Topics in Algebraic Geometry

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Abhinav Sahani

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2016

Supervisor: Dr. Vivek Mohan Mallick

This is to certify that this dissertation entitled Topics in Algebraic Geometry towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents work carried out by Abhinav Sahani at Indian Institute of Science Education and Research Pune under the supervision of Dr. Vivek Mohan Mallick, Assistant Professor, Department of Mathematics, during the academic year 2015-2016.

Vivek Mohan Mallick

Dr. Vivek Mohan Mallick

Committee:
Dr. Vivek Mohan Mallick
Dr. Amit Hogadi

Dedicated to my parents and my younger brother

Declaration

I hereby declare that the matter embodied in the report entitled Topics in Algebraic Geometry are the results of the study carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research Pune, under the supervision of Dr. Vivek Mohan Mallick and the same has not been submitted elsewhere for any other degree.

Abhinav Sahani

Abhinav Sahani

Acknowledgments

I would like to express my gratitude towards Dr. Vivek Mohan Mallick for his guidance and constant support throughout the course of this project. I would also like to thank Department of Mathematics, IISER Pune which gave me a wonderful opportunity to study and learn mathematics.

Abstract

The key objective of this yearlong project was to learn serveral concepts in commutative algebra and algebraic geometry. We started with learning concepts in commutative algebra, which included *primary decomposition, Noetherian and Artinian Rings, regular local rings* and *dimension theory of Noetherian local rings.* After that we studied concepts in algebraic geometry, which included *varieties and morphisms of varieties, sheaves and schemes.* We concluded by stating the *Riemann-Roch theorem* and how that result is used to solve Riemann-Roch problem for the curves.

Contents

Chapter 1

Commutative Algebra

1.1 Primary Decomposition

A prime number in a ring is generalization of a prime number and primary ideal is generalization of power of a prime number.

Definition 1.1.1. Primary Ideal. An ideal $\mathfrak{q}$ is primary if

$$xy \in \mathfrak{q} \implies x \in \mathfrak{q} \,\text{or}\, y^n \in \mathfrak{q} \,\text{for some}\, n \in \mathbb{Z}^+.$$

Theorem 1.1.2. *$\mathfrak{q}$ is primary $\iff$ $A/\mathfrak{q} \neq 0$ and every zero divisor in $A/\mathfrak{q}$ is nilpotent.*

Proof. $\implies$ Let first assume that $\mathfrak{q}$ is primary, and assume that $0 \neq x \in A/\mathfrak{q}$ is zero divisor, i.e. there exists $y \in A/\mathfrak{q}$ such that $xy = 0 = yx$ in $A/\mathfrak{q}$. So we have that $yx \in \mathfrak{q}$, and because $\mathfrak{q}$ is primary, we have $y \in \mathfrak{q}$ or $x^n \in \mathfrak{q}$ and as $y \neq 0$ in $A/\mathfrak{q}$ we have that $x^n = 0$, and so x is nilpotent.
$\impliedby$ Let $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Then $\overline{xy} = 0$ in $A/\mathfrak{q}$, and thus $\overline{y}^n = 0$ in $A/\mathfrak{q}$ for some $n > 0$. And so $y^n \in \mathfrak{q}$ and we are done. □

Note that every prime ideal is primary. It is easy to prove that radical ideal $\sqrt{\mathfrak{q}}$ of primary ideal $\mathfrak{q}$ is prime ideal, as if $xy \in \sqrt{\mathfrak{q}}$, then $(xy)^m \in \mathfrak{q}$ for some $m > 0$. So we have $x^m \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$ for some $n > 0$. And thus we have that $x \in \sqrt{\mathfrak{q}}$ or $y \in \sqrt{\mathfrak{q}}$, and we are done. If $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then $\mathfrak{q}$ is said to be $\mathfrak{p}-$*primary.*
Now we give some examples of primary ideals.
1) Consider A to be the ring of polynomials in two variables x and y with coefficients

in field k. Then the ideal $\mathfrak{q} = (x^2, y^2)$ is primary. Now if $\tilde{A} = A/\mathfrak{q} = k[x,y]/(x^2,y^2)$, if an element t in this ring is zero divisor, it will be of the form $t = \overline{a(x,y).x} + \overline{b(x,y).y}$, and note that $t^3 = 0$. So we have that (x^2, y^2) is a primary ideal. Similarly we can prove that in the same ring ideal (x, y^2) is a primary ideal.
Note that powers of a prime ideals may note be primary ideals but powers of a maximal ideal $\mathfrak{m}$ are indeed $\mathfrak{m}-$*primary.* For the example of a power of a prime ideal not being primary, consider the ring $A = k[x,y,z]/(xy - z^2)$ and let $\overline{x}, \overline{y}, \overline{z}$ denote the images of x, y, z respectively in A. Then $(\overline{x}, \overline{z})$ is a prime ideal in A as $A/(\overline{x}, \overline{z}) \cong k[y]$. Then we have that $\overline{xy} \in (\overline{x}, \overline{z})^2$ as $\overline{xy} = \overline{z}^2$ but $\overline{x} \notin (\overline{x}, \overline{z})^2$ and $\overline{y} \notin \sqrt{(\overline{x}, \overline{z})^2}$. And we are done. For the result concerning the maximal ideals we have the following theorem:

Theorem 1.1.3. *Powers of a maximal ideal* $\mathfrak{m}$ *are* $\mathfrak{m}-$*primary.*

Proof. Let $\mathfrak{a} = \mathfrak{m}^n$. for some $n > 0$. This gives us that $\sqrt{\mathfrak{a}} = \mathfrak{m}$. Then the image of $\mathfrak{m}$ in $A/\mathfrak{a}$ is nilradical of $A/\mathfrak{a}$ and thus $\mathfrak{m}$ is the only prime ideal of $A/\mathfrak{a}$. Thus $A/\mathfrak{a}$ is a local ring and it's every element is either a nilpotent or unit. So every zero divisor in $A/\mathfrak{a}$ is a unit. □

Theorem 1.1.4. *Intersection of finite number of* $\mathfrak{p}-$ *primary ideals is* $\mathfrak{p}-$*primary.*

Proof. Let $\mathfrak{q}_i\,(1 \leq i \leq n)$ be $\mathfrak{p}-$*primary* ideals, and let $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$. We first prove that radical of $\mathfrak{q}$ is $\mathfrak{p}$. $\sqrt{\mathfrak{q}} = \sqrt{\bigcap_{i=1}^n \mathfrak{q}_i} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Now let $xy \in \mathfrak{q}$. Then for some i we have $xy \in \mathfrak{q}_i$ and $y \notin \mathfrak{q}_i$. So we have $x \in \mathfrak{p}$ and thus power of x belongs to $\mathfrak{q}_i$ for all i, and taking suitable power of x, $x^k \in \mathfrak{q}$ for some $k > 0$ and we are done. □

Theorem 1.1.5. *Let* $\mathfrak{q}$ *be a* $\mathfrak{p}-$ *primary ideal and* $x \in A$. *Then*
1) if $x \in \mathfrak{q}$, *then* $(\mathfrak{q} : x) = (1)$.
2) if $x \notin \mathfrak{q}$, *then* $(\mathfrak{q} : x)$ *is* $\mathfrak{p}-$*primary.*
3) if $x \notin \mathfrak{p}$, *then* $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. 1) From the definition $(\mathfrak{q} : x) = \{t \in A : t(x) \subseteq \mathfrak{q}\}$, this part is clear.
2) Let assume we have $yz \in (\mathfrak{q} : x)$ with $y \notin \mathfrak{p}$, then $xzy \in \mathfrak{q} \implies xz \in \mathfrak{q} \implies z \in (\mathfrak{q} : x)$. So we have proved that it is a primary ideal. Now we calculate it's radical. If $t \in (\mathfrak{q} : x) \implies tx \in \mathfrak{q}$. and as $x \notin \mathfrak{q}$, we have $t \in \mathfrak{p}$. So $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$, and thus we have $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$.
3) If $t \in (\mathfrak{q} : x)$, then $tx \in \mathfrak{q} \implies t \in \mathfrak{q}$ as $x \notin \mathfrak{p}$ and we have $(\mathfrak{q} : x) \subseteq \mathfrak{q}$. Now if $t \in \mathfrak{q} \implies tx \in \mathfrak{q} \implies \mathfrak{q} \subseteq (\mathfrak{q} : x)$. □

Definition 1.1.6. Primary Decomposition. Primary decomposition of an ideal $\mathfrak{a}$ of ring A is expression of $\mathfrak{a}$ as a finite intersection of primary ideals, as

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

A primary decomposition is said to be *minimal* if
1)All the $\sqrt{\mathfrak{q}_i}$ are distinct, and
2) $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j (1 \leq i \leq n) \, \forall i$.

Note that we can obtain *minimal* primary decomposition from primary decomposition for an ideal. We do it in two steps: 1) By using 1.1.3 to club together the primary ideals whose radical is the same prime ideal and 2) By getting rid of the redundant terms.
Also note that in general primary decomposition for an ideal need not exist. But in next chapter we will prove that in a *Notherian ring*, every ideal has a primary decomposition. An ideal $\mathfrak{a}$ is said to be decomposable if it has a primary decomposition.
Now some examples.
1) Let $A = k[x, y]$ and $\mathfrak{a} = (x^2, xy)$, then $(x^2, xy) = (x) \bigcap (x, y)^2$. By theorem 1.1.2 we have that $(x, y)^2$ is a primary ideal.
2) In the same ring we have the following primary decomposition

$$(xy, x^3 - x^2, x^2y - xy) = (x) \bigcap (x - 1, y) \bigcap (x^2, y).$$

Theorem 1.1.7. *1st uniqueness theorem. Let $\mathfrak{a}$ be a decomposable ideal in ring A and let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be primary decomposition of $\mathfrak{a}$ with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Then $\mathfrak{p}_i$ are exactly the ideals which occur in the set of ideals $\sqrt{(\mathfrak{a} : x)}$, $(x \in A)$, and hence are independent of the particular decomposition of $\mathfrak{a}$.*

Proof. Let $x \in A$, then $(\mathfrak{a} : x) = (\bigcap \mathfrak{q}_i : x) = \bigcap (\mathfrak{q}_i : x)$. Now $\sqrt{(\mathfrak{a} : x)} = \sqrt{\bigcap (\mathfrak{q}_i : x)} = \bigcap \sqrt{(\mathfrak{q} : x)} = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$ (by previous theorem.). If we assume that $\sqrt{(\mathfrak{a} : x)}$ is prime, then by theorem (1.11) in *Introduction to Commutative Algebra* by *Atiyah and MacDonald*, we have that $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_j$ for some j. So we have proved that every ideal of the form $\sqrt{(\mathfrak{a} : x)}$ is one of the $\mathfrak{p}_j$. Conversely, take $\mathfrak{q}_i$ for some i. Now we choose $x_j \in \mathfrak{a}$ such that $x_j \notin \mathfrak{q}_j$, and thus $x_j \in \bigcap_{j \neq i} \mathfrak{q}_j$,. Then $\sqrt{(\mathfrak{a} : x_i)} = \mathfrak{p}_i$. $\square$

In above proof, we have implicitly shown that for each i there exists $x_i \in \mathfrak{a}$, such that $(\mathfrak{a} : x_i)$ is $\mathfrak{p}_i-$primary.

The prime ideals $\mathfrak{p}_i$ are said to be the ideals associated to $\mathfrak{a}$. The minimal elements of the set $\{\mathfrak{p}\}_{i=1}^n$ are said to be minimal or isolated primes associated to $\mathfrak{a}$ and the other prime ideals are called embedded prime ideals.

