Revista Sergipana de Matemática e Educação Matemática

https://doi.org/10.34179/revisem.v9i3.21800

Special Issue in honor of the 73rd birthday of Professor José Plínio de Oliveira Santos (IMECC-UNICAMP)

ALGEBRAIC ANALOGUES OF CERTAIN THEOREMS OCCURRING IN ELEMENTARY NUMBER THEORY (WARNING: ELEMENTARY NUMBER THEORY IS NOT THAT ELEMENTARY)

Sivaramakrishnan R.
"Rajashree", 36/1328, Thekkemadhom Cross Road, Trichur 680001, Kerala, India
rsjreeg@gmail.com

Abstract

This note makes an attempt to point out some of the familiar situations occurring in early number theory lessons.

Keywords: Commutative rings, semi simple-rings, Euclidean rings.

1 Introduction

(i) The set of natural numbers contains $1, 2, 3, 4, \ldots$; the positive integers used for counting. This set is denoted by $\mathbb{Z}^+$.

(ii) A natural number ≥ 1 is either a prime or a product of prime numbers. An element $m \in \mathbb{Z}^+$ is uniquely expressible as

$$m = p_1^{a_1} \cdots p_2^{a_2} \ldots p_n^{a_n} \tag{1.1}$$

where $p_1, p_2, \ldots p_n$ are distinct primes.

(iii) By a prime p, one means that given $a, b \in \mathbb{Z}^+$, p divides ab implies that either $p \mid a$ or $p \mid b$ or $p \mid b$, where $\mid$ means 'divides'. (1.1) is refereed to as the prime-power decomposition of $m > 1$.

(iv) In (1.1), the prime-power decomposition of m contains a prime factor p which is least among the primes dividing n. That is, every integer n has a least prime divisor.

(v) The set $\mathbb{Z}^+$ of positive integers forms a semi-group under multiplication.

(vi) By adding 0 and negative integers to $\mathbb{Z}^+$, one gets the set $\mathbb{Z}$ of all integers (positive, negative and zero). It is verified that $(\mathbb{Z}, +, \cdot)$ forms a commutative ring with identity (or unity) element 1. That is, $1 \cdot a = a \cdot 1 = a$, for $a \in \mathbb{Z}$.

(vii) The formal definition of a ring R is the following:

A ring R is an ordered triple $(R, +, \cdot)$ consisting of a nonempty set R and two binary operations $+$ and $\cdot$ defined on R such that

(a) $(R, +)$ is an abelian group.

(b) $(R, \cdot)$ is a semi-group and

(c) the operation $(\cdot)$ is distributive (on both sides) over the operation $(+)$.

(viii)

Definition 1.1. *A commutative ring R is a ring $(R, +, \cdot)$ in which multiplication is commutative: that is, for all $a, b \in R$ $a \cdot b = b \cdot a$. It also means that the elements a, b are commutative.*

(ix) Given a ring $(R, +, \cdot)$, $0 \neq a \in R$ is called a left (right) zero divisor if there exists $b(\neq 0) \in R$ such that $a \cdot b = 0$ $(b \cdot a = 0)$. Further, a zero divisor of $(R, +, \cdot)$ is either a left or right zero divisor.

(x) A ring R is without zero divisors if, and only if, R satisfies the cancellation laws for multiplication. That is, for all $a, b \in R$, $a \cdot b = a \cdot c$ and $b \cdot a = c \cdot a$(where $a \neq 0$) imply that $b = c$.

(xi)

Definition 1.2. *A commutative ring is an integral domain if, and only if, it has no zero divisors.*

(xii)

Definition 1.3. *Let I be a non empty subset of a ring R, I is called a two-sided ideal of k if, and only if,*

(i) for $a, b \in I$, one has $a - b \in I$ and

(ii) for $r \in R$ and $a \in I$, the conclusion: $ar \in I, ra \in I$ holds.

(xiii) Let $(R, +, \cdot)$ be a commutative ring with unity. 1_R. $(R, +, \cdot)$ is called 'simple' if it has no non-trial ideals.

