Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.10, No.3, 2020

www.iiste.org

Some Results on Principal Ideals in Unique Factorization Domain

Aneesa Anwar[1], Mamouna Anwar[2*], Aiman Waheed1[1]

[1]Department of Mathematics, Government College Woman University Faisalabad, Faisalabad, Punjab, Pakistan.

[2*]Department of Mathematics, Bahauddin Zakariya University Multan, Multan, Punjab, Pakistan.

[2*]Department of Mathematics, Institute of Southern Punjab Multan, Multan, Punjab, Pakistan.

[1]Department of Mathematics, Ghazi University Dera Ghazi Khan, Dera Ghazi Khan, Punjab, Pakistan.

[1]aneesaanwargcuf@gmail.com,[2*]mamounaanwar83@gmail.com,
[1]blueeyes50gudgk@gmail.com

Abstract

In this study, the intersection algebra of two principal ideals of the unique factorization domain is explained. The generators of the intersection algebra of two principal ideals. The important and sufficient conditions are obtained for the said intersection algebra to be finitely generated. It is also shown that intersection algebra of principal ideals in the polynomial ring is a semigroup ring.

Keywords: Unique Factorization Domain (UFD), Principal Ideals, Polynomial Ring, Commutative Algebra, Abelian Group, Monomial Ideals, Quasi Polynomial, Noetherian ring.

1. Introduction

The research of the unique factorization domain has an importance in the field of commutative algebra and a very interesting concept is intersection algebra of mathematical structures. In this article, some cases of intersection algebra are discussed in the context of UFD. This research is divided into three parts.

In the first part, the basic definitions and concepts of algebra and especially in commutative algebra are given which are necessary to understand the work, and also some examples are presented to explain the definitions or concepts where it is needed.

In the second part, some important results are given which are already have been proved about the intersection algebra of different mathematical structures. These results are exceptional and helped to complete the work of this research.

In the third Part, the UFD (Unique Factorization Domain) is considered and then studied the intersection algebra of principal ideals. The proof of this section is mainly taken from [1]. In this part, the following results are proved.

An example of the intersection algebra of monomial ideals in the polynomial ring is created to illustrate the theory.

- Found the generators of intersection algebra of principal ideals in UFD.
- Found the if and only if conditions for the intersection algebra to be finitely generated.

It also showed that the intersection algebra of monomial ideals in the polynomial ring is a semigroup ring.

2. Preliminaries

In this section of the article, some basic definitions and introductory concepts of algebra are given in general. Particularly the basic definitions of commutative algebra are given and also some examples are presented to illustrate the concepts. These definitions are taken from [2], [3], [4], [5], [6] and [7].

2.1. Abelian group: "An abelian group is a set A, together with an operation $\cdot$ that combines any two elements a and b to form another element denoted $a \cdot b$. the symbol $\cdot$ is a general placeholder for a concretely given operation. To qualify as an abelian group, the set and operation, $(A, \cdot)$, must satisfy five requirements known as the abelian group axioms:

- **Closure:** For all a, b in A, the result of the operation $a \cdot b$ is also in A .
- **Associativity:** For all a, b and c in A, the equation $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds.
- **Identity element:** There exists an element e in A , such that for all elements a in A , the equation $e \cdot a = a \cdot e = a$ holds.
- **Inverse element:** For each a in A , there exists an element b in A such that $a \cdot b = b \cdot a = e$ where e is the identity element.
- **Commutativity:** For all a, b in A , $a \cdot b = b \cdot a$.

A group in which the group operation is not commutative is called a non-abelian group or non-commutative group"

2.2. Ring: "A ring is a set R equipped with two binary operations $+ and \cdot$ satisfying the following three sets of axioms, called the ring axioms

1. R is an abelian group under addition, meaning that:

- $(a+b)+c = a+(b+c) \forall a, b, c \in R$ (that is, $+$ is associative)
- $a+b = b+a \forall a, b$ in R (that is, $+$ is commutative).
- There is an element 0 in R such that $a+0=a$ for all a in R (that is , 0 is the additive identity)
- For each a in R there exists $-a$ in R such that $a+(-a)=0$ (that is $-a$ is the additive inverse of a).

2. R is a semi multiplicative group, meaning that:

- $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ for all a,b,c in R (that is , $\cdot$ is associative).
- There is an element 1 in R such that $a\cdot 1 = a$ and $1\cdot a = a$ for all in R (that is, 1 is the multiplicative identity).

3. Multiplication is distributive with respect to addition:

- $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ for all a,b,c in R (**left distributivity**)
- $(b+c)\cdot a = (b\cdot a)+(c\cdot a)$ for all a,b,c in R (**right distributivity**)."

2.3. Ideal: Let R be a ring. A sub ring I of R is called an ideal if it satisfies the following conditions:

1.$(I,+)$ is a subgroup of $(R,+)$

2.$\forall x\in I, \forall r\in R$: $\mathrm{x}\cdot\mathrm{r}\in \mathrm{I}$.

Equivalently, a right ideal of R is a right $r-sub\bmod ule$ of R .

Similarly a subset I of R is called left ideal of R if it is an additive subgroup of R absorbing multiplication on the left:

1.$(I,+)$ is a sub group of $(R,+)$

2. $\forall x\in I, \forall r\in R$: $\mathrm{r}\cdot\mathrm{x}\in \mathrm{I}$

Equivalently, a left ideal of R is a left $R-sub\bmod ule$ of R ."

Examples of ideal:

- "In a ring R the set R itself forms an ideal of R. Also, the subset containing only the additive identity 0_R forms an ideal. These two ideals are usually referred to as the trivial ideals of R.
- The set of all polynomials with real coefficients which are divisible by the polynomial x^2+1 is an ideal in the ring of all polynomials.
- The set of all $n-by-n$ matrices whose last row is zero forms a right ideal in the ring of all $n-by-n$ matrices. It is not a left ideal. The set of all $n-by-n$ matrices whose last column is zero forms a left ideal but not a right ideal."

