$a - b\sqrt{-5} = (ms - 5nt) - (mt + ns)\sqrt{-5} = (-m + n\sqrt{-5})(-s + t\sqrt{-5}), \text{ and}$$
$$-a + b\sqrt{-5} = -(ms - 5nt) + (mt + ns)\sqrt{-5} = (-m + n\sqrt{-5})(s - t\sqrt{-5})$$

- *Theorem:*
Let$R = Z\sqrt{-5}$, and let p be a rational prime in R. Then:

✓ $p = 5$ is the square of an irreducible element.
✓ If $p \equiv 1$ or $9 \bmod 20$, then p is reducible.
✓ If $p = 2$ or $p \equiv 3,7,11,13,17$; or $19 \bmod 20$, then p is irreducible.

- *Proof:*

✓ Let $p = 5$. It is easy to see that $5 = (\sqrt{-5})(-\sqrt{-5})$. We also know $\sqrt{-5}$ is irreducible as $N(\sqrt{-5}) = 5$ and the only integers that divide 5 are 1 (where all elements with norm 1 are units) and 5 (where only $\pm\sqrt{-5}$ have norm 5) Thus p acts like the square of an irreducible.
✓ Let $p \equiv 1 \bmod 20$. By the Quadratic Reciprocity Theorem[7], $\left(\frac{5}{p}\right) \cdot \left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2}} \cdot \frac{p-1}{2} = (-1)^{p-1} = 1$, so $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{20k+1}{5}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{1}{5}\right) = 1$, Thus, there exists a solution z_0 to $z^2 \equiv -5 \bmod p$ so p is reducible.

➢ *Proposition:*
Let R be a commutative ring with identity and let I be an ideal. Then $\frac{R}{I}$ is an integral domain if and only if I is prime.

- *Proof:*

First, suppose that $\frac{R}{I}$ is an integral domain. Let $a, b \in R$ such that $ab \in I$ then $(a + I)(b + I) = ab + I = I$ since $\frac{R}{I}$ is an integral domain. If $a + I = I$ then $a \in I$ if $b + I = I$, then $b \in I$, Therefore, since either $a \in I$ or $b \in I, I$ is prime.

Now, assume I is prime. We know $\frac{R}{I}$ is a commutative ring with identity so we need only show it has no zero divisors.Suppose $a + I, b + I \in \frac{R}{I}$ such that $ab \in I$ then $(a + I)(b + I) = 0 + I = I$ then $ab \in I$ which implies $a \in I$ or $b \in I$ thus $a + I = 0 + I$ or $b + I = 0 + I$ so, $\frac{R}{I}$ has no zero divisors and $\frac{R}{I}$ is an integral domain.

➢ *Proposition:*
Let R be a commutative ring with identity and let I be an ideal of R. Then $R = I$ is a field if and only if I is maximal.

- *Proof:*

First, suppose $\frac{R}{I}$ is a field and J is an ideal of R such that $I \subset J$. Let $a \in J$ but $a \notin I$, Then $a + I$ is a nonzero element of $\frac{R}{I}$ and, therefore, since $\frac{R}{I}$ is a field, there exists $b \in I$ such that $(a + I)(b + I) = 1 + I$. Since $a \in J$, we have $ab \in J$, and since $1 + I = (a + I)(b + I) = ab + I$, we have $1 - ab \in I \subseteq J$ So, $1 = (1 - ab) + ab \in J$ and $J = R$ as J contains the identity. Thus I is maximal by definition. Now, suppose I is maximal and let $a \in R$ but $a \notin I$. To show $\frac{R}{I}$ is a field, we need only to show that $a + I$ has a multiplicative inverse. Consider the ideal $J = ar + b, r \in R$ and $b \in I$ then $I \subseteq J$. Since I is maximal and $I \neq J$, we have $J = R$ and so J must contain the identity. There exists bprime $\in I$ and $c \in R$ such that $1 = ac + b$ and so $1 + I = ac + b + I = ac + I = (a + I)(c + I)$, Thus $a + I$ has a multiplicative inverse and $\frac{R}{I}$ is a field.