(xiv) Let $(R, +, \cdot)$ be a commutative ring with unity. $(R, +, \cdot)$ is called a principal ideal ring if every ideal of $(R, +, \cdot)$ is a principal ideal, that is, an ideal generated by a single element. A principal ideal ring which is an integral domain is termed a principal ideal domain (P.I.D).

(xv)

Definition 1.4. *Let R be a commutative ring with unity 1_R. An ideal I of the ring R is said to be a maximal ideal provided that $I \neq R$ and whenever J is an ideal of R with $I \subset J \subseteq R$, then $J = R$.*

That is, the only ideal to contain a maximal ideal properly is the ring itself.

(xvi)

Notation. *(I, a) denotes the ideal (of R) generated by the set $I \cup \{a\}$.*

Theorem 1.5. [1] *R denotes a commutative ring with unity 1_R. An ideal I of R is a maximal ideal if, and only if, $(I, a) = R$ for any $a \notin I$.*

Demonstração. The first observation is that (I, a) satisfies

$$I \subset (I, a) \subseteq R$$

If I where a maximal ideal of R, it would mean that $(I, a) = R$.

Conversely, suppose that J is an ideal of R, with the property that $I \subset J \subseteq R$. If $a \in J$ and $a \neq I$, one would get $I \subset (I, a) \subseteq J$. The requirement that $(I, a) = R$ would force $J = R$. Then, it follows that I is a maximal ideal.

□

Next, let R be a commutative ring with unity 1_R.

Theorem 1.6. [1a] *Let $\{I_i\}$ be a collection of ideals of R. Then $\cap I_i$ is an ideal of R.*

Demonstração. The intersection $\cap I_i$ is non-empty, since each I_i contains the zero element of the ring. Let $a, b \in \cap I_i$ and $r \in R$. As each I_i is an ideal, $a - b, ra, ar$ all lie in I_i. This is true for every value of I_i. So, $a - b, ra, ar$ all belong to $\cap I_i$ making $\cap I_i$ an ideal of R. □

Given a commutative ring R with unity 1_R, let S be a nonempty subset of R. The symbol (S) is used to denote

$$(S) = \cap\{I : S \subseteq I : I \text{ an ideal of } R\}$$

The collection of all ideals which contain S is nonempty, since R itself is an ideal of R. By virtue of theorem 1.6, (S) forms an ideal and $(S) \subset I$. Further, (S) is the smallest ideal of R containing S.

If S consists of a finite number of elements say $a_1, a_2, \ldots, a_n$ the ideal is said to be finitely generated with $a_i (i = 1, \ldots n)$ as its generators. An ideal (a) generated by $a \in R$ is called a principal ideal. The ring $\mathbb{Z}$ of integers is finitely generated and is generated by 1.

Theorem 1.7. [1b] *Let R be a commutative ring with unity 1_R. If R is finitely generated, each proper ideal of R is contained in a maximal ideal.*

Demonstração. Suppose that R is finitely generated by the elements $a_1, a_2, \ldots a_n$. One defines

$$A = \{J : I \subseteq J, \text{ where } J \text{ is a proper ideal of } R\}$$

A is nonempty, as I belongs to A
A chain $\{I_i\}$ of ideals in A is introduced.

Claim. *$\cup I_i$ is again a member of A*

The method of proof is as follows :

Let $a, b \in \cup I_i$ and $r \in R$. Then there exists indices I and J for which $a \in I_i$, $b \in I_j$. As the collection $\{I_i\}$ forms a chain of ideals either $I_i \subseteq I_j$ or $I_j \subseteq I_i$. For definiteness, suppose that $I_i \subseteq I_j$. Let $a, b \in I_j$. Then, $a - b \in I_j \subseteq \cup I_i$. Also, the products ar and $ra \in I_i \subseteq \cup I_i$. It follows that $\cup I_i$ is an ideal of R.