2.4. Polynomial ring: "The polynomial ring, $F[X]$, in X over a field F is defined as the set of expressions, called polynomials in X, of the form

$$p = p_0 + p_1X + p_2X^2 + \cdots + p_{m-1}X^{m-1} + p_mX^m$$

Where $p_0, p_1, ..., p_m$ the coefficient of p, are element of F, and X, X^2 ,are symbols, which are considered as "powers of X", and, by convention, follow the usual rules of exponentiation: $X^0 = 1$, $X^1 = X$, and

$X^k X^l = X^{k+l}$,

For any nonnegative integers k and l. The symbol X is called an indeterminate or variable."

2.5. Principal ideal: "A principal ideal is an ideal in a ring R that is generated by a single element a of R through multiplication by every element of R.

- A left principal ideal of R is a subset of R of the form $Ra = \{ra : r \text{ in R}\}$;
- A right principal ideal is a subset of the form $aR = \{ar : r \text{ in R}\}$;
- A two sided principal ideal is a subset of all finite sums of elements of the form ras, namely, $RaR = \{r_1as_1, + \cdots + r_nas_n : r_1, s_1, ..., r_n, s_n \text{ in R}\}$.

  While this definition for two-sided principal ideal may seem to contrast with the others, it is necessary to ensure that the ring remains closed under addition.

If R is a commutative ring, then the above three notions are all the same. In that case, it is common to write the ideal generated by a as $\langle a \rangle$."

2.6. Integral domain: "An integral domain is basically defined as a nonzero commutative ring in which the product of any two nonzero elements is nonzero.

- An integral domain is a nonzero commutative ring with no nonzero divisors.
- An integral domain is a commutative ring in which the zero ideal $\{0\}$ is a prime ideal.
- An integral domain is a nonzero commutative ring for which every nonzero element is cancellable under multiplication."

Examples:

- "The archetypical example is the ring Z of all integers.
- Every field is an integral domain. For example, the field F of all real numbers is an integral domain. Conversely, every artinian integral domain is a field. In particular, all finite integral domains are finite fields. The ring of integers Z provides an example of a non-Artinianinfinite integral domain that is not a field, possessing infinite descending sequences of ideals such as:

  $Z \supset 2Z \supset \cdots \supset 2^n Z \supset 2^{n+1} Z \supset \cdots$
- Rings of polynomials are integral domain if the coefficients come from an integral domain. For instance, the ring $Z[x]$ of all polynomials in one variable with integer coefficients is an integral domain; so is the ring $C[x_1, ..., x_n]$ for all polynomials in $n-$ variables with complex coefficients."

2.7. Unique factorization domain: "A unique factorization domain is defined to be an integral domain R in which every non-zero element x of R can be written as a product (an empty product if x is a unit) of irreducible elements p_i of R and a unit u :

$x = up_1 p_2 ... p_n$ With $n \geq 0$

And this representation is unique in the following sense: If $q_1,...,q_m$ are irreducible elements of R and w is a unit such that

$x = wq_1q_2...q_m$ With $m \geq 0.$

Then $m = n$, and there exists a bijective map $\varphi:\{1,...,n\} \to \{1,...,m\}$ such that p_i is associated to $q_{\varphi(i)}$ for $i \in \{1,...,n\}$.

A unique factorization domain is an integral domain R in which every non-zero element can be written as a product of a unit and prime elements of R ."

Examples:"Most rings familiar from elementary mathematics are UFDs:

1. All principal ideal domains, hence all Euclidean domains, are UFDs. In particular, the integers (also see fundamental theorem of arithmetic), the Gaussian integers and the Eisenstein integers are UFDs.
2. $Z\left[e^{\frac{2\pi i}{n}}\right]$ is a UFD for all integers $1 \leq n \leq 22$,but not for $n = 23$.
3. If R is a UFD, then so is $R[X]$, the ring of polynomials with coefficients in R. Unless R is a field, $R[X]$ is not a principal ideal domain. By iteration, a polynomial ring in any number of variables over any UFD (and in particular over a field)is a UFD.
4. The Auslander-Buchsbaum theorem states that every regular local ring is a UFD."

2.8. Radical of an ideal: "The radical of an ideal I in a commutative ring R , denoted by Rad(I) or $\sqrt{I}$ is defined as

$\sqrt{I} = \{r \in R \mid r^n \in I\}$ for some positive integer n

Intuitively, one can think of the radical of I as obtained by taking all the possible roots of elements of I . Equivalently, the radical of I is the pre-image of the ideal of nilpotent elements (called nilradical) in R/I . The latter shows $\sqrt{I}$ is an ideal itself, containing I

If an ideal I coincides with its own radical, then I is called a radical ideal or semiprime ideal."

Examples:"Consider the quotient ring

$R = C[x, y]/(y^4)$. Notice that any morphism $R \to C$ must have y in the kernel in order to have a well-defined morphism (if we said, for example, that the kernel should be $(x, y-1)$ the composition of $C[x, y] \to R \to C$ would be $(x, y^4, y-1)$ which is the same as trying to force $1 = 0$). Since C is algebraically closed, every morphism $R \to F$ must factor through C ,so we only have the compute the intersection of $\{\ker(\Phi):\Phi \in Hom(R,C)\}$ to compute the radical of (0) . We then find that $\sqrt{(0)}=(y)\subset R.$

Consider the ring Z of integers:

- The radical of the ideal $4Z$ of integer multiples of 4 is $2Z$
- The radical of $5Z$ is $5Z$
- The radical of $12Z$ is $6Z$ ”

2.9. Monomial ideal: “A monomial ideal is an ideal generated by some monomials in a multivariate polynomial ring over a field

An ideal I that can be written

$$I=\left\{\sum a_\alpha x^\alpha \mid \alpha \in A, a_\alpha \in k\right\}$$

For some $A \subseteq Z_{\geq 0}^n$ is a monomial ideal.

An ideal I in $S=Q[x_1,...,x_n]$ is called a monomial ideal if it satisfies any of the following equivalent conditions:

(a) I is generated by monomials,
(b) If $f=\sum_{\alpha\in N^n} k_\alpha x^\alpha$ belongs to I then $x^\alpha \in I$ whenever $k_\alpha \neq 0$,
(c) I is torus-fixed; in other words, if $(c_1,...,c_n)\in (Q^*)^n$ then I is fixed under the action $x_i \mapsto c_i x_i$ for all i ”

Example: Let $I\langle x^2\rangle$. Then I is a monomial ideal and $A=\{n \in | Z, n\geq 2\}$

2.10. Semigroup ring: “Let G be a monoid. Let R be a ring. Then the semi group ring of G over R is actually the structure that can be seen as the set of formal sums,

$$\sum_{g\in G} r_g g$$

Where $r_g \in R$ and $g\in G$ and $r_g=0$ for all but finitely many g .