Also note that, though the prime associated to a decomposable ideal are uniquely determined as proven in the *1st uniqueness theorem* above, the ideal many not have a unique primary decomposition. For example: $(x^2, xy) = (x)\bigcap(x,y)^2 = (x)\bigcap(x^2, y)$ are two different primary decomposition of the same ideal. However, there are some uniqueness properties which we will explore further in this chapter (*2nd uniqueness theorem*).

Theorem 1.1.8. *Let $\mathfrak{a}$ be a decomposable ideal and $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \supseteq \mathfrak{a}$, then $\mathfrak{p}$ contains a minimal prime ideal belonging to $\mathfrak{a}$. In other words, minimal prime ideals belonging to $\mathfrak{a}$ are minimal ideals of set of prime ideals which contain $\mathfrak{a}$.*

Proof. $\mathfrak{a} \subseteq \mathfrak{p} \implies \bigcap_{i=1}^n \mathfrak{q}_i \subseteq \mathfrak{p} \implies \sqrt{\bigcap \mathfrak{q}_i} \subseteq \sqrt{p} \implies \bigcap \sqrt{\mathfrak{q}_i} \subseteq \mathfrak{p} \implies \bigcap \mathfrak{p}_i \subseteq \mathfrak{p}$. Again by theorem (1.11) in *Introduction to Commutative Algebra* by *Atiyah and MacDonald*, we have that $\mathfrak{p}_i \subseteq \mathfrak{p}$. And hence $\mathfrak{p}$ contains a minimal prime belonging to $\mathfrak{a}$. $\square$

Geometric Interpretation of Primary Ideals. Let A be the ring $k[x_1, x_2, \cdots, x_n]$ and $\mathfrak{a}$ be an ideal in A. Then ideal $\mathfrak{a}$ corresponds to a algebraic set X in $\mathbb{A}^n$. In algebraic geometry, algebraic sets correspond to radical ideals and irreducible algebraic sets correspond to prime ideals. We know that any algebraic set can be decomposed as a union of irreducible algebraic sets, and the decomposition of algebraic sets into union of irreducible ones corresponds to writing radical ideal as intersection of primary ideals. In this correspondence, the minimal primes correspond to irreducible components of X, and the embedded primes correspond to subvarieties of the irreducible components, i.e., varieties embedded in the irreducible components, and hence the name. For example: let $\mathfrak{a} = (x^2, xy)$ in $A = k[x,y]$. Then primary decomposition of $\mathfrak{a}$ is $\mathfrak{a} = (x)\bigcap(x,y)^2$. Here the ideal (x) is prime(primary) and prime ideal associated to $(x,y)^2$ is (x,y). Now here $(x) \subset (x,y)$. So here (x) is minimal prime associated to $\mathfrak{a}$, and (x,y) is embedded prime. Thus here the variety corresponding to $\mathfrak{a}$ is the line $x = 0$, and the embedded prime (x,y) corresponds to the origin $(0,0)$.

Here is another example: let $\mathfrak{a} = (x^3 - xy^3)$ in $A = k[x, y]$. The primary decomposition is $\mathfrak{a} = (x) \bigcap (x^2 - y^3)$. It is easy to see that both these primary ideals are prime ideals, and in fact it is actually an prime decomposition of $\mathfrak{a}$. Both of these ideals are minimal prime ideals associated to $\mathfrak{a}$. Here the algebraic set corresponding to ideal $\mathfrak{a}$ is union of the vertical line $x = 0$ and the curve $x^2 - y^3 = 0$.
Now we probe for the properties of primary decomposition under localization:

Theorem 1.1.9. *Let S be a multiplicatively closed set in A and let $\mathfrak{q}$ be a $\mathfrak{p}-$primary ideal, then*
1) If $S \bigcap \mathfrak{p} \neq \emptyset$, then $S^{-1}A = S^{-1}\mathfrak{q}$.
2) If $S \bigcap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$ primary and it's contraction in A is $\mathfrak{q}$.
Hence there is one to one correspondence between primary ideals in $S^{-1}A$ and primary ideals in A whose radical ideals don't meet S (or primary ideals in $S^{-1}A$ and contracted ideals in A).

Proof. 1) Let's assume $t \in S \bigcap \mathfrak{p}$, then for some $n > 0$, we have $t^n \in S \bigcap \mathfrak{q}$. And thus $t^n/1 \in S^{-1}\mathfrak{q}$. Now $1/t^n \in S^{-1}A$ and thus $S^{-1}A = S^{-1}\mathfrak{q}$.
2) Now assume that $S \bigcap \mathfrak{p} = \emptyset$, then $s \in S$ for, and $as \in \mathfrak{q} \implies a \in \mathfrak{q}$. Now from *3.11* from *Atiyah and MacDonald*, we have that $\mathfrak{q}^{ec} = \bigcup_{s \in S}(\mathfrak{q} : s) = \mathfrak{q}$. Again using the same theorem we will calculate the radical of $S^{-1}\mathfrak{q}$, as follows: $\sqrt{S^{-1}\mathfrak{q}} = S^{-1}\sqrt{\mathfrak{q}} = S^{-1}\mathfrak{p}$. Now we prove that $S^{-1}\mathfrak{q}$ is primary. We know that $S^{-1}A/S^{-1}\mathfrak{q} \cong S^{-1}(A/\mathfrak{q})$. Assume that $a/s \in S^{-1}(A/\mathfrak{q})$ is zero divisor every zero divisor, then $\exists b/t \in S^{-1}(A/\mathfrak{q})$ such that $ab/st = 0$ in $S^{-1}(A/\mathfrak{q})$, i.e. $\exists\, s' \in S$ such that $s'ab = 0$, then $a(s'b) = 0$ in $A/\mathfrak{q}$. As every zero divisor in $A/\mathfrak{q}$ is nilpotent, we have that $a^k = 0$ for some $k > 0$ in $A/\mathfrak{q}$. Now $s^k \in S$, as we have $0 = (a/s)^k \in S^{-1}(A/\mathfrak{q})$, and we are done. □

For the next theorem, $S(\mathfrak{a})$ denotes the contraction of ideal $S^{-1}\mathfrak{a}$ in A for any ideal $\mathfrak{a}$ and any multiplicatively closed set S in A. Now suppose that in the minimal primary decomposition of $\mathfrak{a}$, $\mathfrak{q}_i$ are numbered in such a way that $S \bigcap \mathfrak{p}_i = \emptyset\,(1 \leq i \leq m)$ and $S \bigcap \mathfrak{p}_i \neq \emptyset\,(m + 1 \leq i \leq n)$. Then

Theorem 1.1.10. *Let $\mathfrak{a}$ be a decomposable ideal with minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ (with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}\,\forall i$), and let S be a multiplicatively closed subset of A. Now suppose that in the minimal primary decomposition of $\mathfrak{a}$, $\mathfrak{q}_i$ are numbered in such a way that $S \bigcap \mathfrak{p}_i = \emptyset\,(1 \leq i \leq m)$ and $S \bigcap \mathfrak{p}_i \neq \emptyset\,(m + 1 \leq i \leq n)$. Then*

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

and these decompositions are minimal primary decompositions.

Proof. $S^{-1}\mathfrak{a} = S^{-1}\bigcap_{i=1}^{n}\mathfrak{q}_i = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i$ (using previous theorem.) Now $S^{-1}\mathfrak{q}_i$ is a $S^{-1}\mathfrak{p}_i - primary$ ideal for $1 \leq i \leq m$, and because $S^{-1}\mathfrak{p}_i$ are diffenent ideals, this is the minimal decomposition for $S^{-1}\mathfrak{a}$. Now for the second part

$$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = (\bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m}(S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m}\mathfrak{q}_i$$

and we are done. □

Definition 1.1.11. A set $\sum$ of prime ideals belonging to $\mathfrak{a}$ is said to be *isolated* if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and if $\mathfrak{p}' \subseteq \mathfrak{p}$ for some prime ideal $\mathfrak{p} \in \sum$, then $\mathfrak{p}' \in \sum$.

Theorem 1.1.12. *2nd uniqueness theorem. Let $\mathfrak{a}$ be a decomposable ideal, and let $\mathfrak{a} = \bigcap_{i=1}^{n}\mathfrak{q}_i$ be the minimal primary decomposition of $\mathfrak{a}$. Let $\{\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \cdots, \mathfrak{p}_{i_m}\}$ be an isolated set of primary ideals belonging to $\mathfrak{a}$. Then $\mathfrak{q}_{i_1}\bigcap\mathfrak{q}_{i_2}\bigcap\cdots\bigcap\mathfrak{q}_{i_m}$ is independent of decomposition.*

Proof. Here let $\sum = \{\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \cdots, \mathfrak{p}_{i_m}\}$. Now assume that $S = A - \mathfrak{p}_{i_1}\bigcap\mathfrak{p}_{i_2}\bigcap\cdots\bigcap\mathfrak{p}_{i_m}$. Now for any prime $\mathfrak{p}$ belonging to $\mathfrak{a}$, we have that

$$\mathfrak{p} \in \sum \implies \mathfrak{p}\bigcap S = \emptyset;$$

$$\mathfrak{p} \notin \sum \implies \mathfrak{p} \not\subseteq \bigcup_{\mathfrak{p}' \in \sum}\mathfrak{p}' \implies \mathfrak{p}\bigcap S \neq \emptyset.$$

Now here

$$S(\mathfrak{a}) = \mathfrak{q}_{i_1}\bigcap\mathfrak{q}_{i_2}\bigcap\cdots\bigcap\mathfrak{q}_{i_m},$$

hence it only depends on $\mathfrak{a}$. □

Note that the above theorem implies that *the primary components $\mathfrak{q}_i$ corresponding to minimal prime ideals* $\mathfrak{p}_i$ are uniquely determined by $\mathfrak{a}$, but the embedded primary components are not in general uniquely determined by $\mathfrak{a}$.

Primary Decomposition of Modules. In the first part of this section we studied the primary decomposition of decomposable ideals of a ring. In the same way we can study primary decomposition of modules. Here we will study primary decomposition of modules by proving theorems which are analogous to the first part of this section.

Definition 1.1.13. Radical of a submodule. Let A be a commutative ring and let N be a submodule of $A-$module M. Then radical of N is

$$r_M(N) = \{x \in A : x^t M \subseteq N \text{for some } \ t > 0\}.$$

Theorem 1.1.14. *show that* $r_M(N) = \sqrt{(M : N)} = \sqrt{(Ann(M/N))}$.