Claim. *$\cup I_i$ is a proper ideal of R.*

Suppose the contrary. Then, $\cup I_i = R = (a_1, a_2, \ldots, a_n)$, the ideal generated by $a_1, \ldots, a_n$, since R is a finitely generated ring. Then, each generator a_k would belong to I_{i_k} of the chain $\{I_i\}$. As there are only finitely many I_{i_k}, one contains all others. Let It be marked $I_{i'}$. It follows that $I_{j'} = R$, which is impossible. Further, $I \subseteq \cup I_i$. The conclusion is that

$$\cup I_i \in A.$$

Appealing to Zorn's Lemma [1c], the family A contains a maximal element M. It follows from the definition of A that M is a proper ideal of R with $I \subseteq M$.

Claim. *M is a maximal ideal of R.*

Let J be an ideal for which $M \subset J \subseteq R$. Since M is a maximal element of the family A, J cannot belong to A. Then, J is an improper ideal and so $J = R$. The conclusion is that M is a maximal ideal of R and this statement completes the proof. □

Theorem 1.8 (Krull-Zorn Theorem)**.** [1d] *In a ring R with unity 1_R, each proper ideal is contained in a maximal ideal.*

Remark 1. *In the ring $\mathbb{Z}$ of integers, every ideal is contained in a maximal ideal. But the maximal ideals of $\mathbb{Z}$ are the ideals generated by primes. In other words, given an integer $n(> 1) \in \mathbb{Z}$, there exists a smallest prime p which divides n.*

2 Simple rings

A ring which is not commutative is considered. Let $\mathbb{R}$ denote the field of real numbers. $M_n(\mathbb{R})$ denotes the set of $n \times n$ matrices with entries from $I_{\mathbb{R}}$ $(n > 1)$. As a notational device, one writes E_{ij} to denote an $n \times n$ matrix whose (i, j)th entry is 1 where $j = i$ and zeros elsewhere. It is verified that $M_n(\mathbb{R})$ is a non-commutative ring with identity element $[\delta_{ij}]$ where

$$\delta_{ij} = \begin{cases} 1; & j = i; \\ 0; & \text{otherwise.} \end{cases} \tag{2.1}$$

Suppose that $I \neq [0]$ is an ideal of $M_n(\mathbb{R})$. Then I will contain some nonzero matrix $[a_{ij}]$ (say) with an rsth entry $a_{rs} \neq 0$. Since I is a two-sided ideal of $M_n(\mathbb{R})$, the product

$$E_{rr}[b_{ij}][a_{ij}]E_{ss}$$

belongs to I where the matrix $[b_{ij}]$ is chosen to have the element a_{rs}^{-1} down its main diagonal and zeros elsewhere. As a result of all the zero entries in the various factors , it is easy to check that this product is equal to E_{rs}. Knowing this, the relation

$$E_{ij} = E_{ir}E_{rs}E_{sj}(i, j = 1, 2, \ldots)$$

implies that all the n^2 of the matrices E_{ij} are contained in I. Grasping firmly the situation, one notes that the identity matrix $[\delta_{ij}]$ where

$$\delta_{ij} = \begin{cases} 1; & j = i; \\ 0; & \text{otherwise.} \end{cases}$$

could be written as

$$[\delta_{ij}] = E_{11} + E_{12} + \cdots + E_{nn} \tag{*}$$

(*) leads to the conclusion that $[\delta_{ij}] \in I$.

Observing that in a ring with identity, no proper (right , left or two-sided) ideal I contains the identity element,

$$I = M_n(\mathbb{R}).$$

In other words, $M_n(\mathbb{R})$ possesses no nonzero proper ideals and thus $M_n(\mathbb{R})$ is a simple ring [1e].

3 Semi-simple Rings

A property of the set of positive integers is a fact that the set $\mathbb{N}$ of positive integers has an infinite number of primes. The necessary ground-work has to be provided.
Let R be a commutative ring with unity.

Definition 3.1. *An ideal I of the ring R is said to be a maximal ideal if $I \neq R$ and J is an ideal of R with $I \subset J \subseteq R$, then $J = R$.*

Theorem 3.2. *In the ring $\mathbb{Z}$ of integers, maximal ideals correspond to those generated by primes.*

Demonstração. It is noted that $\mathbb{Z}$ is a principal ideal domain (PID). That is to say that every ideal of $\mathbb{Z}$ is generated by an integer $n(n \geq 0)$. As $\mathbb{Z}$ has no divisors of zero, $\mathbb{Z}$ is an integral domain in which every ideal is principal. $\mathbb{Z}$ is an example of a principal ideal domain (PID). □

It is known [1f] that if R is a finitely generated ring, then each ideal or R is contained in a maximal ideal.