III. IRREDUCIBLE POLYNOMIAL

- If R is an integer domain and $R[x]$ is polynomial ring over R then $f(n) \in R[x]$ is a polynomial is said to be irreducible
- If $f(n) = h(n)g(n)$, where $h(n) \in R[x]$ and $g(n) \in R[x]$ then either $h(n$ and $g(n)$ is unit in R

- *Example:*

Let $f(n) = x^3 + x^2 + x + 1$ over Q|R|C

- *Solution:*

$$x^2(x + 1) + (x + 1) = (x + 1)(x^2 + 1)$$

Where h(n) $= x + 1$ but neither $h(n) = x + 1$ is unit element in Q, $g(n) = x^2 + 1$ But neither $g(n) = x^2 + 1$ is unit element in Q So $f(n) = x^3 + x^2 + x + 1$ is not irreducible polynomial.

- *Example:*

Proof that if $f(n) = 3x^2 + 21$ over Q is Irreducible?

- *Solution:*

$f(n) = 3(x^2 + 7)$, where $h(n) = 3$ so $h(n)$ is a unit element in Q[x], $g(n) = x^2 + 7 = 0, x = \pm\sqrt{-7} \notin Q$, because $\notin Q$, so $f(n) = 3x^2 + 21$ is irreducible polynomial in Q. $f(n) = 3(x - \sqrt{7}i)(x + \sqrt{7}i)$ is irreducible in Q.

- *Example:*

Let $f(n) = x^2 + 1$ over $R \mid C$ proof that f(n) is irreducible?

- *Solution:*

➢ *Over R:*

$f(n) = x^2 + 1 = 0, x^2 = -1, x = \pm\sqrt{-1} = \pm if(n) = x^2 + 1 = (x - i)(x + i)$ So $(x + i) \notin R(n), (x - i) \notin R(n)$ then $f(n)$ is irreducible.

➢ *Over C:*

Also $f(n)$ is irreducible in C

IV. DEDEKIND'S IDEALS

We are now ready to take a look at the ideals in $Z[\sqrt{-5}]$. Richard Dedekind studied our ring and its ideals, in particular. In fact, $Z[\sqrt{-5}]$ is the quintessential example of what is now known as a Dedekind Domain [8]. How can we save unique factorization in rings like $\sqrt{-5}$ In order to motivate the answer, consider Hilbert's example of the set of integers $M = 1,5,9, \ldots, 4n + 1, \ldots$. In this monoid, the factorization $949 = 2121$ shows that unique factorization does not hold. The different factorization can, however, be explained by introducing the "ideal numbers" 3 and 7 and observing that $949 = 2121$ comes from pairing up the factors in the ideal factorization $441 = 3^2 \times 7^2$ in two different ways. Now let us do the same in R by introducing the ideals. Recall that an ideal a in a ring R is a set closed with respect to addition and multiplication by ring elements [8]:

➢ *Example:*

Consider again the ring $R = \sqrt{-5}$, show that R is a Dedekind domain?

- *Solution:*

We see from this example that a Dedekind domain is in general not a unique factorization domain, the element 2 is irreducible, but not prime in R, so that it does not have a factorization into prime elements. However, we will prove now that a Dedekind domain always has an analogue of the unique factorization property for ideals, i.e. every non-zero ideal can be written uniquely as a product of non-zero prime ideals (which are then also maximal since Dedekind domains are 1-dimensional). If a complex number is a root of a nonzero monic polynomial in $Q[X]$, it is called an algebraic number. If it is a root of a nonzero monic polynomial in $Z[X]$, it is called an algebraic integer. Some examples that are both algebraic numbers and algebraic integers are $\sqrt{-5}$ as $\sqrt{-5}$ is a root of the monic polynomial x^2+5, and -1 , as -1 is a root of $x+1$. An example of an algebraic number that is not an algebraic integer is $\frac{1}{2}$ as it is a root of $x-\frac{1}{2}$, which is not in $Z[X]$, and $2x-1$, which is not monic, Any other polynomial satisfied by $\frac{1}{2}$ is either not in $Z[X]$ or is not monic. It is interesting to point out (but more difficult to show) that π and e are not algebraic numbers. A number field has the form $Q[\alpha]$, where α is an algebraic number. If we want to look at algebraic integers in a number field $Q[\alpha]$ (where α again is an algebraic number), we can look at $Z[\alpha]$. However, $Z[\alpha]$ does not always contain all algebraic integers of $Q[\alpha]$. For example, in the ring $Q[\sqrt{-3}]$, $\frac{-1+\sqrt{-3}}{2}$ is an algebraic integer as it is a root of $x^2+x+1 \in Q[X]$, in fact, the algebraic integers of $Q[\sqrt{-3}]$ are the elements of $Z\left[\frac{-1+\sqrt{-3}}{2}\right]$ in $Q[\sqrt{-5}]$, however, the algebraic integers are exactly the set of elements in $Z[\sqrt{-5}]$ In studying the algebraic integers of quadratic number fields (number fields of the form $Q(\sqrt{d})$ where $d \in$ Zand d is not a perfect square).