Proof. We are given that

$$r_M(N) = \{x \in A : x^t M \subseteq N \text{ for some } t > 0\}.$$

□

if N is a submodule of M, the radical of N in M is defined to be Now $x \in r_M(N) \iff$ for some$q > 0, x^q M \subseteq N \iff$ for some$q > 0, x^q \in (M : N) \iff x \in \sqrt{(M : N)}$.
Now we know that $(N : M) = \operatorname{Ann}((N + M)/N)$, and since $N \subseteq M$, we have that $(N : M) = \operatorname{Ann}(M/N)$. Now taking radicals on both sides, we have that $\sqrt{(M : N)} = \sqrt{(\operatorname{Ann}(M/N))}$.
Now proving formulas analogous to (1.13):
2) $\sqrt{r_M(N)} = r_M(N)$. $x \in \sqrt{r_M(N)} \iff \exists q > 0 \,\text{such that}\, x^q \in r_M(N) \iff \exists\, p, q > 0 \,\text{such that}\, x^{pq} M \subseteq N \iff x \in r_M(N)$.
3) $r_M(N \bigcap P) = r_M(N) \bigcap r_M(P)$. If $x \in r_M(N \bigcap P)$, for some $p > 0, x^p M \subseteq N \bigcap P \implies x^p M \subseteq N \ x^p M \subseteq P \implies r_M(N \bigcap P) \subseteq r_M(N) \bigcap r_M(P)$.
If $x \in r_M(N) \bigcap r_M(P) \implies \exists\, p, q > 0$ such that $x^p M \subseteq N$ and $x^q M \subseteq P$. Taking $t = \max\{p, q\}$, we have that $x \in r_M(N \bigcap P)$ and thus $r_M(N \bigcap P) \supseteq r_M(N) \bigcap r_M(P)$.
4) $r_M(N) = (1) \iff M = N$. If $1 \in \sqrt{(\operatorname{Ann}(M/N))} \iff 1 \in \operatorname{Ann}(M/N) \iff M/N = 0 \iff M = N$.
5) $r_M(N + P) \supseteq \sqrt{(r_M(N) + r_M(P))}$. $P \subseteq (N + P) \implies r_M(P) \subseteq r_M(N + P)$ as $x^p M \subseteq P \implies x^p M \subseteq (N + P)$. Similarly we have that $r_M(N) \subseteq r_M(N + P)$. So we have that $r_M(N) + r_M(P) \subseteq r_M(N + P)$. Now taking radicals $\sqrt{r_M(N) + r_M(P)} \subseteq \sqrt{r_M(N + P)}$. Using **2)**, we have $\sqrt{r_M(N) + r_M(P)} \subseteq r_M(N + P)$.

Solution 21. We are given that a submodule Q of M is primary if $Q \neq M$ and every zero divisor in M/Q is nilpotent. We show that $(Q:M)$ is a primary ideal as follows: suppose $xy \in (Q:M)$ and $y \notin (Q:M) = \mathrm{Ann}(M/Q)$, so thus we have that $xy(M/Q) = 0$, but $y(M/Q) \neq 0$. Thus the endomorphism of M/Q, $\phi_{xy} = 0 = \phi_x \circ \phi_y$. Note also that $\phi_y \neq 0$. These statements imply that ϕ_x has non empty kernel. Thus x is zero-divisor in M/Q. Now as Q is primary in M, thus by definition we have that x is nilpotent in M/Q, which is equivalent to $\underbrace{\phi_x \circ \cdots \circ \phi_x}_{n\,\text{times}} = \phi_{x^n} : M/Q \longrightarrow M/Q$ is zero endomorphism. Equivalently, the endomorphism of M, $\phi_{x^n} : M \longrightarrow M$ has image in Q, so we have that $x^n \in (Q:M)$, and thus $(Q:M)$ is primary.

Theorem 4.3*. Let $Q_i, (1 \leq i \leq n)$ be $\mathfrak{p}-$*primary* in M, then $\bigcap_{i=1}^n Q_i$ is $\mathfrak{p}-$*primary* in M.

Proof. Let $Q = \bigcap_{i=1}^n Q_i$. Now as $Q_i \neq M \ \forall\, i$, we have that $M \neq Q$. Now let $x \in A$ is a zero-divisor of $M/Q \implies \exists y \in M$ such $xy \in Q \implies xy \in Q_i \,\forall i \implies x$ is a zero-divisor of $M/Q_i \implies x^{n_i}M \subseteq Q_i$. Taking $n = \max_i\{n_i\}$, $x^n M \subseteq Q_i \,\forall i$, and hence $x^n M \subseteq Q$. This implies that x is nilpotent in M/Q. Now calculating radical of $Q, r_M(Q) = r_M(\bigcap_{i=1}^n Q_i) = \sqrt{(\bigcap_{i=1}^n Q_i : M)} = \sqrt{\bigcap_{i=1}^n (Q_i:M)} = \bigcap_{i=1}^n \sqrt{(Q_i:M)} = \mathfrak{p}$.

Theorem 4.4*. Let $N \subseteq M$ be a $\mathfrak{p} - $*primary* submodule, where M and N are $A-$modules, and let m be an element of M. Then

1) If $m \in N$, then $(N:m) = (1)$.

2) If $m \notin N$, then $(N:m)$ is $\mathfrak{p} - $*primary*.

3) Let $x \in A$ and $x \notin \mathfrak{q}$, $(N:x) = \{m \in M : mx \in N\} = N$.

Proof. 1) Using $(N:m) = \{a \in A : am \in N\}$, we have that $(N:m) = (1)$.

2) Suppose that $xy \in (N:m)$ and $y \notin (N:m)$, then we have that $xym \in N$ and $ym \notin N$. This implies that x is a zero-divisor in M/N, and $\exists\, n > 0$ such that x^n and $\phi_{x^n} : M/N \longrightarrow M/N$ is zero endomorphism of M/N, thus we have that $x^n M \subseteq N$, and this implies that $x^n m \in N \implies x^n \in (N:m)$. Thus we have that $(N:m)$ is primary.

Now we calculate the radical of primary ideal $(N:m)$. Note that $m \in M$ implies that $(N:M) \subseteq (N:m)$. Now taking radicals implies that $\mathfrak{p} \subseteq \sqrt{(N:m)}$. Now if $x \in \sqrt{(N:m)} \implies \exists\, n > 0, x^n \in (N:m) \implies x^n m \in N \implies 0 = x^n \bar{m} \in M/N \implies x$ is a zero-divisor of M/N. So there exists $p > 0$ such that ϕ_{x^p} is zero endormorphism of M/N, i.e. $x^p M \subseteq N$. And so $x \in r_M(N) = \mathfrak{p} \implies \mathfrak{p} \supseteq \sqrt{(N:m)}$. So we have that $(N:m)$ is $\mathfrak{p} - $*primary*.

3) If $m \in N$, then $xm \in N \implies N \subseteq (N:x)$. Now we assume that $m \in (N:x)/N$,

then we have that $xm \in N$ and $\bar{m} \neq 0$ in M/N. This means that x is zero-divisor in M/N, and for some $n > 0$, we have that $x^n M \subseteq N$, but then $x \in r_M(N) = \mathfrak{p}$, which is a contradiction.

Solution 22. In this question we prove analogs of *theorem 4.5.*

Theorem 4.5*. Let N be a decomposable submodule of M, with minimal primary decomposition, $N = \bigcap_{i=1}^{n} Q_i$ and $\mathfrak{p}_i = r_M(Q_i), (1 \leq i \leq n)$, then $\mathfrak{p}_i$ are exactly the ideal which occur in the set of ideals $r(N : m), m \in M$, and hence are independent of particular decomposition of N.

Proof. We have that that $Q_i \not\supseteq \bigcap_{j\neq i} Q_j$, which implies $\exists m \in \bigcap_{j\neq i} Q_j/Q_i$. Consider $(N : m) = (\bigcap_i Q_i : m) = (Q_i : m) \bigcap (\cap_{i\neq j} Q_j : m)$. Now using *theorem 4.4**, we have that $(N : m)$ is $\mathfrak{p}_i - primary$. Thus each $\mathfrak{p}_i$ is $\sqrt{(N : m)}$ for some $m \in M$.

Now assume that $\sqrt{(N : m)}$ is a prime $\mathfrak{p}$ for some $m \in M$. Then $\sqrt{(N : m)} = \sqrt{(\bigcap_{i=1}^{n} Q_i : m)} = \bigcap_i \sqrt{(Q_i : m)} \implies \mathfrak{p} = \bigcap_i \mathfrak{p}_i \implies \mathfrak{p} = \mathfrak{p}_i$ for some i.

1.2 Chain Conditions on Rings

Let $\sum$ be a partially ordered set with partial order $\leq$. Then we can prove the following theorem on $\sum$.

Theorem 1.2.1. *The following two conditions on $\sum$ are equivalent:*
1) Any increasing chain $x_1 \leq x_2 \leq \cdots$ of elements of $\sum$ stabilizes.
2) Any non-empty subset of $\sum$ has a maximal element.

Proof. 1) $\implies$ 2). Let say 2) is not true. Then there exists a set which contains no maximal element, and we can create a strictly increasing chain of elements of $\sum$ which doesn't stabilize.

2) $\implies$ 1). Here consider the non-empty set $\{x_n\}_{n\geq 1}$. By condition 2, it will have a maximal element, and thus this chain will stabilize. $\square$

If the set of submodules of a module M is ordered by $\subseteq$ relation, then 1) in *theorem 1.2.1* is called the *ascending chain condition*, and if they are ordered by $\supseteq$ relation, then 1) in *theorem 1.2.1* is called *descending chain condition.*

Definition 1.2.2. Noetherian and Artinian Modules. If a module M satisfies the ascending chain condition, then it is called *Noetherian module,* and if it satisfies the descending chain condition, it is called *Artinian module.*

Here are some examples of Noetherian and Artinian modules:

Example1. Consider $\mathbb{Z}$ as a $\mathbb{Z}-$module, then it satisfies the ascending chain condition but not descending chain condition. This can be seen as follows: If $a \in \mathbb{Z}$ and $a \neq 0$, then we have a sequence which doesn't satisfy the d.c.c.: $(a) \supset (a^2) \supset (a^3) \supset \cdots \supset \cdots$. Now it is easy to see that any ascending chain of modules will stabilize: If we have a submodule $(a) \subset \mathbb{Z}$, and $a \neq 0$, then $(a) \subseteq (b) \iff b|a$, now we can't have infinitely many b dividing a.

Example2. $k[x]$, where k is a field, satisfies ascending chain condition on ideals. This follows from the fact that $k[x]$ is a principal ideal domain, and if $(f(x)) \subset (g(x))$(a proper inclusion), then $\deg g(x) < \deg f(x)$, which implies that any strictly increasing chain of ideals in $k[x]$ must be finite. But $k[x]$ doesn't satisfy d.c.c on ideals: $(x) \supset (x^2) \supset (x^3) \supset \ldots \supset (x^n) \supset \ldots$ is a descending chain of ideals which doesn't stabilize.

Theorem 1.2.3. *M is a Noetherian $A-$module. $\iff$ Every submodule of M is finitely generated.*

Proof. $\implies$ Let N be a submodule of M, then consider the set $\sum$ of all finitely generated submodules of N. Then this set will be nonempty as 0 is finitely generated. Then by theorem 1.2.1, there exists a maximal element in $\sum$, let say $\tilde{N}$. If N is not finitely generated, then $N \neq \tilde{N}$. Then take $\bar{x} \in N/\tilde{N}$, so we have another finitely generated submodule $\tilde{N} + Ax$ of N such that $\tilde{N} \subset \tilde{N} + Ax \subset N$, which is a contradiction.

$\impliedby$ Let's assume we have a ascending chain of submodules of M: $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$, then $\bigcup_{i=1}^{\infty} M_i$ will be a submodule of M, and thus will be finitely generated, let's say $\bigcup_{i=1}^{\infty} M_i = \langle x_1, x_2, \ldots, x_r \rangle$. Now let $x_i \in M_i$, and take $n = \max n_{i 1 \leq i \leq r}$. Then $M_n = \bigcup_{i=1}^{\infty} M_i$, and thus the above chain is stationary. $\square$

Theorem 1.2.4. *Let M, M' and $''$ be $A-$modules with* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *is an exact sequence. Then we have the following:*

1) M is Noetherian $\iff$ M' and M'' are Noetherian modules.

2) M is Artinian $\iff$ M' and M'' are Artinian modules.