Definition 3.3. *An ideal I of R (a commutative ring with unity) is called a prime ideal if for all $a, b \in R$, $ab \in I$ implies that either $a \in I$ or $b \in I$.*

This is the analogue of the result stated below.

In the set $\mathbb{N}$ of positive integers, if p is a prime dividing ab (where a, b are positive integers), p divides ab implies either p divides a or p divides b.

It is noted that in a commutative ring with identity, every maximal ideal is a prime ideal.

Definition 3.4. *The Jacobson radical of a commutative ring R with unity denoted by $J(R)$ is the set*

$$J(R) = \cap\{M \mid M \text{ is a maximal ideal of } R\}$$

If $J(R) = \{0\}, R$ is said to be a ring without Jacobson radical or R is a semi simple ring.

To show that the ring $\mathbb{Z}$ of integers is semi-simple the first observation is that the maximal ideals of $\mathbb{Z}$ correspond to prime numbers.

It is noted that $(\mathbb{Z}, +, \cdot)$ is an integral domain in which every ideal is principal. That is, $(\mathbb{Z}, +, \cdot)$ is a principal ideal domain (PID). Further, in $(\mathbb{Z}, +, \cdot)$ maximal ideals correspond to prime numbers, the ideal generated by n (a positive integer) is a prime ideal if and only if n is a prime. Further, in $(\mathbb{Z}, +, \cdot)$ prime ideals are maximal ideals. Moreover, prime ideals of $(\mathbb{Z}, +, \cdot)$ are generated by prime p. So, according to definition 3.4 one notes that the Jacobson radical of $\mathbb{Z}$ is given by

$$J(\mathbb{Z}) = \cap\{(p) : p, \text{ a prime}\} \tag{3.1}$$

Since no number is divisible by every prime, one concludes that $J(\mathbb{Z}) = (0)$. Thus, $\mathbb{Z}$ is a semi-simple ring[1g].

Theorem 3.5. [1h] *Let R be a principal ideal domain. Then, R is semi-simple if, and only if, R is either a field or has an infinite number of maximal ideals.*

Demonstração. As R is a PID, R has a set of prime elements. Let $\{p_i\}$ be the set of primes of R. This is generated by the fact that as R is a PID, a nontrivial ideal (p), generated by a prime p is such that (p) is a maximal ideal (and so a prime ideal) if, and only if, p is an irreducible (prime) element of R [1j]. So, the maximal ideals of R are,simply, the principal ideals (p). So, an element a (belonging to R) becomes an element of $J(R)$ [1i], the Jacobson radical of R if, and only if, a is divisible by each prime p_i. So, $a \in J(R)$ if and only if, a is divisible by each prime p_i. If R has an infinite number of maximal ideals, then $a = 0$, since every non-zero non invertible element of R is uniquely representable as a finite product of primes. So, R is a PID $\Rightarrow$ the Jacobson radical of R is (0) or R is semi simple.

In the opposite direction, suppose that R has only a finite number of primes $p_1, p_2, \ldots, p_n$, then

$$J(R) = \cap_{i=1}^{n} pi = (p_1, p_2, \ldots, p_n) \neq (0)$$

a contradiction to the hypothesis that $J(R) = 0$. □

Finally, one notes that if the set $\{p_i\}$ is empty, then each nonzero element of R is invertible and so, then, R is a field in which case $rad\, R = \{0\}$.

Corollary 3.6 (An Important Corollary)**.** *The ring of integers $\mathbb{Z}$ has an infinite numbers of maximal ideals which are generated by primes, thus, giving an algebraic proof of Euclid's theorem.*

4 Euclidean Rings [2]

Definition 4.1. *An integral domain D is said to be a Euclidean ring if, for every $a \neq 0$ in D there is defined a non negative integer $d(a)$ such that*

(i) for all $a, b, \in D$ both nonzero $d(a) \leq d(ab)$,

(ii) for all $a, b, \in D$ both nonzero there exist $s, t \in D$ such that $a = sb + t$ where either $t = 0$ or $d(t) < d(s)$.