Note: Actually the semi group ring can be seen as the direct product of R with its copies. For each element of G . There is one copy of R .

2.11. Noetherian ring: “In mathematics, more specifically in the area of abstract algebra known as ring theory, a noetherian ring is a ring that satisfies the ascending chain condition on ideals; that is, given any chain of ideals:

$$I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

There exists an n such that:

$$I_n = I_{n+1} = \cdots$$

There are other equivalent formulations of the aNoetherian ring.

For non-commutative rings, it is necessary to distinguish between three very similar concepts:

- A ring is left-noetherian if it satisfies the ascending chain condition on left ideals.
- A ring is right-noetherian if it satisfies the ascending chain condition on right ideals.
- A ring is noetherian if it is both left-and right-noetherian.

For commutative rings, all three concepts coincide, but in general they are different.”

Examples:

- “Any field, including fields of rational numbers,real numbers, and complex numbers, is noetherian. (A field only has two ideals itself and (0))
- Any principal ideal domain, such as the integers, is noetherian since every ideal is generated by a single element.”

2.12. Ascending chain condition: “The ascending chain condition (ACC) and descending chain condition (DCC) are finiteness properties satisfied by some algebraic structures, most importantly ideals in certain commutative rings.

A partially ordered set (poset) P is said to satisfy the ascending chain condition (ACC) if every strictly ascending sequence of elements eventually terminates.

Equivalently, given any sequence

$$a_1 \le a_2 \le a_3 \le \cdots,$$

There exists a positive integer n such that

$$a_n = a_{n+1} = a_{n+2} = \cdots\text{”}$$

2.13. Prime ideal: “A prime ideal is a proper ideal whose complement is closed under multiplication.

This is equivalent to saying:

$$ab \in p \Leftrightarrow a \in p \text{ or } \mathrm{b} \in \mathrm{p}$$

An ideal P of a commutative ring R is prime if it has the following two properties:

- If a and b re two elements of R such that their product ab is an element of P, then a is in P or b is in P ,
- P is not equal to R for the whole ring.”

Examples:

- "A simple example: For $R = Z$. the set of even numbers is a prime ideal
- In the ring $Z[X]$ of all polynomials with integer coefficients, the ideal generated by 2 and X is a prime ideals. It consists of all those polynomials whose constant coefficient is even."

2.14. Quotient ring: "A quotient ring, also known as factor ring, difference ring or residue class ring, is a construction quite similar to the quotient groups of group theory and the quotient spaces of linear algebra. It starts with a ring R and a two sided ideal I in R, and constructs a new ring, the quotient ring R/I , whose elements are the cosets of I in R subject to special $+$ and $\cdot$ operations."

2.15. Local ring: "A ring R is a local ring if it has any one of the following equivalent properties:

- R has a unique maximal left ideal.
- R has a unique maximal right ideal.
- $1 \neq 0$ and the sum of any two non-units in R is a non-unit.
- $1 \neq 0$ and if x is any element of R, then x or $1-x$ is a unit.
- If a finite sum is a unit, then it has a term that is unit(this says in particular that the empty sum cannot be a unit, so it implies $1 \neq 0$)

A local ring that is an integral domain is called a local domain."

Examples:

- "All fields (and skew fields) are local rings, since $\{0\}$ is the only maximal ideal in these rings.
- A nonzero ring in which every element is either a unit or nilpotent is a local ring.
- An important class of local rings is discrete valuation rings, which are local principal ideal domain that are not fields.
- Quotient rings of local rings are local."

2.16. Commutative ring: "A ring is a set R equipped with two binary operations, i.e operations combining any two elements of the ring to a third. They are called addition and multiplication and commonly denoted by $+$ and $\cdot$;e.g. $a+b$ and $a \cdot b$. To form a ring these two operation have to satisfy a number of properties: the ring has to be an abelian group under addition as well as a monoid under multiplication, where multiplication distributes over addition; i.e.,

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

The identity elements for add multiplication are denoted 0 and 1, respectively. The coordinate plan had four different quadrants.

If the multiplication is commutative, i.e

$$a \cdot b = b \cdot a$$

Then the ring R is called commutative. In the reminder of this article, all rings will be commutative, unless explicitly stated otherwise."

Example: "An important example, and in some sense crucial,is the ring of integers Z with the two operations of addition and multiplication. As the multiplication of integers is a commutative operation, this is a commutative ring. It is usually denoted Z as an abbreviation of the German word Zahlen (numbers)

A field is a commutative ring where every non-zero element a is invertible; i.e. has a multiplicative inverse b such that $a.b = 1$

Therefore, by definition, any field is a commutative ring. The rational, real andcomplex numbers form field. If R is a given commutative ring, then the set of all polynomial in the variable X whose coefficient are in R forms the polynomial ring, denoted $R[X]$. The same holds true for several variables."

2.17. Module: "Let R be a ring and M an abelian group. We call M a left $R-\text{mod}ule$ if there is a function

$$R \times M \to M : (r,m) \mapsto rm,$$

Called a scalar multiplications, satisfying

1. $(r+s)m = rm + sm$
2. $r(m+n) = rm + rn, and$
3. $(rs)m = r(sm)$

For all $r, s \in R,$ $\text{m,n} \in \text{G}.$

We call R the ring of scalars of M .

We can also define a right $R-\text{mod}ule$ analogously by using a function

$$M \times R \to M : (m,r) \mapsto mr.$$

In particular the third property then reads

$$m(rs) = (mr)s$$

Note that the two notions coincide if R is a commutative ring, and in this case we can simply say that M is an R-module."

Examples of module:

- The $K-\text{mod}ules$ over a field K are simply the K -vector spaces.
- Any matrix ring of a ring R is a R-module under componentwise scalar.