Proof. 1) $\implies$ Let $M'_1 \subseteq M'_2 \subseteq M'_3 \subseteq \ldots$ be an ascending chain of submodules of M'. Then $(\alpha(M'_i))_{i=1}^{\infty}$ is a chain in M, which will stabilize. Now $\alpha(M'_n) = \alpha(M'_{n+1})$ $\implies$ $M'_n = M'_{n+1}$ as follows: We already know that $M'_n \subseteq M'_{n+1}$. Now if $x \in M'_{n+1}$, then $x \in \alpha(M'_n)$, and because α is injective, we have that $x \in M'_n$. And thus M'

is Noetherian. Now let $M_1'' \subseteq M_2'' \subseteq M_3'' \subseteq \ldots$ be an ascending chain of submodules of M'', then $(\beta^{-1}(M_i''))_{i=1}^{\infty}$ will be a chain in M, and thus it will stabilize. Now $\beta^{-1}(M_n'') = \beta^{-1}(M_{n+1}'') \implies M_n'' = M_{n+1}''$ as follows: we already know that $M_n'' \subseteq M_{n+1''}$. If $x \in M_{n+1''}$, then $\beta^{-1}(x) \in \beta^{-1}(M_n'') \implies x \in M_n''$. Thus the original chain also stabilizes in M''.

$\Longleftarrow$ For an ascending chain of submodules $(M_i)_{i=1}^{\infty}$ in M, we have two corresponding ascending chains: $(\alpha(M') \bigcap M_i)_{i=1}^{\infty}$ in M' and $(\beta(M_i))_{i=1}^{\infty}$ in M''. Here we are identifying $\alpha(M') \bigcap M_i$ as submodules of M'. Note that as both M' and M'' are Noetherian, both of these chains will stabilize. So proving that M is Noetherian boils down to the following: For submodules $M_1 \subseteq M_2 \subset M$,

$$\alpha(M') \bigcap M_1 = \alpha(M') \bigcap M_2 \,\text{and}\, \beta(M_1) = \beta(M_2) \implies M_1 = M_2.$$

Let $x \in M_2$, then $\beta(x) \in \beta(M_1)$. Thus there exists $y \in M_1$, such that $\beta(y) = \beta(x)$, thus $\beta(x-y) = 0$ Thus $(x-y) \in \ker \beta = \operatorname{im} \alpha = \alpha(M')$. Now $(x-y) \in M_2 \implies (x-y) \in \alpha(M') \bigcap M_1 = \alpha(M') \bigcap M_2 \implies (x-y) \in M_1 \implies x \in M_1 \implies M_1 = M_2$, and thus we are done

2) Similar to the first part. □

Definition 1.2.5. Noetherian and Artinian Rings. A ring A is said to be *Noetherian ring* if it is an Noetherian as an $A-$module. Similarly we can define *Artinian rings.*

Theorem 1.2.6. *Finitely generated modules of a Noetherian(resp. Artinian) ring are Noetherian(resp. Artinian) modules.*

Proof. Let M be a finitely generated module of Noetherian ring A. Then we will have a surjective morphism $\underbrace{A \oplus A \oplus \ldots \oplus A}_{n\,\text{times}} \longrightarrow M$ for some $n > 0$. So $M \cong A^n/I$, where I is the kernel of previous homomorphism. Thus we have an exact sequence $I \rightarrowtail A^n \twoheadrightarrow M$, and using the previous theorem, we have our result.
Statement for Artinian rings can be proven similarly. □

Theorem 1.2.7. *Quotients of Noetherian(resp. Artinian) are Noetherian(resp. Artinian) rings.*

Proof. Let $\mathfrak{a}$ be an ideal of A, then we have an exact sequence $\mathfrak{a} \rightarrowtail A \twoheadrightarrow A/\mathfrak{a}$. So again theorem 1.2.4, we have that $A/\mathfrak{a}$ is A module. Now using the fact that $A/\mathfrak{a}$ is an $A-$module, we can give it a canonical $A/\mathfrak{a}-$module structure. □

Definition 1.2.8. Chain and Length of a Chain. A *chain of submodules* of a module M is a sequence $(M_i)\,(0 \le i \le n)$ of submodules such that we have:

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

The *length* of such a chain is n.

Definition 1.2.9. Composition Series. A chain of submodules of a module M is called *composition series* if no extra module can be inserted within the chain. This is equivalent to the following condition: For all $0 \le i \le n$, M_{i-1}/M_i is a simple module.

Theorem 1.2.10. *Let M be a module, then every composition chain of M has equal length and any chain of submodules of M can be extended to a composition series.*

Proof. Let $l(M)$ denote the length of a composition series of a module M. Thus if M doesn't has a composition series, then $l(M) = +\infty$.
We first prove that $N \subset M \implies l(N) \implies l(M)$. Let (M_i) be a composition series of M of finite length. Then $N_i = N \bigcap M_i$ are submodules of N. Now we have a homomorphism $\begin{tikzcd} N_{i-1} \arrow[r] \arrow[rr, bend right] & M_{i-1} \arrow[r] & M_{i-1}/M_i \end{tikzcd}$ and N_i lies in the kernel of this homomorphism. Thus N_{i-1}/N_i is isomorphic to a subring of M_{i-1}/M_i, and hence $N_{i-1}/N_i \subseteq M_{i-1}/M_i$. And because latter is a simple module, we have that $N_{i-1} = N_i$ or $N_{i-1}/N_i = M_{i-1}/M_i$. This means that in (N_i) there may be some repeating terms, and after removing the repeating terms, we will have a composition series of N, and so $l(N) \le l(M)$. Now we prove that if $l(N) = l(M)$, then $N = M$. If $l(M) = l(N)$, then $N_{i-1}/N_i = M_{i-1}/M_i$ for each i, and so $M_{n-1} = N_{n-1}$, and thus $M_{n-2} = N_{n-2}, \ldots,$ and thus we have that $M = N$.
Now we prove that any chain in M has length $\le l(M)$. Let $M = M_0 \supset M_1 \supset M_2 \supset \ldots$ be a chain of length k, then as proven, we will have $l(M) > l(M_1) > l(M_2) > \ldots > l(M_k) = 0$, and hence $l(M) \ge l$.
Consider any composition series of M. If it's length is k, then as proven above, we will have $k \le l(M)$, and by the definition of $l(M)$, we have $k = l(M)$. Thus every composition series in M has the same length. Now if a chain in M doesn't have length $l(M)$, it is not a maximal chain, and thus we can insert submodules in the chain to make it a maximal chain, and thus extend it to a composition series. $\square$

Theorem 1.2.11. *Let M be a module. Then M has a composition series $\iff$ M satisfies both chain conditions.*

Proof. $\Longrightarrow$ If M has a composition series, then all chains of submodules of M are of bounded lengths, and hence they satisfy both a.c.c. and d.c.c.
$\Longleftarrow$ We will prove this part by constructing a composition series of M. Let $M = M_0$. Now as M is Noetherian, it has a maximal submodule, let it be M_1. Similarly M_1 has a maximal submodule, call it M_2. Thus we have a chain $M = M_0 \supset M_1 \supset M_2 \supset \dots$. As M also satisfies d.c.c., this chain must be finite, and hence M has a composition series. $\square$

We define the *length of a module* M to be length of (any) composition series in M and denote it by $l(M)$.

Theorem 1.2.12. *The length of a module $l(M)$ is an additive function on the class of all $A-$modules with $l(M)$ finite.*

Proof. Let M, M' and M'' be $A-$modules of finite length such that we have the following exact sequence: $M' \overset{\alpha}{\hookrightarrow} M \xrightarrow{\beta} M''$. Now to prove this theorem we have to show that $l(M) = l(M') + l(M'')$. Let $l(M') = n$ and $l(M'') = m$, then let $M' \supset M_1' \supset M_2' \supset \dots \supset M_n' = 0$ be a composition series in M' and let $M'' \supset M_1'' \supset M_2'' \supset \dots \supset M_m'' = 0$ be a composition series in M''. Then $M = \beta^{-1}M'' \supset \beta^{-1}M_1'' \supset \beta^{-1}M_2'' \supset \dots \beta^{-1}0 = \alpha M' \supset \alpha M_1' \supset \alpha M_2' \supset \dots \supset \alpha M_n' = 0$ is a composition series in M, and thus $l(M) = l(M') + l(M'')$. $\square$

Primary Decomposition in Noetherian Rings. We studied primary decomposition in the first section of this chapter. Here we will prove that every ideal in a Noetherian ring has a primary decomposition. Note that ideals in a ring may not be primary decomposable.

Definition 1.2.13. Irreducible ideal. An ideal $\mathfrak{a}$ is a ring A is called irreducible if whenever

$$\mathfrak{a} = \mathfrak{b} \bigcap \mathfrak{c} \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}.$$

Here $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A.

In the next two theorems we will prove that every ideal in a Noetherian ring is primary decomposable.

Theorem 1.2.14. *In a Noetherian ring every ideal is finite intersection of irreducible ideals.*

Proof. Let's assume that the above statement is not true, then there exists a set $\sum$ of ideals of Noetherian ring A for which the statement of theorem is not true. As the ring is Noetherian, the set $\sum$ has a maximal ideal, let's say $\mathfrak{a}$. As $\mathfrak{a}$ is reducible, we have that $\mathfrak{a} = \mathfrak{b} \bigcap \mathfrak{c}$, such that $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{a} \subset \mathfrak{c}$. Then $\mathfrak{b}$ and $\mathfrak{c}$ can be represented as finite intersection of irreducible ideals, and therefore $\mathfrak{a}$ can also be represented as finite intersection of irreducible ideals, which is a contradiction. □

Theorem 1.2.15. *In a Noetherian ring every irreducible ideal is primary.*

Proof. Let $\mathfrak{a}$ be a irreducible ideal Noetherian ring A, then to prove the above statement, it is enough to show that if zero ideal in $A/\mathfrak{a}$ is irreducible, then it is primary. Now assume that $xy = 0$ with $y \neq 0$ in $A/\mathfrak{a}$. Now consider the following ascending chain of ideals $\mathrm{Ann}\,(x) \subseteq \mathrm{Ann}\,(x^2) \subseteq \mathrm{Ann}\,(x^3) \subseteq \ldots$. By a.c.c., this chain will be stationary, therefore for some $n > 0$, $\mathrm{Ann}\,(x^n) = \mathrm{Ann}\,(x^{n+1}) = \ldots$. Now we have that $(x^n) \bigcap (y) = 0$. To prove this statement let's assume that $a \in (x^n) \bigcap (y)$, then $a = ty$ for some $t \in A/\mathfrak{a}$, and thus $ax = txy = 0$. Now as $a \in (x^n) \implies a = bx^n \implies ax = bx^n + 1 = 0 \implies b \in \mathrm{Ann}\,(x^n) = \mathrm{Ann}\,(x^{n+1})$. And thus we have that $a = bx^n = 0$. So we have proven that $(x^n) \bigcap (y) = 0$. Now we have the following representation for zero ideal $(0) = (x^n) \bigcap (y)$. Now as (0) is irreducible in $A/\mathfrak{a}$, we have that $x^n = 0$ as $y \neq 0$. Thus zero ideal in $A/\mathfrak{a}$ is irreducible $\implies$ it is primary. □

From the above two theorems, it is clear that every ideal in a Noetherian ring is primary decomposable. So all the results of the first section of this chapter are applicable to Noetherian rings. Now we prove some other theorems concerning Noetherian rings.