Note: $d(0)$ is not defined.

The set $\mathbb{Z}$ of integers serves as an example. The condition (ii) resembles the division algorithm in the integral domain $\mathbb{Z}$ which says:

If $a, b \in \mathbb{Z}$ with $b \neq 0$ there exist integers q and r such that $a = bq + r$ where either $r = 0$ or $0 < r < |b|$.

The concept of a Euclidean ring is a generalization of the integral domain $\mathbb{Z}$ of integers.

Theorem 4.2. *Given an Euclidean ring D, suppose that A is an ideal of D. Then, there exists an element $a_0 \in A$ such that A consists of elements a_0d where $d \in D$.*

If A is the zero ideal, one has to take $a_0 = 0_D$ and the conclusion of the theorem holds trivially.

When $A \neq (0)$, there exists $a_0 \neq 0$ and $a_0 \in A$. Pick a_0 such that $d(a_0)$ is minimal. This is possible since d takes on non-negative integer values.

Suppose that $a \in A$. As D is a Euclidean domain, there exist $t, r \in D$ such that $a = ta_0 + r$ where $r = 0$ or $d(r) < d(a_0)$. Since $a_0 \in A$ and A is an ideal of D, $ta_0 \in A$. But, $r = a - ta_0$. This implies that $r \in A$ and r is such that $d(r) < d(a_0)$. This contradicts the minimality of $d(a_0)$. So, $r = 0$. Thus, $a = ta_0$ So, every element of A is a multiple of a_0, proving that A is a principal ideal of D, or D is a principal ideal domain.

Notation. *Let D be a principal ideal domain. If $a \in D$, principal ideal of D, generated by $a \in D$ is denoted by (a). That is, $(a) = \{xa : x \in D\}$.*

Remark 2. *The conclusion of theorem 4.2 is that every ideal of a Euclidean domain is principal. In other words, a Euclidean domain is a principal ideal domain, abbreviated as PID. However, there exist principal ideal domains that are not Euclidean domains. See T. Motzkin [3]*

Remark 3. *A Euclidean domain D possess a unit element.*

The reason is that as D is a PID and so D, itself is a principal ideal of D. One writes $D = (n_0)$ for aome $n_0 \in D$. So every element of D is a multiple of $n_0 \in D$. Therefore, $n_0 = n_0 e$ for some $e \in D$. If $a \in D$, then $a = bn_0$ for some $b \in D$. Then,

$$ae = (bn_0)e = b(n_0 a) = bn_0 = a.$$

As the Euclidean domain is commutative, e serves as the required unit element.

4.1 Divisibility Properties

Definition 4.3. *Let R be a commutative ring with unity 1_R. Suppose $a \neq 0$ and b are elements of R. One says that a divides b which is, symbolically, expressed as $a \mid b$. When a does not divide b one writes $a \nmid b$. It follows that*

1. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
2. *if $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$.*
3. *If $a \mid b$, then $a \mid bc$ for all $c \in R$.*

Definition 4.4. *Let R be a commutative ring with unity. Given $a, b \in R$, an element d in R is called the greatest common divisor (g.c.d) of a and b, if*

1. *$d \mid a$ and $d \mid b$*
2. *whenever $c(\in R)$ is such that $c \mid a$ and $c \mid b$, then $c \mid d$.*

Remark 4. *The notation $d = (a, b)$ is used to denote the g.c.d of a and b.*

Theorem 4.5. *Given a Euclidean ring D, any two elements a, b of D have a greatest common divisor g. Moreover, $g = xa + yb$ for some $x, y \in D$.*

Demonstração. Let A be the set of elements of the form $ka + lb$ where k, l vary over the elements of D.