V. HOW IDEALS FACTOR

We considered factorization of elements in $Z[\sqrt{-5}]$; here we look at factorization of ideals in $Z[\sqrt{-5}]$. Much like an element of a ring R, an ideal is reducible if it can be expressed as the product of two proper, nontrivial ideals[8]. Let us first consider principal ideals. Say, we have an element $a \in Z$ such that $a=bc$. Then the ideal generated by (a) can be factored as $(a)=(b)(c)$. Thus, for any composite integer, the corresponding ideal generated by that integer will also be reducible, What about rational primes in $Z[\sqrt{-5}]$. We know how they factor as elements, but how do they factor as ideals? We know that if a prime is reducible as an element, it will be reducible as an ideal but if it is irreducible as an element, will it be irreducible as an ideal? It turns out that sometimes it is irreducible as an ideal but sometimes it is not. An ideal generated by an irreducible element is not necessarily irreducible as an ideal,First, we need to establish a way of factoring an ideal generated by certain rational primes [9].

➢ *Corolory:*

Every nonzero prime ideal in A is a maximal ideal.

- *Proof:*

For any nonzero prime ideal p of A, $\frac{A}{p}$ is a domain that is finite-dimensional over a field is itself a field, so p is maximal.

- *Theorem:*

Let p be a rational prime in $Z[\sqrt{-5}]$ then
(a) (p) ramifies if $p=2$ or $p=5$.
(b) (p) splits if -5 is a square modulo p.

- *This can occur in one of two ways:*

(a) If $p \equiv 1$ or $9\mathrm{mod}20$, then p factors in $Z[\sqrt{-5}]$ as a product of two irreducible a and b. Then $(p)=(a)(b)$.
(b) If $p \equiv 3$ or $7\mathrm{mod}20$, then p is reducible as an element and (p) is reducible as an ideal.
(c) The element p is irreducible in $Z[\sqrt{-5}]$ (and thus the ideal (p) is irreducible) if -5 is not a square modulo p, which is exactly when p is 11,13,17 or $19\mathrm{mod}20$.

➢ *Proof Theorem:*

We will break the proof into four cases.

(a) Let $=2$: Then $(p)=(2)=(1+\sqrt{-5},2)(1-\sqrt{-5},2)$, Since $2-(1-\sqrt{-5},2)$ we have $(1+\sqrt{-5},2)=(1\sqrt{-5},2)$.

Thus (a) Let $p \equiv 1,9\mathrm{mod}20: p=ab$ for some non-units $a, b \in Z[\sqrt{-5}]$, Thus $(p)=(a)(b)$.