Theorem 1.2.16. *In a Noetherian ring A, every ideal contains a power of its radical.*

Proof. Assume that $\mathfrak{a}$ is an ideal in Noetherian ring A, and let $\sqrt{\mathfrak{a}}$ be the radical ideal of $\mathfrak{a}$. Then let $\sqrt{\mathfrak{a}} = \langle x_1, x_2, \ldots, x_r \rangle$. Now let $x_i^{n_i} \in \mathfrak{a}$ for each i. Now let $m = \sum_{i=1}^{r}(n_i - 1) + 1$, then we have that $(\sqrt{\mathfrak{a}})^m$ will be generated by monomials of the form $x_1^{k_1} x_2^{k_2} \ldots x_r^{k_r}$ with $\sum k_i = m$. Then the way we have defined m implies that $k_i < n_i$ for at least one index i, hence all of the monomials which generate $(\sqrt{\mathfrak{a}})^m$, lie in $\mathfrak{a}$, and therefore $(\sqrt{\mathfrak{a}})^m \subseteq \mathfrak{a}$. □

If in the above theorem 1.2.16 we take $\mathfrak{a}$ to be the zero ideal, then some power of nilradical will be zero. So in a Noetherian ring, nilradical is nilpotent.

Theorem 1.2.17. *Let A be a Noetherian ring, and let $\mathfrak{m}$ be a maximal ideal of A, and let $\mathfrak{q}$ be any ideal in A, then the following statements are equivalent:*
1) $\mathfrak{q}$ is $\mathfrak{m}-$primary.
2)$\sqrt{\mathfrak{q}} = \mathfrak{m}$
3) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n > 0$.

Proof. 1) $\Longrightarrow$ 2). Follows from the definition of a primary ideal.
2) $\Longrightarrow$ 1). Follows from theorem 1.2.16 and theorem 1.1.3.
2) $\Longrightarrow$ 3). Follows from theorem 1.2.16.
3) $\Longrightarrow$ 2). $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m} \Longrightarrow \sqrt{\mathfrak{m}^n} \subseteq \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{m}} \Longrightarrow \mathfrak{m} \subseteq \sqrt{\mathfrak{q}} \subseteq \mathfrak{m}$.

□

1.3 Dimension Theory

Definition 1.3.1. Graded Rings and Modules. A *graded ring* is a ring A together with a family of subgroups $(A_n)_{n\geq 0}$ of additive group of A such that
1) $A = \bigoplus_{n=0}^{\infty} A_n$
2) $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$.
If A is a graded ring, then a *graded $A-$module* is an $A-$module M together with a family of subgroups $(M_n)_{n\geq 0}$ such that
1) $M = \bigoplus_{n=0}^{\infty} M_n$
2) $A_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$.

Note that it follows from the above definition that A_0 is a subring of A, and A_n and M_n are A_0 modules for each n. An example of graded ring is $A = k[x_1, x_2, \cdots, x_r]$ with A_n being set of all homogeneous polynomials of degree n. An element y of M is called *homogeneous* if $y \in M_n$ for some $n > 0$. Any element $y \in M$ can be written as $\sum_n y_n$ where $y_n \in M_n$ and all but finitely many y_n are zero. Also note that $A_+ = \bigoplus_{n>0} A_n$ is an ideal of A.
A homomorphism of graded $A-$modules M and N is an $A-$module homomorphism $f : M \longrightarrow N$ such that $f(M_n) \subseteq N_n$ for all $n \geq 0$.

Theorem 1.3.2. *In a graded ring A the following two statements are equivalent:*
1) A is a Noetherian ring.
2) A_0 is Noetherian and A is finitely generated as an A_0-algebra.

Proof. 1) $\implies$ 2). As $A_0 \cong A/A_+$, and A is a Noetherian ring implies that A_0 is Noetherian ring. As A_+ is an ideal in A, it is finitely generated, $A_+ = \langle x_1, x_2, \ldots, x_s \rangle$, which we can take to be homogeneous elements of A, with degree of x_i to be k_i. Now let A' be the subring of A generated by $x_1, x_2, \ldots, x_s$ over A_0. Now we will use induction to show that $A_n \subseteq A'$ for all $n \geq 0$. For $n = 0$, it is obvious. Now we assume it is true for $\leq (n-1)$ and prove it for $n > 0$. Let $y \in A_n$, then $y \in A_+$, and thus y is a linear combination of x_i, let say $y = \sum_{i=1}^{s} a_i x_i$, where $a_i \in A_{n-k_i}$. Now using the inductive hypothesis shows that $a_i's$ are polynomials in $x_i's$, with coefficient in A_0, and thus y also is a polynomial in $x_i's$ with coefficients in A_0, and therefore $y \in A'$, and thus $A_n \subseteq A'$ for all $n \geq 0$, and thus $A = A'$, and thus the latter part of the theorem is true.
2) $\implies$ 1). In this case, we will have that $A \cong A_0[x_1, x_2, \ldots, x_n]/I$, for some $n > 0$. Now as A_0 is a Noetherian ring, by Hilbert's basis theorem, we have that A is a Noetherian ring. □

Hilbert Functions Let A be a Noetherian graded ring with $A = \bigoplus_{n=0}^{\infty} A_n$. By theorem 1.3.2 we can take A to be a finitely generated A_0-algebra, generated by elements $x_1, x_2, \cdots, x_s$, i.e. $A = A_0[x_1, x_2, \cdots, x_s]$ and we can take all the $x_i, (1 \leq i \leq s)$ to be homogeneous. Let say degree of x_i is k_i for $1 \leq i \leq s$.
Let M be a finitely generated graded $A-$module. Then M is generated by finite number of homogeneous elements, say $m_j (1 \leq j \leq t)$, and let $\deg m_j = r_j$. Thus is $y \in M_n$, then $y = \sum_j f_j(x) m_j$, where $f_j(x)$ is a homogeneous element of A of degree $n - r_j$. Now as we have proven previously in theorem 1.3.2 that A is an finitely generated A_0 algebra, we can replace $f_j(x)$ by monomials in $x_i's$ with coefficients in A_0. Thus M_n is finitely generated as an A_0-module and is genereated by $g_j(x) m_j$, where $g_j(x)$ is a monomial in x_i of total degree $n - r_i$.

Definition 1.3.3. Poincare Series. Let λ be an additive function on the class of all finitely generated A_0-modules, which takes values in $\mathbb{Z}$. The Poincare series of M(with respect to λ) is the following power series:

$$P(M,t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n \qquad \in \mathbb{Z}[[t]].$$

Theorem 1.3.4. *The Poincare series $P(M,t)$ of the above describe finitely generated* *gradedA−module M, is a rational function in t of the form*

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})} \quad , \textit{where}\, f(t) \in \mathbb{Z}[t].$$

Proof. we prove this theorem by inducting on the number of generators s of A over A_0. If $s = 0$, then $A = A_0$, and $A_n = 0$ for all $n > 0$. Thus we have that M is a finitely generated A_0-module. Then there will exists $n > 0$ such that for all $m \geq n$, $M_m = 0$, and thus in this case $P(M,t)$ will be a polynomial in t.
Now suppose that $s > 0$ and the theorem is true for $s-1$. Now we have an $A-$module homomorphism given by $M_n \xrightarrow{x_s} M_{n+k_s}$, which is multiplication by x_s, which gives rise to the following exact sequence:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0 \tag{1.1}$$

Let $K = \bigoplus_n K_n$, and let $L = \bigoplus_n L_n$. Then both these modules are finitely generated $A-$moduels, as K is a submodule of M and L is a quotient module of M. These are also $A_0[x_1, x_2, \ldots, x_{s-1}]$ module as x_s annihilates both of these modules. Now applying λ to the above exact sequence (1.1), we have the following

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0. \tag{1.2}$$

Now multiplying by t^{n+k_s} and summing up with respect to n

$$\sum_n t^{n+k_s}\lambda(K_n) - \sum_n t^{n+k_s}\lambda(M_n) + \sum_n t^{n+k_s}\lambda(M_{n+k_s}) - \sum_n t^{n+k_s}\lambda(L_{n+k_s}) = 0$$

$$t^{k_s}P(K,t) - t^{k_s}P(M,t) + [P(M,t) + g_1(t)] - [P(L,t) + g_2(t)] = 0$$

here $g_1(t)$ and $g_2(t)$ both are polynomials in t

$$(1 - t^{k_s})P(M,t) = P(L,t) - t^{k_s}P(K,t) + g(t) \tag{1.3}$$

here $g(t) = g_2(t) - g_1(t)$. Now applying the inductive hypothesis, we will have

$$P(L,t) = \frac{f_1(t)}{\prod_{i=1}^{s-1}(1-t^{k^i})}, \qquad P(K,t) = \frac{f_2(t)}{\prod_{i=1}^{s-1}(1-t^{k^i})}$$

, where $f_1(t), f_2(t) \in \mathbb{Z}[t]$.

Now putting the expressions for $P(L,t)$ and $P(K,t)$ in 1.3, we get $P(M,t)$ in the desired form. $\square$

The order of the pole of $P(M,t)$ at $t=1$ is denoted by $d(M)$. In the next theorem we will denote $d(M)$ by d

Theorem 1.3.5. *If each $k_i = 1$, then for $n \gg 0$, $\lambda(M_n)$ is a polynomial in n, with rational coefficients of degree $d-1$.*

Proof. Using theorem 1.3.4, we have that

$$\lambda(M_n) = \text{coefficient of}\, t^n \,\text{in}\, \frac{f(t)}{(1-t)^s}.$$

Now we cancel powers of $(1-t)$ from the above expression we may assume that $s=d$ and $f(t)$ is not divisible by $(1-t)$, which is equivalent to $f(1) \neq 0$. Now assume that polynomial $f(t) = \sum_{k=0}^{N} a_k t^k$, and using the following binomial expansion

$$\frac{1}{(1-t)^d} = (1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

Thus for $n \gg N$, we have that

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{d+n-k-1}{d-1}.$$

And thus we have an expression for $\lambda(M_n)$ as a polynomial in variable n.

$\square$

Remark. The polynomial obtained in theorem 1.3.5 is called the **Hilbert function** or **Hilbert polynomial** of M with respect to λ.

Theorem 1.3.6. *If $x \in A_k$ is not a zero-divisor in M, then $d(M/xM) = d(M) - 1$.*

Proof. If $x \in A_k$ is not a zero-divisor in M, then in equation 1.1 $K_n = 0$. Thus $K = 0$, and from equation 1.3 it follows that $d(M/xM) = d(M) - 1$. $\square$

Now we will study the Hilbert functions obtained from a local ring by passing to the associative graded rings.

Theorem 1.3.7. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ be a $\mathfrak{m}-$primary ideal, M be a finitely generated $A-$module, (M_n) be a stable $\mathfrak{q}-$filtration of M. Then we have the following statements:*
1) For each $n \geq 0$, the length of M/M_n is finite.
2) For $n \gg 0$, this length is a polynomial $g(n)$ in n, whose degree is $\leq s$, where s denotes the least number of generators of $\mathfrak{q}$.
3) For the polynomial $g(n)$, degree and leading coefficients are independent of chosen filtration, but depends on M and $\mathfrak{q}$.