Claim. *A is an ideal of D*

Since A is the set of elements of the form $ka + lb$, suppose that $sa + tb \in A$, for some $s, t \in D$.

$$m = k_1 a + l_1 b, \quad n = k_2 a + l_2 b.$$

Then, $m \pm n = (k_1 \pm k_2)a + (l_1 \pm l_2)b \in A$. Similarly, for any $r \in D$,

$$\begin{aligned} rm &= r(k_1 a + l_1 b) \\ &= (r(k_1)a + (rl_1)b \in A. \end{aligned}$$

Since A is an ideal of D, by theorem 4.2 there exists an element $a_0 \in A$ such that every element in A is a multiple of a_0. Since $a_0 \in A$ and every element of A is of the form $sa + tb$,

$$a_0 = s_1 a + t_1 b \text{ for some } s_1 t_1 \in D$$

By remark (3) D has a unit element say 1_D. Then,

$$a = 1_D a + 0_D b \in A; \quad b = 0_D a + 1_D b \in A. \tag{**}$$

As a and b are elements of A by (**), one has $a_0 \mid a$, $a_0 \mid b$.

Lastly, suppose that $c \in D$ is such that $c \mid a$ and $c \mid b$ then $c \mid s_1 a + t_1 b = a_0$. Therefore, a_0 satisfies the conditions for a being the g.c.d of a and b. In other words, any two elements a, b in D have a greatest common divisor g which is a linear combination of a and b. □

Definition 4.6. *Let D be an integral domain with unit element 1_D. An element $a \in D$ is a unit in D if there exists an element $b \in D$ such that $ab = 1_D$.*

Theorem 4.7. *Suppose that $a, b \in D$ are such that $a \mid b$ and $b \mid a$ hold. Then, $a = ub$ where u is a unit in R.*

Demonstração. Since $a \mid b$, one could write$b = sa$ for some $s \in D$. Since $b \mid a$, $a = tb$ for some $t \in D$. Then, $b = sa = s(tb) = (st)b$. As a, b belong to an integral domain, canceling b from $b = (st)b$ one gets $st = 1_D$. Or, s is a unit in D and t is a unit in D and so $a = ub$ where u is a unit. □

Definition 4.8. *Let D be an integral domain with unit element. Two elements $a, b \subset D$ are said to be associates if $b = na$ for some unit n in D.*

It is verified that in a Euclidean ring D with unity 1_D two greatest common divisors of two given elements of D are associates.

Theorem 4.9. *Let D be a Euclidean ring having elements a, b (say). If b is not a unit in D, then $d(a) < d(ab)$.*

Demonstração. Consider the ideal $A = (a) = \{xa : x \in D\}$ of D. By the property of a Euclidean ring, $d(a) \leq d(xa)$ for $0 \neq X \in D$. That is, the d-value of a is the minimum among d-values of elements of A. Suppose that $ab \in A$. If $d(ab) = d(a)$, it could be deduced that the d-value of ab is, also, minimal and every element in A is a multiple of ab. It follows that $a = abs$ for some $s \in D$. As D is an integral domain, cancellation law allows one to conclude that $bs = 1_D$. that is to say b is a unit in D, contrary to the assumption that b is not a unit. The conclusion is that $d(a) < d(ab)$. □

Definition 4.10. *In a Euclidean ring D, a non-unit π s called a prime element of D whenever $\pi = ab$, where $a, b \in D$, either a or b is a unit.*

Theorem 4.11. *Let D be a Euclidean ring. Then, every element of D is either a unit in D or can be written as a product of prime elements of D.*

Demonstração. Given $a \in D$, proof is by induction $d(a)$. If $d(a) = d(1_D)$, then a is a unit in D and so the first part of the theorem holds.

It is assumed that the theorem is true for all elements x in D such that $d(x) < d(a)$. The approach is to show that the theorem is true for a, also, by mathematical induction.