2.18. Submodules: Given a left R-module M a submodule of M is a subset $N \subseteq M$ satisfying

1. N is a subgroup of M and
2. For all $r \in R$ and all $n \in N$ we have $rn \in N$

The second condition above states that submodules are closed under left multiplication by elements of R ; it is implicit that they inherit their multiplication from their containing module;

$R \times N \to N$ must be the restriction of $R \times M \to M$

Examples: Any module M is a submodule of itself, called the improper submodule, and the zero submodule consisting onlyof the additive identity of M , called the trivial submodule.

- A left ideal I is a submodule of R viewed as an S -module, where S is any(not necessarily proper) subring of R

2.19. Quasi polynomial: "A quasi polynomial (pseudo polynomial) is a generalization of polynomials. While the coefficients of a polynomial come from a ring, the coefficients of quasi polynomial are instead periodic functions with integral period. Quasi polynomial appear throughout much of combinatorics as the enumerators for various objects.

A quasi polynomial can be written as

$$q(k) = c_d(k)k^d + c_{d-1}(k)k^{d-1} +,...,+c_0(k)$$

Where $c_i(k)$ is a periodic function with integral period. If $c_d(k)$ is not identically zero, then the degree of q is d

Equivalently, a function $f : N \to N$ is a quasi-polynomial if there exist polynomials $p_0,..., p_{s-1}$ such that $f(n) = p_i(n)$ when $n \equiv i \bmod s$. The polynomials p_i are called the constituents of f ."

Example: Given two quasi polynomial F and G , the convolution of F and G is

$$(F * G)(k) = \sum_{m=0}^{k} F(m)G(k-m)$$

Which is a quasi-polynomial with degree $\leq \deg F + \deg G + 1$.

2.20. Characteristic of ring: "The characteristic of a ring R , often denoted char(R) , is defined to be the smallest number of times one must use the rings multiplicative identity(1) in a sum to get the additive identity(0) if the sum does indeed eventually attain 0; the ring is said to have characteristic zero if this sum never reaches the additive identity.

That is, $char(R)$ is the smallest positive number n such that

$$\underbrace{1+\cdots+1}_{n \text{ summands}}=0$$

If such a number n exists, and 0 otherwise.

The characteristic may also be taken to be the exponent of the rings additive group, that is, the smallest positive n such that

$$\underbrace{a+\cdots+a}_{n \text{ summands}}=0$$

For every element a of the ring (again, if n exists; otherwise zero)."

2.21. Dimension of ring: "The Krull dimension has been introduced to provide an algebraic definition of the dimension of an algebraic variety: the dimension of the affine varity defined by an ideal I in a polynomial ring S is the krull dimension of S/I"

2.22. Power of an ideal: "Let R be a commutative unital ring I be an ideal in R . The n^{th} power of I , denoted I^n ,is defined in the following equivalent ways:

- It is the ideal generated by n -fold products of elements from I
- It is the product of the ideal I with itself, n times.

In symbols, it is the additive subgroup generated by elements of the form $a_1a_2...a_n$ where $a_i \in I$. The second power of an ideal is termed its square, and the third power is termed its cube."

2.23. Generators of ideals:

- Let R be a commutative ring.
- Let $I \subset R$ be an ideal.
- Let $S \subset I$ be a subset.

Then S is a generator of I if and only if I is the ideal generated by S .

2.24. Generator of power of ideal: let I be a graded ideal in a polynomial ring R , which is generated minimally by $x_1,\cdots,x_k$. Then the power of I, i.e I^t is generated by monomials of the form $x_1^{a_1},...,x_n^{a_n}$ where $a_1+...+a_n=t$. Denote this set by S ."

2.25. Noetherian filtration: An a noetherian A is called filtered, if for every non-negative integer i there is a subspace A_i such that

1) $A_i \subseteq A_j$ if i ≤ j,
2) $A_i \cdot A_j \subseteq A_{i+j}$
3) $A=\bigcup_{i=0}^{\infty} A_i.$

The set $\{A_i \mid i \in N\}$ is called a filtration of A.

3. Literature Review

During recent years a lot of research has been done in this region of commutative algebra. For instance see [8], [9], [10], [11], [12], [13], [14] and [15]. Some results are presented here.

A lot of studies have been done since the definition of monomial ideals of a ring. Because it is really easy to deal with the monomial ideals and in this way, we can prove some results about the generic ideals in the case of the polynomial ring. Because we can generalize the results from the monomial ideals to any ideal generated by polynomials.

In [8] the authors consider A such that $j_i \subseteq \sqrt{I} \forall i$. The authors took I is not nilpotent. Let A be a commutative noetherian ring with identity and I, J ideals in A with $J \subseteq \sqrt{I}$. Also,assume that the ideal I is not nilpotent and $\bigcap_k I^K = (0)$. Then for each positive integer m one can define $v_1(J,m)$ to be the largest integer n such that $J^m \subseteq I^n$. Similarly , $w_J(I,n)$ is defined to be the smallest integer m such that $J^m \subseteq I^n$ .Then the following results are found.

Definition: [8]"Let A be a noetherian ring. We say that $v : A \to \mathbf{Z} \cup \{\infty\}$ is a discrete valuation on A if $\{x \in A \mid v(x) = \infty\}$ is a prime ideal P , v factors through $A \to A/P \to \mathbf{Z} \cup \{\infty\}$, and the induced function on A/P is a rank one discrete valuation on A/P. If I is an ideal in A , then we denote $v(I) := \min\{v(x) \mid x \in I\}$."

If R is a noetherian ring, we denote by $\overline{R}$ the integral closure of R in its total quotient ring $Q(R)$.

Definition: [8]"Let I be an ideal in a noetherianring A. An element $x \in A$ is a said to be integral over I if x satisfies an equation $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in I^i$. The set of all elements in A that are integral over I is an ideal $\overline{I}$,and the ideal I is called integrally closed if $I = \overline{I}$ .If all the powers I^n are integrally closed, then I is said to be normal.

After the above definition the author gave an interesting remark."

Remark: [8]with the notation established above, for every positive integer n we have

$$\overline{I^n} = \bigcap_{i=1}^{h} I^n V_i \cap R.$$

In particular, we have the following.