Proof. 1) Consider associated graded ring $G(A) = \bigoplus_n \mathfrak{q}^n/\mathfrak{q}^{n+1}$. Now from the filtration (M_n), we get a $G(A)-$module, $G(M) = \bigoplus_n M_n/M_{n+1}$. Now we state some properties of these algebraic structures: by *theorem 8.5*, *Introduction to Commutative Algebra* by Atiyah and MacDonald, which states that a ring A is Artinian $\iff$ it is Noetherian and dim $A = 0$. Using this statement we have that $G_0(A) = A/\mathfrak{q}$ is an Artinian ring, as A is Noetherian local ring. Now *theorem 10.22* of the same book states that: 1) $G(A)$ is Noetherian, and 2) $G(M)$ is a finitely generated graded $G(A)-$module. Now as each of the Noetherian $A-$modules $G_n(M) = M_n/M_{n+1}$ are annihilated by ideal $\mathfrak{q}$, we can give these $A/\mathfrak{q}-$module structures. Hence these are Noetherian $A/\mathfrak{q}-$modules. Now using theorem 1.2.10, we have that M_n/M_{n+1} satisfies both d.c.c. and a.c.c. Now from theorem 1.2.11, we have that these are of finite length. Now from the exact sequences:

$$M_r \rightarrowtail M_{r-1} \twoheadrightarrow M_{r-1}/M_r$$

we can deduce that (because l is an additive function, as we have already proven in theorem 1.2.12.)

$$l_n = l\left(\frac{M}{M_n}\right) = \sum_{r=1}^{n} l\left(\frac{M_{r-1}}{M_r}\right) \tag{1.4}$$

Thus using the fact that for each r, $l\left(\frac{M_{r-1}}{M_r}\right)$ is finite, we will have that $l\left(\frac{M}{M_n}\right)$ is finite from above equation.

2) Assume that $\mathfrak{q} = \langle x_1, x_2, \ldots, x_s \rangle$, and assume that $\bar{x}_i$ is the image of x_i in $\mathfrak{q}/\mathfrak{q}^2$.

Now from theorem 1.3.2 we will have that $G(A)$ is generated as an $A/\mathfrak{q}-$algebra by $\bar{x_i}'s$. As each of the $\bar{x_i}$ has degree 1, (this follows directly from the fact that each $\bar{x_i} \in G_1(A) = \mathfrak{q}/\mathfrak{q}^2$.) we have from theorem 1.3.5 that $l(M_n/M_{n+1})$ is a polynomial, let's say $f(n)$, of degree $\leq s-1$ for all $n \gg 0$. Now we have the following exact sequence

$$\frac{M_n}{M_{n+1}} \rightarrowtail \frac{M}{M_{n+1}} \twoheadrightarrow \frac{M}{M_n}$$

, which implies that $l_{n+1} - l_n = f(n)$, and thus it follows that l_n is a polynomial $g(n)$ of degree $\leq s$, for $n \gg 0$.

3) Let's we have another stable $\mathfrak{q}-$filtration of M, $(\tilde{M_n})$, and define $\tilde{g}(n) = l(M/\tilde{M_n})$. Now *theorem 10.6* in *Introduction to Commutative Algebra* by Atiyah and MacDoanald states that any two stable $\mathfrak{q}-$filtrations have bounded difference, i.e., there exists an integer n_0 such that for all $n \geq 0$, we have that $M_{n+n_0} \subseteq \tilde{M_n}$ and $\tilde{M}_{n+n_0} \subseteq M_n$. Thus it follows easily that $g(n+n_0) \geq \tilde{g}(n)$, and $\tilde{g}(n+n_0) \geq g(n)$. Thus for all large n we have that $\lim_{n\to\infty} g(n)/\tilde{g}(n) = 1$. And because $g(n)$ and $\tilde{g}(n)$ both are polynomials in n, we have that g and $\tilde{g}$ have the same degree and leading coefficient. □

The polynomial $g(n)$ for the filtration $(\mathfrak{q}^n M)$ is denoted by $\chi_{\mathfrak{q}}^M(n)$, and if $M = A$, then we write $\chi_{\mathfrak{q}}$ in place of $\chi_{\mathfrak{q}}^A$ and term it as the *characteristic polynomial* of the $\mathfrak{m}-$primary ideal $\mathfrak{q}$.

Theorem 1.3.8. *The degree of $\chi_{\mathfrak{q}}(n)$ is equal for different $\mathfrak{m}-$primary ideals of A.*

Proof. Let $\mathfrak{q}$ be a $\mathfrak{m}-$primary ideal. Then to prove the above statement, we prove that $\deg \chi_{\mathfrak{m}}(n) = \deg \chi_{\mathfrak{q}}(n)$. As A is Noetherian, we have that $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, and therefore we have that $\mathfrak{m}^{nr} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$, and this implies that $\chi_{\mathfrak{m}}(n) \leq \chi_{\mathfrak{q}}(n) \leq \chi_{\mathfrak{m}}(rn)$, and letting $n \longrightarrow \infty$, we have our result. □

Now the common degree of $\chi_{\mathfrak{q}}(n)$ will be denoted by $d(A)$. Also $\delta(A)$ denotes the least number of generators of a $\mathfrak{m}-$primary ideal. Also $\dim A$ denotes the supremum of the lengths of the all chains of prime ideals in A.

Dimension Theorem for Noetherian Local Rings. In this section we will prove that for a Noetherian local ring A, the numerical values of $d(A)$, $\delta(A)$ and dim (A) are equal. We will prove this by showing that $\delta(A) \leq \dim A \leq d(A) \leq \delta(A)$.

Theorem 1.3.9. $d(A) \leq \delta(A)$.

Proof. It follows from the part 2) of theorem 1.3.7 and theorem 1.3.8. Note that in theorem 1.3.7, we are taking $M = A$ and stable filtration $(M_n) = (\mathfrak{q}^n A)$ for proving this theorem. $\square$

Theorem 1.3.10. *Let $A, \mathfrak{q}$ and $\mathfrak{m}$ be as before. Let M be a finitely generated $A-$module, $x \in A$ a non-zero-divisor in M and let $M' = M/xM$, then we have the following relation in polynomials*

$$deg\, \chi_{\mathfrak{q}}^{M'} \leq deg\, \chi_{\mathfrak{q}}^{M} - 1.$$

Proof. Assume $N = xM$, then we have the following exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M' \longrightarrow 0$$

Now the ideal $\mathfrak{q}^n$ will give rise to the following exact sequence

$$0 \longrightarrow \frac{N}{N \bigcap \mathfrak{q}^n M} \longrightarrow \frac{M}{\mathfrak{q}^n M} \longrightarrow \frac{M'}{\mathfrak{q}^n M'} \longrightarrow 0$$

Now if we assume that $g(n) = l\left(\frac{N}{N \bigcap \mathfrak{q}^n M}\right)$, we will have for $n \gg 0$

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0.$$

Now *theorem 10.9* in *Introduction to Commutative Algebra* by Atiyah and MacDoanald states that if M' is a submodule of finitely generated module M and (M_n) a stable filtration, then $(M' \bigcap M_n)$ is also a stable filtration of M'. Applying this theorem here, we have that $(N \bigcap \mathfrak{q}^n M)$ is a stable filtration of N. Also note that $M \cong N$ (via the map $m \mapsto xm$, and isomorphism because x is non-zero-divisor in M.), thus from theorem part 3) of theorem 1.3.7, $g(n)$ and $\chi_{\mathfrak{q}^M}$ have the same leading coefficient, and the statement of the theorem follows. $\square$

If we put $M = A$ in the above theorem, and follow the notation described previously, we get the following statement

Corollary 1.3.11. *If A is a Noetherian local ring and x is a non-zero-divisor in A, then*

$$d\left(\frac{A}{(x)}\right) \leq d(A) - 1.$$

Now we prove the second determining result of this section:

Theorem 1.3.12. *dim* $A \leq d(A)$.

Proof. We prove this theorem by induction on $d(A)$. If $d(A) = 0$, then for $n \gg 0$, $l(A/\mathfrak{m}^n)$ will be constant, thus for some n, we will have $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, and thus by Nakayama's lemma we have that $\mathfrak{m}^n = 0$. And now because A is a Noetherian ring, and 0 is a product of maximal ideals, we have that A is Artin ring, and thus $\dim A = 0$. Now assume that $d(A) > 0$, and take any chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r$ of prime ideals in A. Take $x \in \mathfrak{p}_1/\mathfrak{p}_0$. Now let $A' = A/\mathfrak{p}_0$, and let x' be the image of x in A'. Then as A' is an integral domain and $x' \neq 0$ in A', we have by corollary 1.3.11 that

$$d\left(\frac{A'}{(x')}\right) \leq d(A') - 1.$$

Now if $\mathfrak{m}'$ is a maximal ideal of A', then $A'/\mathfrak{m}'^n$ is isomorphic to a subring of $A/\mathfrak{m}^n$ and so

$$l\left(\frac{A'}{\mathfrak{m}'^n}\right) \leq l\left(\frac{A}{\mathfrak{m}^n}\right)$$

and thus we have that $d(A') \leq d(A)$. So then we have that

$$d\left(\frac{A'}{(x')}\right) \leq d(A) - 1.$$

Now, we use the inductive hypothesis to conclude our proof. By inductive hypothesis, any chain of prime ideals in $A'/(x')$ is of length $\leq d(A) - 1$, but also the images of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ for a chain of length $r - 1$ in $A'/(x')$, thus we have that $r - 1 \leq d(A) - 1 \implies r \leq d(A)$. As we have taken any arbitrary chain of primes, we have that *dim* $A \leq d(A)$. ☐

Now we prove the last theorem to prove the main theorem of this section.

Theorem 1.3.13. *dim* $A \geq \delta(A)$.

Proof. Assume that $\dim A = d$. Then we prove this theorem by showing that there exists an $\mathfrak{m}-$primary ideal in A generated by d elements. We construct these generators $x_1, \ldots, x_d$ in such a way such that for each i, every prime ideal containing $(x_1, \ldots, x_i)$ has height $\geq i$. For $i = 0$ it is obvious. Now assume $i > 0$ and we have constructed $x_1, \ldots, x_{i-1}$. Suppose we have (if there exists) minimal prime ideals $\{\mathfrak{p}_j\}_{1 \leq j \leq s}$ which contain $(x_1, \ldots, x_{i-1})$ and are of height exactly $i - 1$. We have

$\mathfrak{p}_j \neq \mathfrak{m} \forall j$ as $i - 1 < d = \text{height}\, \mathfrak{m}$, and thus it follows that $\mathfrak{m} \neq \bigcup_{j=1}^{s} \mathfrak{p}_j$. Now take $x_i \in \mathfrak{m} / \bigcup_{j=1}^{s} \mathfrak{p}_j$. Now let $\mathfrak{q}$ be any prime ideal which contains $(x_1, \dots, x_i)$. Thus $\mathfrak{q}$ will contain some minimal prime ideal $\mathfrak{p}$ associated with $(x_1, \dots, x_{i-1})$. Now there are two possibilities, first that if $\mathfrak{p} = \mathfrak{p}_j$ for some j, then $x_i \in \mathfrak{q}$ and $x_i \notin \mathfrak{p}$, and hence $\mathfrak{q} \supset \mathfrak{p}$, and thus height $\mathfrak{q} \geq i$. Now if $\mathfrak{p} \neq \mathfrak{p}_j$ for all j, then height $\mathfrak{q} \geq i$ and thus $\mathfrak{p} \geq i$. Thus we have proven that every prime ideal containing $(x_1, \dots, x_i)$ has height $\geq i$.
Now we prove that $(x_1, \dots, x_d)$ is primary. We will prove that it's radical is $\mathfrak{m}$. Now if $\mathfrak{p}$ is a prime ideal and it contains $(x_1, \dots, x_d)$, then height $\mathfrak{p} \geq d$, but that implies that $\mathfrak{p} = \mathfrak{m}$ as height $\mathfrak{m} = d$. And thus we are done. □

Now we give the main theorem of this section.