(b) Let $p \equiv 3\mathrm{mod}20$: We want to show that there exists z such that $z^2 \equiv 5\mathrm{mod}p$ Then, (p) would be reducible which says $(p)=(z+\sqrt{-5},p)(z-\sqrt{-5},p)$ More over, $(z+\sqrt{-5},p)$ and $(z-\sqrt{-5},p)$ are prime ideals, we will use Legendre symbols. So

$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) = (-1)^{\frac{20k+3-1}{2}}\left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$ and $\left(\frac{-5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{20k+3}{5}\right) = -\left(\frac{3}{5}\right) = 1$, Thus there exists z such that $z^2 \equiv -5 \mathrm{mod} p$ and (p) is reducible. Let $p \equiv 7 \mathrm{mod} 20$ then $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) = (-1)^{\frac{20k+3-1}{2}}\left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$ and $\left(\frac{-5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = -\left(\frac{20k+7}{5}\right) = -\left(\frac{2}{5}\right) = 1$,

Thus $(p) = (z + \sqrt{-5}, p)(z - \sqrt{-5}, p)$ for $p \equiv 3$ or $7 \mathrm{mod} 20$.

(c) For $p \equiv 11,13,17,19 \mathrm{mod} 20$, we know there does not exist z such that $z^2 \equiv 5 \mathrm{mod} p$, so $x^2 + 5$ is irreducible in $Z_p[X]$ and $\frac{z_p[X]}{x^2+5}$ is an integral domain. Of course, $\frac{z_p[X]}{(x^2+5)} \cong \frac{z_p[X]}{(p,x^2+5)} \cong \frac{Z\sqrt{-5}}{(P)}$, therefore if $p \equiv 1113,17$ or $19 \mathrm{mod} 20$, then (p) is irreducible.

So far, we have looked at all of the principal ideals in $Z\sqrt{-5}$ generated by rational integers, but what about those generated by a general element? We can non trivially factor the ideal generated by a reducible elements: if $\alpha = \beta\gamma$ then

$$(\alpha) = (\beta)(\gamma)$$

Let's look at some examples. The ideal $(2 + 4\sqrt{-5})$ can be factored into $(2)(1 + 2\sqrt{-5})$ and the ideal $(7 + \sqrt{-5})$ can be factored into $(1 + \sqrt{-5})(2 - \sqrt{-5})$.

What about irreducible elements in our ring? We already saw that $(23) = (8 + \sqrt{-5}, 23)(8 - \sqrt{-5}, 23)$ where 23 is irreducible in our ring. So we know that there exist irreducible elements that are reducible as ideals.

VI. CONCLUSION

In studying the ring $[\sqrt{-5}]$, we established many results its ideals. For elements, we studied reducibility for ideals, in particular for ideals generated by integers. We have proved exactly what happens to ideals generated by rational primes in our ring. We also glanced at the work of Richard Dedekind, who had the insight to take our ring and develop a whole theory that described it and other rings. Dedekind's work explains exactly why unique factorization holds for ideals. We have studied and discovered many interesting properties of the ring $Z[\sqrt{-5}]$. Perhaps the most interesting is the simple fact that unique factorization fails for elements but holds for ideals. This division creates an interesting dichotomy between elements and ideals, particularly being that ideals are, in some sense, a generalization of elements of the ring.

REFERENCES

[1]. T. M. Apostol, Introduction to analytic number theory. Springer Science & Business Media, 1998.
[2]. L. Lynch, "Factorability in the ring z [-5]," 2004.
[3]. C. F. Gauss, Disquisitiones arithmeticae. Yale University Press, 1966.
[4]. L. Carlitz, "A characterization of algebraic number fields with class number two.," Proceedings of the American Mathematical Society, vol. 11, no. 3, pp. 391-392, 1960 .
[5]. A.Chatters, "Non-commutative unique factorization domains," in Mathematical Proceedings of the Cambridge Philosophical Society, vol. 95, pp. 49-54, Cambridge University Press, 1984.
[6]. N. H. McCoy, "Prime ideals in general rings," American Journal of Mathematics, vol. 71, no. 4, pp. 823-833, 1949 .
[7]. A.Yap, "Gauss' quadratic reciprocity theorem and mathematical fruitfulness," Studies in History and Philosophy of Science Part,A vol. 42, no. 3, pp. 410-415, 2011.
[8]. R. Dedekind, Theory of algebraic integers. Cambridge University Press, 1996.
[9]. L. Kronecker, "Grundzüge einer arithmetischen theorie der algebraische grössen.," 1882.