Remark: [8]If K, L are ideals in $A, v_1, \cdots, v_h$ are the Rees valuations of L ,and $v_i(K) \geq v_i(L)$ for all $i = 1, ..., h,$ then $\overline{K} \subseteq \overline{L}$.

Definition: [8]A local noetherian ring (A, m) is analytically unramified if its m-adic completion $\hat{A}$ is reduced.

Theorem: [8]Let A be a locally analytically unramified ring .Then for each $j = 1, ..., r$ we have

$$E_j \cap Q^{k+1} \subseteq C \cap (D_j \times R_{\geq 0}) \subseteq \overline{E_j}.$$

Theorem: [8] Let $a_1, ..., a_k$ be thereal numbers. The limit

$$\lim_{m_1, ..., m_k \to \infty} \frac{v_1(\underline{J}, m_1, ..., m_k)}{a_1 m_1 + \cdots + a_k m_k}$$

exists if and only if there exists a rational number l such that $la_s = \alpha_{s1} = \alpha_{s2} = \cdots = \alpha_{sr}$ for all $s = 1, ..., k.$ In this case the limit is equal to l .

Theorem: [8]Assume that the ideal I has only one Rees valuation. Then the limit

$$\lim_{m_1, ..., m_k \to \infty} \frac{v_1(\underline{J}, m_1, ..., m_k)}{a_1 m_1 + \cdots + a_k m_k}$$

exists if and only if

$$l_1(J_1)/a_1 = \cdots = l_1(J_k)/a_{k.}$$

In mathematics a unique factorization domain is an integral domain.

A commutative ring in which the product of non-zero element is non-zero non-unit element can be written as a product of prime elements uniquely up to orders an units.

In [9] the authors discussed some results about monomial ideals. Let $A = K[x_1, ..., x_d]$ with $x_1, ..., x_d$ indeterminates and B be a $sub-k-a\lg ebra$ of A generated by monomials in $x_1, ..., x_d$ .Then B is also a $sub-k-a\lg ebra$ module of A ,generated over K as a module by monomials.

Theorem: [9]If M_1 and M_2 are finitely generated submonoids of N^m , then so is

$$M = M_1 \cap M_{2.}$$

Theorem: [9]If $I_1, I_2 \subset k[x_1,...,x_d]$ are monomial ideals, then the length functions f_k are quasipolynomial for all $k \geq 0$.

Theorem:[9]If I is an ideal generated by finitely many monomials, then $K = conv(\log I)$ is the intersection of finitely many closed half-spaces.

Theorem: [9]Let $H_{1,1}^+,...,H_{1,k_1}^+,...,H_{n,1}^+,...,H_{n,k_n}^+$ be half-spaces, and let

$$Q_{a_1,...,a_n} = \bigcap_{i,j} a_i H_{i,j}$$

be a family of polytopes indexed by $a_1,...,a_n$. Then the volume of $Q_{a_1,...,a_n}$ is a continuous function of $a_1,...,a_n$. In addition, there exist a finite number of hyper planes in $R_{\geq 0}^n$ such that for $a_1,...,a_n$ not contained in any of the hyper planes, the volume of the polytope $Q_{a_1,...a_n}$ is given by a degree d form in $a_1,...,a_n$.

Theorem: [9]If $I_1,...,I_n$ are each generated by a single monomial, then f_0 has the form given in the above theorem, hence is quasipolynomial of degree $d+2$.

Theorem: [9]Let I and J be monomial ideals in $R = [x_1,...,x_d]$, where k has characteristic p , and let $S = R/I$ .Assume $I+J$ is m_R -primary. Then the Hilbert-Kunz function, $HK_{S,J}(e)$, is eventually a polynomial of degree $\dim S$ in p^e .

Definition: [9]If $M_1 = \cdots = M_N = M, I_1,...,I_n$ are all principal ideals, and R has characteristic $p > 0$, then the function $HK_{M,I} : a \to f_0(p^a,...,p^a)$ is called the Hilbert-Kunz function on M of the ideal $I = I_1 + \cdots + I_n$. The more standard definition is in term of bracket powers,

$$I^{[p^e]} = \left(\left\{ i^{p^e} \mid i \in I \right\}\right).$$

With this notation,

$$HK_{M,J}(a) = length\left(M / I^{[p^e]} M\right).$$

Because R has characteristic p , $I^{[p^e]} = I_1^{p^e} + \cdots + I_n^{p^e}$,which shows that $HK_{M,I}$ is dependent only on I and not on the choice of $I_1,...,I_n$

Theorem: [9] If H is a half-space containing $\log I$,then aH contains $\log I^a$.

Theorem: [9]If I is generated by h monomials, and if K is the convex hull of $\log(I)$, then

$$\log(I^a) \supset Z^d \cap (a+h)K.$$

Theorem: [9] Let A be a subset of R^d such that both A and its boundary ∂A

have finite volume. Then

$$vol(A) - vol(\partial A)\sqrt{2} \le \#(A) \le vol(A) + vol(\partial A)\sqrt{2}$$

Theorem: [9]Fix $(b_1,...,b_n) \in N^n, a > 0.$ then

$$\lim_{m\to\infty} \frac{length\left(\dfrac{R}{I_1^{mb_1} + \cdots + I_n^{mb_n}}\right)}{vol\left(\bigcap_i mb_i A_i\right)} = 1$$

In [12] the authors proved very important and interesting results about power of ideals. A be commutative noetherian ring with unit a and b two ideals of A . By “radical of a” mean the ideal $R(a)$ composed of the $x \in A$ such that some power of x lies in a.

Theorem: [12]the sequences $\left(\upsilon_b(a,n)/n\right)$ and $\left(w_b(a,n)/n\right)$ infinite) limits $l_b(a)$ and $L_b(a)$.

Theorem: [12]the operations of multiplication and addition are compatible with the equivalence relation $a \sim b$ between ideals of A .

Theorem: [12](“Cancellation law”). If α, β and β' are equivalence classes of ideals of A having the same radical,the relation $\alpha\beta = \alpha\beta'$ implies $\beta = \beta'$.

Theorem: [12] the relations $\beta \ge \alpha$ and $\beta = \beta + \alpha$ in $\Im(A)$ are equivalent.