Theorem 1.3.14. *Dimension theorem. For a Noetherian local ring A, the numerical values of these three integers are equal:*
1) The supremum of the lengths of all the chains of prime ideals in A.
2) The degree of characteristic polynomial $\chi_{\mathfrak{m}}(n)$, $d(A)$.
3) Least number of generators of a $\mathfrak{m}-$primary ideal of A, $\delta(A)$.

Proof. Follows directly from theorems 1.3.9, 1.3.12 and 1.3.13. □

Chapter 2

Varieties

Proofs of theorems in this chapter are omitted. For their proofs refer to *Algebraic Geometry* by Robin Hartshorne.

2.1 Affine and Projective Varieties

In this section we studied ***affine varieties*** and ***projective varieties*** from section 1 and section 2 of chapter 1 *Algebraic Geometry* by *Robin Hartshorne.* Some of the important theorems of which we studied proofs in this section are stated below.

Theorem 2.1.1. *There is one-to-one correspondence between inclusion reversing correspondence between algebraic sets in $\mathbb{A}^n$ and radical ideals in $A = k[x_1, \ldots, x_n]$. Furthermore an algebraic set is irreducible iff its corresponding radical ideal is a prime ideal.* □

Theorem 2.1.2. *Every algebraic set Y in $\mathbb{A}^n$ can be represented as union of varieties $Y = Y_1 \bigcup Y_2 \bigcup \ldots \bigcup Y_n$. If we assume that $Y_j \not\subseteq Y_i$, for each $i \neq j$, then these varieties Y_i are uniquely determined.* □

Theorem 2.1.3. *Let $Y \subset \mathbb{A}^n$ be an affine algebraic set and let $A(Y)$ be it's coordinate ring. Then dimension of Y is equal to the dimension of $A(Y)$.* □

If $f \in k[x_0, x_1, \ldots, x_n]$ is a linear homogeneous polynomial, then the solution set of f is called a hyperplane. Now if $f = x_i$, then we denote this hyperplane by H_i, for $0 \leq i \leq n$. Now define open subsets $U_i \in \mathbb{P}^n$ to be $\mathbb{P}^n - H_i$. Then $\mathbb{P}^n$ is covered by $U_i's$. Now we define a mapping $\varphi_i : U_i \longrightarrow \mathbb{A}^n$ as follows: If $(a_0, a_1, \ldots, a_n) \in U_i$, then

$$(a_0, a_1, \ldots, a_n) \mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}\right).$$

Note that in the above map we have omitted a_i/a_i. Now we have the following theorem:

Theorem 2.1.4. *The map φ_i gives a homeomorphism between U_i and $\mathbb{A}^n$, where U_i inherits topology from $\mathbb{P}^n$ and $\mathbb{A}^n$ has Zariski topology.* □

Note that the above theorem implies that any projective (quasi-projective) can be covered by affine (quasi-affine) varieties. It can also be proven that φ_i is indeed isomorphism of varieties for all i.

2.2 Morphisms

Theorem 2.2.1. *If f and g are two regular functions on a variety X such that they agree on a open subset $U \subseteq X$, then $f = g$ agree on X.* □

Theorem 2.2.2. *Let $Y \subseteq \mathbb{A}^n$ be an affine variety with $A(Y)$ being it's coordinate ring. Then the following statements are true:*
1) Ring of all regular functions on Y, $\mathcal{O}(Y)$ is isomorphic to $A(Y)$, i.e., $\mathcal{O}(Y) \cong A(Y)$.
2) For each point $P \in Y$, we define $\mathfrak{m}_P \subseteq A(Y)$ to be the ideal of all vanishing at P. Then there is a one to one correspondence between points of Y and maximal ideals of $A(Y)$, given by $P \mapsto \mathfrak{m}_P$.
3) $\mathcal{O}_P \cong A(Y)_{\mathfrak{m}_P}$, and $dim\,\mathcal{O}_P = dim\,Y$.
4) The function field of Y, $K(Y)$ is isomorphic to the quotient field of $A(Y)$. □

Now we state a similar theorem for projective varieties, but before that some notation: If S is a graded ring, then $S_{(\mathfrak{p})}$ denotes the subring of elements of degree 0 in the localization of S with respect to multiplicative subset T of S, which contains all the homogeneous elements of S which are not in $\mathfrak{p}$. Now if $f \in S$, we denote by $S_{(f)}$ the subring of elements of degree 0 in the ring S_f.

Theorem 2.2.3. *Let $Y \subseteq \mathbb{P}^n$ be a projective variety with homogeneous coordinate ring $S(Y)$, then*

1) $\mathcal{O}(Y) \cong k$.
2) For any point $P \in Y$*, we define* $\mathfrak{m}_P \subseteq S(Y)$ *to be ideal generated by homogeneous functions* $f \in S(Y)$ *which vanish at* P*, then* $\mathcal{O}_P \cong S(Y)_{(\mathfrak{m}_P)}$.
3)$K(Y) \cong S(Y)_{((0))}$. $\square$

Theorem 2.2.4. *Let* X *be any variety and let* Y *be an affine variety. Then we have a natural bijection between the following set*

$$Hom_{varieties}(X, Y) \longleftrightarrow Hom_{k-algebra}((A(Y), \mathcal{O}(X)))\ .$$

$\square$

Theorem 2.2.5. *Let* X *and* Y *be two affine varieties, then* X *and* Y *are isomorphic as varieties* $\iff$ $A(X)$ *and* $A(Y)$ *are isomorphic as* $k-$*algebras.* $\square$

2.3 Rational Maps

Theorem 2.3.1. *Let* X *and* Y *be two varieties and let* φ *and* ψ *be two morphisms from* X *to* Y *such that they agree on some nonempty open subset* U *of* X*, then they agree on whole of* X. $\square$

Definition 2.3.2. Let X and Y be two varieties, then a rational map $\varphi : X \longrightarrow Y$ is an equivalence class of pairs $\langle U, \varphi_U \rangle$, where φ_U is a morphism from U to Y, and $\langle U, \varphi_U \rangle \sim \langle V, \varphi_V \rangle$ if $\varphi_U|_{U\cap V} = \varphi_V|_{U\cap V}$. A rational map is called birational if it has an inverse rational map.

Theorem 2.3.3. *For any two varieties* X *and* Y*, the following are equivalent.*
1) X *and* Y *are birationally equivalent.*
2) There exists open subsets $U \subseteq X$ *and* $V \subseteq V$ *such that* $U \cong V$.
3) Function fields of X *and* Y *are isomorphic as* $k-$*algebras.* $\square$

2.4 Nonsingular Varieties

Definition 2.4.1. Nonsingular Variety. Let $Y \subseteq \mathbb{A}^n$ be an affine variety, and let $I(Y) = \langle f_1, f_2, \ldots, f_t \rangle$, where $f_i \in k[x_1, x_2, \ldots, x_n]$ for all i. Then Y is called non-singular at a point $P \in Y$, if the matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_1}|_P & \cdots & \frac{\partial f_1}{\partial x_n}|_P \\ \vdots & \ddots & \vdots \\ \frac{\partial f_t}{\partial x_n}|_P & \cdots & \frac{\partial f_t}{\partial x_n}|_P \end{bmatrix}$$

has rank $n - r$, where r is the dimension of Y. Variety Y is called non-singular if it is non-singular at every point.

Definition 2.4.2. Regular Local Ring. Noetherian local ring A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$ is regular local ring if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$.

Theorem 2.4.3. *Let $P \in Y \subseteq \mathbb{A}^n$, where Y is an affine variety. Then Y is non-singular at $P \iff \mathcal{O}_{P,Y}$ is a regular local ring.*

Multiplicity and Intersection Multiplicity.

Definition 2.4.4. Intersection Multiplicity. If Y and Z are two curves in $\mathbb{A}^2$, given by equations $f = 0$ and $g = 0$ respectively, and if $P \in Y \cap Z$, then we define the intersection multiplicity $(Y.Z)_P$ to be length of $\mathcal{O}_P$-module $\frac{\mathcal{O}_P}{(f,g)}$.

Here are some examples:

Example1. Let $x = 0$ and $y = 0$ be two curves in $\mathbb{A}^2$, then intersection multiplicity of these two curves at at $(0,0)$ is the length of $k[x,y]_{(x,y)}$ module $\frac{k[x,y]_{(x,y)}}{(x,y)} \cong k$, length of which is 1.

Example2. Let the curves Y and Z be given by $y = x^2$ and $y^2 = x^3$ respectively. These two curves intersect at $(0,0)$ and $(1,1)$. At $(0,0)$

$$(Y.Z)_{(0,0)} = \text{length of } \; k[x,y]_{(x,y)} \text{ module } \frac{k[x,y]_{(x,y)}}{(y^2 - x^3, y - x^2)}$$

$$\frac{k[x,y]_{(x,y)}}{(y^2 - x^3, y - x^2)} \cong \frac{k[x]_{(x)}}{(x^4 - x^3)} \cong k \oplus k[x] \oplus k[x^2]$$

Definition 2.4.5. Multiplicities. Let $Y \subseteq \mathbb{A}^2$ be a curve defined by $f(x,y) = 0$. Let $P = (a,b) \in \mathbb{A}^2$. Make a liner change $x \longmapsto x - a, y \longmapsto y - b$. and $f'(x,y) = f(x+a, y+b)$ and write $f' = f'_0 + f'_1 + f'_2 + \cdots f'_l$, where f'_i is the homogeneous polynomial of degree i in x and y. Then the multiplicity of P in Y, denoted by $\mu_P(Y)$ is the least l such that $f'_l \neq 0$.

Also note that $P = (a,b) \in \mathcal{Z}(f) \iff f_0'(0,0) = 0 \iff \mu_{(a,b)}(Y) > 0$. Thus we have that $P \in Y \iff \mu_P(Y) > 0$.

Theorem 2.4.6. *Let $Y \subseteq \mathbb{A}^2$ be defined by equation $f(x,y) = 0$, then $(0,0)$ is a smooth point $\iff \mu_{(0,0)}(Y) = 1$.*

Proof. We can write $f(x,y)$ as

$$f(x,y) = 0 + \left.\frac{\partial f}{\partial x}\right|_{(0,0)} x + \left.\frac{\partial f}{\partial y}\right|_{(0,0)} y + \text{higher order terms}$$

$$f(x,y) = \begin{bmatrix} \left.\frac{\partial f}{\partial x}\right|_{(0,0)} & \left.\frac{\partial f}{\partial y}\right|_{(0,0)} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \text{higher order terms.}$$

Now if $(0,0)$ is a smooth point, we will have *Rank* $\begin{bmatrix} \left.\frac{\partial f}{\partial x}\right|_{(0,0)} & \left.\frac{\partial f}{\partial y}\right|_{(0,0)} \end{bmatrix} = 1$, and thus $\mu_{(0,0)}(Y) = 1$.

And if $\mu_{(0,0)}(Y) = 1$, then either $\left.\frac{\partial f}{\partial x}\right|_{(0,0)} \neq 0$ or $\left.\frac{\partial f}{\partial y}\right|_{(0,0)} \neq 0$, and thus rank of matrix $\begin{bmatrix} \left.\frac{\partial f}{\partial x}\right|_{(0,0)} & \left.\frac{\partial f}{\partial y}\right|_{(0,0)} \end{bmatrix}$ will be one, and thus $(0,0)$ is a non-singular point. □

Chapter 3

Schemes

Proofs of some theorems in this chapter are omitted. For their proofs refer to *Algebraic Geometry* by Robin Hartshorne.