If a is a prime in D, the conclusion of the theorem is obvious. Suppose that a s not a prime in D. Then, a could be displayed as $a = bc$ where neither b nor c is a unit in D. By theorem 4.9,

$$d(b) < d(bc) = d(a)$$
$$\textit{and } d(c) < d(bc) = d(a).$$

By introduction hypothesis, b and c could be written as products of a finite number of prime elements of D. That is,

$$b = \pi_1 \cdot \pi_2 \cdot \ldots, \pi_n, \; c = \pi'_1 \cdot \pi'_2 \ldots \pi'_m$$

where $\pi_i, \pi'_j (i = 1, 2, \ldots, n \; ; j = 1, 2, \ldots, m)$ are prime elements of D. So, then, $a = bc = \pi_1 \cdot \pi_2 \cdot \ldots \pi_n \cdot \pi'_1 \cdot \pi'_2 \cdot \ldots \pi'_m$. or , a is capable of factorization into prime elements of D. This concludes the proof. □

Example 4.12. *The ring $\mathbb{Z}$ of integers, being a Euclidean domain, is a unique fatorization domain.*

General Notions Occurring in Number Theory

N1 The number of primes is infinite.

N2 Let p be a prime and a, b given integers. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

N3 Any two integers have a g.c.d

N4 Given an integer n. n has the prime factorization

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \; (a_i \geq 0, i = 1, 2, \ldots, k)$$

and $p_1, p_2, \ldots, p_k$ are distinct primes.

That is, unique factorization theorem holds for the set of integers

N5 Given an integer n, one could find out the least prime p dividing n

General Notions Occurring in Algebra

A1 Let R be a principal ideal domain. Then R is semi-simple if, and only if, R is either a field or has an infinite number of maximal ideals.

A2 Let D be a Euclidean ring. Suppose that π is a prime element in D. If $\pi \mid ab$ where $a, b \in D$, then π divides either a or b.

A3 Let D be a Euclidean ring. Any two elements $a, b \in D$ have a greatest common divisor.

A4 let D be a Euclidean ring. An element a of D has a unique factorization primes $\pi_1, \pi_2, \ldots, \pi_n$.

That is, $a = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_n^{a_n}$.

A5

Definition 4.13. *Let R be a commutative ring with unity 1_R. Suppose that I denotes an ideal of R. The nil radical of I written $\sqrt{I}$ is the set*

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some integer } n \in \mathbb{Z}(n \text{ varies with } r)\}$$

In the ring $\mathbb{Z}$ of integers, when $n \in \mathbb{Z}$ is such that

$$n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$$

the nil radical of the principal ideal (n) is such that

$\sqrt{(n)} = (p_1p_2\ldots p_k)$ the ideal generated by the product $p_1p_2\ldots p_k$.

For, Let $a = \max\{a_1, a_2, \ldots, a_k\}$. Write the integer $t = p_1p_2\ldots p_k$. Then, $t^a \in$ the ideal generated by n. So, then, $(p_1, p_2, p_k) \subseteq \sqrt{(n)}$, the radical of the ideal generated by n. For some integer m, if $m \in \sqrt{(n)}$, then m is divisible by each of the primes $p_1, p_2, \ldots, p_k$. That is, m is an element of the ideal $(p_1) \cap (p_2) \cap \ldots \cap (p_k) = (p_1p_2\ldots p_k)$. Thus, the nil radical of (n) is the ideal generated by $p_1p_2\ldots p_k$ [1j] One could choose a least prime among the primes.

Referências

[1] David M. Burton: *A first course in RINGS AND IDEALS*, Addison Wesley Publishing Company, Reading, Marsachusetts. Mento Park, California, London. Don Mills, Onatario (1970) page 71.

[1a] .... pp 18–19.

[1b] .... page 73.

[1c] .... pp 296–299.

[1d] .... page 74.

[1e] .... page 18.

[1f] .... page 73.

[1g] .... page 158.

[1h] .... page 162.

[1i] .... page 99.

[1j] .... page 79.

[2] I. N. Hersiten : *Topics in Algera*, Blaisdell Publishing company. Adiwision of Ginn and Company. New York Toronto London First Edition (1964) Third Printing (1965) pp 104–109

[3] T.Motzkin, The Euclidean Algorithm, Bull.Amer.Math,Soc. Vol 55 (1949)pp 1142–1146.

Accept in 12 September 2024.