Theorem:[12]If α^s and α^t are defined in $\Im(A)$,then α^{s+t} is defined, and one has $\alpha^{s+t} = \alpha^s\alpha^t$ .If α^s and α^{st} are defined in $\Im(A)$,then $(\alpha^s)^t$ is defined and one has $\alpha^{st} = (\alpha^s)^t$. If α^s and β^s are defined in $\Im(A)$, then $(\alpha\beta)^s$ is defined ,and one has $\alpha^s\beta^s = (\alpha\beta)^s$.

Theorem: [12]the relation $\alpha^s = \alpha^t$ implies $s = t$. The relation $\alpha^s = \beta^s$ implies $\alpha = \beta.$

Theorem: [12] If $\overline{\alpha} \ne \overline{\beta}$, then $\alpha^x\beta^y = \left(\alpha^{u'}\beta^{v'}\right)^w$ implies

$$x = u'w \text{ and } y = v'w.$$

Theorem: [12]If $\overline{\alpha} \neq \overline{\beta}$, and when elements α and β are chosen in $\overline{\alpha}$ and $\overline{\beta}$, then the ratio s/t is uniquely determined by $\overline{\gamma}$.

Theorem:[12] Let A be a local ring of dimension $d \geq 1, b$ an ideals of A which is primary for the ideal od non units , and a an ideal of A such that $\dim(A/a) < d$.Then $l_s(a)$ is defined , and is a finite real numbers.

In [13] the author proved the important results about Noetherian filtration and finite algebra. Some are presented here.

Definition:[13]A ring A is said to be Noetherian if it satisfies the ascending chain condition on ideals, i.e. for any increasing chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals of R there exists an integer K such that $I_n = I_k$ for all $n \geq k$. A left $A-\text{mod}ule\ M$ is Noetherian if it satisfies the ascending chain condition on submodules.

Definition: [13]Let A be a ring. If A has a maximal ideal m , then we say that A is a local ring, denoted (A, m) .

Definition: [13] A unique factorization domain is defined to be an integral domain R in which every non-zero element x of R can be written as a product (an empty product if x is a unit) of irreducible elements p_i of R and a unit u:

$x = u\, p_1 p_2 ... p_n$ With $n \geq 0$

and this representation is unique in the following sense: If $q_1, ..., q_m$ are irreducible elements of R and w is a unit such that

$x = w\, q_1 q_2 ... q_m$ With $m \geq 0$,

then $m = n$, and there exists a bijectivemap

$$\varphi : \{1, ..., n\} \to \{1, ..., m\}$$

such that p_i is associated to $q\varphi_{(i)}$ for $i \in \{1, ..., n\}$.

Definition: [13]A principal ideal domain is an integral domain in which every proper ideal can be generated by a single element. The term "principal ideal domain" is often abbreviated P.I.D. Examples of P.I.D.s include the integers, the Gaussian integers, and the set of polynomials in one variable with real coefficients

Definition: [13] A pair (I,J) of ideals of a ring A , call the algebra $\beta=\oplus_{r,s}\left(I^r\cap J^s\right)u^r v^s$ the intersection algebra of I and J . If this algebra is finitely generated over R, we say that I and J have finite intersection algebra.

Definition: [13]Let A be a Noetherian ring, and I,J ideals in A with $J\subseteq\sqrt{I}$. Also assume that I is not nilpotent and $\bigcap_k I^k=(0)$. Then for each positive integer m ,define $v_1(J,m)$ to be the largest n such that $J^m\subseteq I^{n.}$. Also, we can examine the sequence $\{v_1(J,m)\}_m$, which here we will abbreviate to $v(m)$.

Theorem: [13]let R be aUnique factorization domain and I,J principal ideals in R . Then I,J have finite intersection algebra.

Theorem:[13]For any $a,b,c,d\in \mathrm{N}, \max(a-b,c-d)+\max(b,d)=\max(a,c)\Leftrightarrow \left((a-b)-(c-d)\right)(b-d)\geq 0.$

Theorem:[13]Let R be a principal ideal domain with I,J ideals in R . Then I and J have finite intersection algebra.

Theorem:[13]Let I,J be ideals in a Noetherian local ring A such that $J\subseteq\sqrt{I}$, the ideals I,J are not nilpotent, and $\bigcap_k I^k=(0)$. Assume that J is principal and the ring $\beta=\oplus_{m,n}J^m\cap I^n$

isNoetherian. Then there exists a positive integer t such that

$$v(m+t)=v(m)+v(t)$$

for All $m\geq t.$

Theorem: [13]Let R be a unique factorization domain and I and J nonzero principal ideals in R such that

$$J\subseteq\sqrt{I}$$

Then there exists a positive integer t such that

$$v(m+t)=v(m)+v(t).$$

Some Results on Principal Ideals in Unique Factorization Domain

In this analysis throughout the ring will be a polynomial ring. Also in this analysis, our ring will be commutative.

The aim of this chapter to study the intersection of two principal ideals and powers of the principal ideals. The concept of intersection algebra is used to study the said structures. Also, find the generators of the intersection of two principal ideals and also the intersection of powers of these principle ideals in the Noetherian ring. Our Noetherian ring is a polynomial ring.

Let S is a polynomial ring and I and J are ideals of S . Then the intersection algebra of these ideals is a structure which is denoted and defined as

$$B = \oplus_{n,m\in N} I^n \cap J^m$$

Further we introduced two new variables u_1, u_2 then the intersection algebra can be redefined as

$$B_s(I,J) = \sum_{n,m\in N} I^n \cap J^m u_1^n u_2^m$$

Clearly $B_s(I,J) \subseteq S[u_1,u_2]$.

If this algebra has finite generators then is called finitely generated.

The concept is illustrated with the help of following example.

Let $S = k[x_1, x_2]$ be a ring and let $I = (x_1^3 x_2^3)$ and $J = (x_1 x_2^4)$. Then the elements of the intersection algebra B will be of the form

$$k_1 + k_2 x_1^{10} x_2^{13} u_1^3 u_2^3 + k_3 x_1^7 x_2^{16} u_1^2 u_2^4 + k_4 x_1^{17} x_2^{17} u_1^4 u_2^4$$

Clearly $k_1, k_2, k_3, k_4 \in I^0 \cap J^0$, and

$$x_1^{10} x_2^{13} u_1^3 u_2^3 \in I^3 \cap J^3 u_1^3 u_2^3 = (x_1^9 x_2^6) \cap (x_1^3 x_2^{12}) u_1^3 u_2^3 = (x_1^9 x_2^{12}) u_1^3 u_2^3$$

And

$$x_1^7 x_2^{16} u_1^2 u_2^4 \in I^2 \cap J^4 u_1^2 u_2^4 = (x_1^6 x_2^4) \cap (x_1^4 x_2^{16}) u_1^2 u_2^4 = (x_1^6 x_2^{16}) u_1^3 u_2^3$$

And with this example it is clear that this algebra has natural grading that is N^2 -grading.

A semi group G is called an affine semigroup if there is an isomorphism between G and any subgroup of Z^d for some integer d .

An affine semigroup is called pointed if it contain the identity element.

We consider any two sets of numbers $A = \{a_1, ..., a_n\}$ and $B = \{b_1, ..., b_n\}$ then these sets of numbers are called fan ordered if

$\frac{a_i}{b_i} \geq \frac{a_{i+1}}{b_{i+1}}$ for all $i = 1,...,n-1$

If there exists a fan order between A and B. And if $a_{i+1} = b_0 = 0$ and $a_0 = b_{n+1} = 1$.

Let

$m_i = \left\{ \lambda_1 (b_i, a_i) + \lambda_2 (b_{i+1}, a_{i+1}) \mid \lambda_1, \lambda_2 \in R_{\geq 0} \right\}$

Then the fan associated with these sets of numbers is defined as

$\sum_{A,B} = \{ m_i \mid i = 0,...,n \}$

Theorem3.1

If S be a unique factorization domain. Let $I = \left(w_1^{a_1},..., w_n^{a_n} \right)$ and $J = \left(w_1^{b_1},..., w_2^{b_n} \right)$ are principal ideals generated by irreducible elements. Let $\sum_{A,B}$ be the associated fan for $A = \{a_1,...,a_n\}$ and $B = \{b_1,...,b_n\}$. Then the intersection algebra is generated by the set

$$\{ w_1^{a_1 r_{ij}},..., w_i^{a_i r_{ij}} w_{i+1}^{b_{i+1} s_{ij}},..., w_n^{b_n s_{ij}} \mid i = 0,...,n, \ j = 1,...,n_i \}$$

Where (r_{ij}, s_{ij}) run over the Hilbert basis for each $Q_i = m_i \cap Z^2$ where $m_i \in \sum_{A,B}$.

Proof:

As we already know that the intersection algebra is N^2-graded. So to complete the proof of theorem we will consider only a homogenous monomial from algebra. Let $b \in B$.

Let

$$\deg(b) = (r, s)$$

Where $(r,s) \in m_i \cap Z^2$ for some $m_i \in \sum_{A,B}$, hence $(r,s) \in N^2$.

Now according to the definition of associated fan

$$\frac{a_i}{b_i} \geq \frac{s}{r} \geq \frac{a_{i+1}}{b_{i+1}}$$

Now if we consider $\frac{a_i}{b_i} \geq \frac{s}{r}$ then $a_i r \geq b_i s,$ and by the ordering of a_i, b_i we can easily see that

$$a_j r \geq b_j s \forall j < i$$

If we consider $\frac{s}{r} \geq \frac{a_{i+1}}{b_{i+1}}$ then $a_{a_{i+1}} r \leq b_{i+1} s$ and by same argument we can easily see that

$$a_j r \leq b_j s \forall j > i$$

So

$$b \in I^r \cap J^s u^r v^s$$

$$b \in \left(w_1^{a_1}, \dots, w_n^{a_n}\right)^r \cap \left(w_1^{b_1}, \dots, w_n^{b_n}\right)^s u^r v^s$$

$$b \in \left(w_1^{a_1 r}, \dots, w_i^{a_i r} w_{i+1}^{b_{i+1} s}, \dots, w_n^{b_n s}\right) u^r v^s$$

As b belong to this ideal then b will be of the type

$$b = g w_1^{a_1 r}, \dots, w_i^{a_i r} w_{i+1}^{b_{i+1} s}, \dots, w_n^{b_n s} u^r v^s$$

Where $g \in S$ be a monomial.

Now since $(r, s) \in Q_{i,}$ so this ordered pair has a decomposition of the form

$$(r, s) = \sum_{j=1}^{n_i} q_j \left(r_{ij}, s_{ij}\right)$$

Where $q_j \in \mathbb{N}$. Hence $r = \sum_{j=1}^{n_i} q_j r_{ij}$ and $s = \sum_{j=1}^{n_i} q_j s_{ij.}$

Therefore

$$b = g\left(w_1^{a_1 r}, \dots, w_i^{a_i r} w_{i+1}^{b_{i+1} s}, \dots, w_n^{b_n s} u^r v^s\right)$$

Further

$$b = g \prod_{j=1}^{n_i} w_1^{q_j\left(a_1 r_{ij}\right)}, \dots, w_i^{q_j\left(a_i r_{ij}\right)} w_{i+1}^{q_j\left(b_{i+1} s_{ij}\right)}, \dots, w_n^{q_j\left(b_n s_{ij}\right)} u^{q_j r_{ij}} v^{q_j s_{ij}}$$

As q_j is common power of every term so we can write it as

$$b = g \prod_{j=1}^{n_i} \left(w_1^{a_1 r_{ij}}, \dots, w_i^{a_i r_{ij}} w_{i+1}^{b_{i+1} s_{ij}}, \dots, w_n^{b_n s_{ij}} u^{r_{ij}} v^{s_{ij}}\right)^{q_j}$$

This shows that every monomial of ring S is generated by finite set of generators, which complete the proof of the theorem.

Definition 3.2 Let F be a field. The semigroup ring $F(G)$ of a semigroup G is the $F-a\lg ebra$ with $F-basis$ $\{l^a \mid a \in G\}$ and multiplication defined as

$$l^a \cdot l^b = l^{a+b}$$

When $K = \{ f_1, ..., f_i \}$ is a collection of monomial in W

$F(K)$ is equal to the semigroup ring $F(G)$, where

$$G = \mathrm{N}\log(f_1)+,...,+\mathrm{N}\log(f_i)$$

is the subsemigroup of N^i generated by $\log(K)$

Let B both as an $W-a\lg ebra$ and as a $F-a\lg ebra$ and keep in mind which structure one is considering when proving results. While there are important distinctions between the two, finite generation as an algebra over W is equivalent to finite generation as algebra over F .

Theorem 3.3

Let S be a ring that is finitely generated as an algebra over a field F . Then B is finitely generated as an algebra over S iffit is finitely generated as an algebra over F .

Proof:

Let B be finitely generated over F .

Which means there must exists a finite subset of F which generate B . So every element of B can be written as a combination of those elements.

Since

$$F \subset S$$

So the subset which generates B is also subset of S .

Hence B is automatically finitely generated over S .

Let $\{c_1, ..., c_n\}$ be the set of generators. For any $c \in B$,

We have

$$c = \sum_{i=1}^{q} r_i c_i^{\beta i} \text{ Where } r_i \in S$$

Where β_i 's are integral powers.

But we know that S is finitely generated over F , which means every element of S can be written as a combination of elements of finite subset of F .

Say that set is $\{s_1, ..., s_m\}$,

So

$$r_i = \sum_{j=1}^{p} a_{ij} s_j^{\chi_{ij}} \text{ where } a_{ij} \in F$$

So

$$c = \sum_{e}^{i} \left(\sum_{j}^{p} a_{ij} s_j^{\chi_{ij}} \right) c_i^{\beta i}$$

B is finitely generated as an algebra over F with $\{c_1, ..., c_n, s_1, ..., s_m\}$,which is proved complete proof of the theorem.

Definition3.4 Let $S = F[x]$ and $x = \{x_1, ..., x_n\}$ be the set generators. Then $F[x] = F[x_1, ...x_n]$ it is the polynomial ring over a field F . It contains n number of variables.

Suppose $A = \{f_1, ..., f_q\}$ in which set the number of elements are finite. So this called the finite

set of distinct monomials in S . Such that

$$f_i \neq 1 \quad \forall i$$

The monomial subring spanned by A is the $F - suba\lg ebra.$

$$F[A] \subset S$$

We know that $F[A] = F[f_1, ...f_q]$

Then

$$F[A] = F[f_1, ...f_q] \subset S$$

Definition 3.5 A monomial, also called power product. A monomial is a product of powers of variables with nonnegative integer exponent.

For any $d \in \mathrm{N}^n$, the set $x^d = x_1^{d_1}, ..., x_n^{d_n}$ where $d = \{d_1, ...d_n\}$ is the set of nonnegative integer exponents.

Suppose that f is a monomial in polynomial ring S . The f has an exponent vector

$$f = x^{\alpha}$$

Which is an exponent vector, the exponent vector is denoted by

$$\log(f) = \alpha \in \mathrm{N}^n$$

If R is the set of monomials in the polynomial ring S

Then

$\log(R)$ denotes the set of nonnegative integer exponent vectors of monomial in R .

Theorem 3.6

If S is a polynomial ring over a field F . The polynomial ring S contains n numbers of variables. I and J are two ideals of polynomial ring S ,

these ideals are generated by monomials (nonnegative power product of variables whose leading coefficient is one) in S ,then G is a semi group ring.

Proof: As we already know that I and J are monomial ideals. Then the intersection of all these ideals denoted as

$$I^n \cap J^m \qquad \forall \text{n and m}$$

Where,

n, m are powers of the principal ideals.

So,

Each power of principal ideals such as (n,m) are the component of G . The each component of G is generated by monomials.

Therefore,

G is a subring of $F[x_1,...x_n,u_1,u_2]$ .The subring G is generated over the field F .

Now,

From the list of monomials

$$\{b_i \mid i \in A\}.$$

Now,

Consider the Q is the semi group. The semi group Q is generated by

$$\{\log(b_i) \mid i \in A\}$$

Then,

$$G = F[Q]$$

And G is a semi group over the field F .

This show that a polynomial ring over the field and ideals generated by monomials in S . Then G is semi group ring, which complete the proof of the theorem.

Bibliography

[1] Sara, M., "On the Intersection Algebra of Principle Ideals," Communication in Algebra, pp. 623-635, 2015.

[2] Atiyah M.F,&Macdonald I.G., "Introduction to commutative algebra,," addition wesley publishing compony, 1969.

[3] Bruns,w.&herzog,J., "Cohen MacaulyRing,," Revised edition,cambridge,cambridge university press, 1996.

[4] Dummit,D.S&Foote, R.M., "Abstract algebra," John wiley and sons', 2004.

[5] Herzog,J.& Hibi, T., "Monomial ideals,," Springer, pp. Gradnate textin Maths 260,, (2010).

[6] W.Bruns and J.Herzog,, "Cohen-Macaulay rings," Cambridge studies in Advanced Mathematics, vol. 39, Cambridge University Press, 1993.

[7] villarreal,R.H, "Monomial algebras," Marcel Dekker Inc, 2001.

[8] Ciuperca,C., F.,Spiroff, S., "Asymptotic growth of powers of ideals.," Illinois Journal of Mathematics, pp. 51(1):29-39, 2007.

[9] Fields, J. B. , "Length functions determined by killing powers of several ideals in a local ring. Ph.D. Dissertation, University of Michigan.," Ann Arbror, Michigan, (2000).

[10] Fields, J. B., "Lengths of Tors determined by killing powers of ideals in a local ring.," pp. 104-133, 2002.

[11] Nagata, M ., "Note on a paper of samuel concerning asymptotic properties of ideals.," Mem .college Sci.Univ.Koto Ser. A Math, pp. 30(2):165-175, 1957.

[12] Samuel ,P., "Some asymptotic properties of powers of ideals .," Annals of mathematis (2), pp. 56(1):11-21.

[13] Sara,M, "Noetherian Filtrations and Finite Intersection Algebras.," Master 's thesis ,Georgia State Univeristy., 2008.

[14] Sturmfels, B., Miller,E., "Combinatorial Commutative Algebra.," Berlin: Springer., 2005.

[15] Grenel, G.M. and pfister, G., "A singular introduction to commutative algebra.," Springer., 2007.