3.1 Sheaves

Definition 3.1.1. Presheaf. Let X be a topological space. A *presheaf* $\mathcal{F}$ of abelian groups on X is a rule which assigns to each open set $U \subset X$ an abelian group $\mathcal{F}(U)$ and to each inclusion $V \subset V$, a morphism of abelian groups $\rho_{UV} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ such that the following conditions are met:
1) ρ_{UU} is the identity map $\mathcal{F}(U) \longrightarrow \mathcal{F}(U)$.
2) For $W \subset V \subset U$, we have $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.
Note that we also require $\mathcal{F}(\emptyset) = \emptyset$.

If $\mathcal{F}$ is a presheaf on X, we refer to $\mathcal{F}(U)$ as sections of the presheaf $\mathcal{F}$ on U and we refer the maps ρ_{UV} as restriction maps. If $s \in \mathcal{F}(U)$, we sometimes write $s|_V$ is place of $\rho_{UV}(s)$.

Definition 3.1.2. Sheaf. A *sheaf* $\mathcal{F}$ on a topological space X is a presheaf which satifies the following additional properties:
1) Let $U = \{U_i\}_{i\in I}$ be a open covering of open set U of X and if $\exists s \in \mathcal{F}(U)$ such that $s|_{U_i} = 0 \, \forall \, i$, then $s = 0$.
2) Let $U = \{U_i\}_{i\in I}$ be a open covering of open set U of X and there exists a collections $s_i \in \mathcal{F}(U_i)$ such that

$$s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$$

then $\exists s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$.

Alternative Definition: A presheaf $\mathcal{F}$ is a sheaf if for any open cover $\{U_i\}_{i \in I}$ of open subset U of X, the following diagram is an equalizer diagram.

$$\mathcal{F}(U) \longrightarrow \prod_{i \in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j \in I} \mathcal{F}(U_i \bigcap U_j)$$

Now we give an example of a presheaf that is not a sheaf. Let X be a topological space and for an open set $U \subseteq X$, we define a rule $\mathcal{F}(U) = \{ f : U \longrightarrow \mathbb{R} \,|f \text{ is constant}\}$ and for $V \subset U$, define the restriction to be usual restriction of function. Then it is clear that it is a presheaf. Now we prove that it is not a sheaf. Let U_1 and U_2 be two disjoint nonempty open subsets of X and let $U = U_1 \bigcup U_2$ and define $f_1 \in \mathcal{F}(U_1)$ such that $f_1(u_1) = 0 \, \forall u_1 \in U_1$ and $f_2 \in \mathcal{F}(U_2)$ such that $f_2(u_2) = 1 \, \forall u_2 \in U_2$. Then the overlap condition $f_1|_{U_1 \bigcap U_2} = f_2|_{U_1 \bigcap U_2}$ is true because the intersection is empty. But the gluing condition that $\exists f \in \mathcal{F}(U)$ such that $f|_{U_1} = f_1$ and $f|_{U_2} = f_2$ is not true because f must be a constant $\forall u \in U = U_1 \bigcup U_2$.

Now in next theorem we give an example of a sheaf.

Theorem 3.1.3. *Let X be a variety over a field k. Assign open set $U \subset X$, set $\mathcal{O}(U)$, the ring of ring of regular functions from U to k and for $V \subset U$, let $\rho_{UV} : \mathcal{O}(U) \longrightarrow \mathcal{O}(V)$ be the usual restriction map. Then $\mathcal{O}$ is a sheaf of rings on X.*

Proof. It is clear that it is a presheaf. □

Definition 3.1.4. Stalk of a presheaf. The stalk of a presheaf $\mathcal{F}$ on a topological space X at a point $P \in X$ is

$$\mathcal{F}_P = \lim_{P \in U} \mathcal{F}(U)$$

where lim denotes direct limit. The elements of $\mathcal{F}_P$ are called germs of sections of $\mathcal{F}$ at P.

Note that for any open set $U \subseteq X$, there is a canonical map:

$$\mathcal{F}(U) \longrightarrow \prod_{P \in U} \mathcal{F}_P$$

given by $s \longmapsto \prod_{P \in U} < U, s >$.

Theorem 3.1.5. *Let X be a topological space and $\mathcal{F}$ be a sheaf on X. Then for every open set $U \subseteq X$, the map $\mathcal{F}(U) \longrightarrow \prod_{P \in U} \mathcal{F}_P$ is injective.*

Proof. Let $s, s' \in \mathcal{F}(U)$ map to the same element in $\prod_{P \in U} \mathcal{F}_P$. This means that for all $P \in U$, s and s' have the same image in the stalks $\mathcal{F}_P$. So for every $P \in U$, there exists a neighborhood V_P of P such that $P \in V_P \subseteq U$, with the property that $s|_{V_P} = s'|_{V_P}$. Now $U = \{V_P\}_{P \in U}$ is an open covering of U. As $(s - s')|_{V_P} = 0$ for all $P \in U$, by the uniqueness condition of being a $\mathcal{F}$ sheaf, we have that $s = s'$, and thus the map is injective. $\square$

Definition 3.1.6. Morphism of presheaves. A *morphism* $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ of presheaves(or sheaves) is a rule which assigns each open set $U \subset X$ a morphism $\phi(U) : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ of abelian groups such that for inclusion of open set $V \subset U$ the following diagram commutes

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r, "\phi(U)"] \arrow[d, "\rho_{UV}"'] & \mathcal{G}(U) \arrow[d, "\rho'_{UV}"] \\ \mathcal{F}(V) \arrow[r, "\phi(V)"'] & \mathcal{G}(V) \end{tikzcd}$$

Note that ρ and ρ' are restriction maps of $\mathcal{F}$ and $\mathcal{G}$ respectively. And also that morphism $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ induces a morphism $\phi_P : \mathcal{F}_P \longrightarrow \mathcal{G}_P$ on stalk level for each $P \in X$.

Theorem 3.1.7. *A morphism $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ of sheaves is isomorphism $\iff$ the induced morphism on stalk level $\phi_P : \mathcal{F}_P \longrightarrow \mathcal{G}_P$ is isomorphism for each $P \in X$.*

Proof. We first assume that ϕ_P is an isomorphism. We show that for any open subset $U \subseteq X$, $\phi(U) : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ is an isomorphism and then define the inverse morphism ψ for ϕ by $\psi(U) = \phi(U)^{-1}$ for open $U \subseteq X$. *Injectivity of* $\phi(U)$. Let $s \in \mathcal{F}(U)$ such that $\phi(U)(s) = 0$ in $\mathcal{G}(U)$. Thus for every point $P \in U$, we have that image of $\phi(U)(s)$, $\phi(U)(s)_P \equiv < U, \phi(U)(s) >$ in the stalk $\mathcal{G}_P$ is zero as $\phi(U)(s)$ is zero. As ϕ_P is injective, we have that $s_P \equiv < U, s >$ in $\mathcal{F}_P$ is zero. Now s_P being zero means that there exists a neighborhood W_P of P such that $s_P \equiv < W_P, 0 >$, and thus there exists a neighborhood $Y_P \subseteq U$, such that $s|_{Y_P} = 0$. Now U can be covered by these neighborhoods Y_P by varying P, and thus the first sheaf property we have that $s = 0$. *Surjectivity of* $\phi(U)$. Assume that $t \in \mathcal{G}(U)$. For $P \in U$, let t_P denotes its germ at P. Now since ϕ_P is surjective, there exists $s_P \in \mathcal{F}_P$ such that $\phi_P(s_P) = t_P$. Now let $s_P \in \mathcal{F}_P$ be denoted by $< V_P, s(P) >$, where V_P is a neighborhood of P and $s(P) \in \mathcal{F}(V_P)$. Then $\phi(V_P)(s(P))$ and $t|_{V_P}$ are two elements of $\mathcal{G}(V_P)$ such that both of them have same germ at P. Hence they agree on an open

subset of V_P. So, if necessary, replacing V_P by a smaller neighborhood of V_P, we may assume that $\phi(V_P)(s(P)) = t|_{V_P}$ in $\mathcal{G}(V_P)$. Now U is covered by such neighborhoods V_P and each $\mathcal{F}(V_P)$ contains a section $s(P)$. Now if $P, Q \in X$, then note that their restriction $s(P)|_{V_P \bigcap V_Q}$ and $s(P)|_{V_P \bigcap V_Q}$ in $\mathcal{F}(V_P \bigcap V_Q)$ maps to $t|_{V_P \bigcap V_Q}$ by ϕ. And since ϕ is injective as proven above, we have that $s(P)|_{V_P \bigcap V_Q} = s(Q)|_{V_P \bigcap V_Q}$. Now by sheaf property 2), there exists $s \in \mathcal{F}(U)$ such that $s|_{V_P} = s(P)$ for all $P \in X$. Now it is easy to prove that $\phi(U)(s) = t$.
Now assume that ϕ is isomorphism and we try to show that $\phi_P : \mathcal{F}_P \longrightarrow \mathcal{G}_P$ is an isomorphism $\forall\, P \in X$. *Injectivity of* ϕ_P. Let $s_P \in \mathcal{F}_P$ such that $\phi_P(s_P) = 0$. Let s_P be denoted by $< V_P, s >$, where V_P is neighborhood of P and $s \in \mathcal{F}(V_P)$. Then $\phi_P(s_P)$ is given by $< V_P, \phi(V_P)(s) >$. As $\phi_P(s_P) = 0$, we have that, if needed restricting to a neighborhood $U_P \subseteq V_P$ of P, $\phi(V_P)(s)|_{U_P} = 0$, or $\phi(U_P)(s|_{U_P}) = 0$ because ϕ is injective, we have that $s|_{U_P} = 0$, which will imply that $s_P = 0$. *Surjectivity of* ϕ_P. Let $t_P \in \mathcal{G}_P$. Let $< V_P, t(P) >$, where V_P is a neighborhood of P. As ϕ is surjective, there exists $s(P)$ such that $\phi(V_P)(s(P)) = t(P)$. Now let the germ of $s(P)$ of P, be denoted by s_P, $< V_P, s(P) > \equiv s_P$. Then $\phi_P(s_P) =< V_P, t(P) >= t_P$. $\square$

Definition 3.1.8. kernel, cokernel, image. Let $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves. Then we define presheaf kernel of ϕ to be presheaf given by $U \mapsto \ker(\phi(U))$. Similarly we define presheaf cokernel and presheaf image of ϕ to be presheaves given by $U \mapsto \operatorname{coker}(\phi(U))$ and $U \mapsto \operatorname{image}(\phi(U))$ respectively.

Note that $U \mapsto \ker(\phi(U))$ satifies all the conditions of being a presheaf as follows. We define restriction map for $V \subset U$, from $\ker(\phi(U))$ to $\ker(\phi(V))$ such that the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & \ker(\phi(U)) \arrow[r] \arrow[d, dotted, "T"'] & \mathcal{F}(U) \arrow[r, "\phi(U)"] \arrow[d, "\rho_{UV}"'] & \mathcal{G}(U) \arrow[d, "\rho'_{UV}"'] \\
0 \arrow[r] & \ker(\phi(V)) \arrow[r] & \mathcal{F}(V) \arrow[r, "\phi(V)"'] & \mathcal{G}(V)
\end{tikzcd}$$

The above diagram commutes because for $x \in \ker(\phi(U)) \subset \mathcal{F}(U)$, we have $\phi(V) \circ \rho_{UV}(x) = \rho'_{UV} \circ \phi(U)(x) = 0$. Note that the map T can be viewed as restriction of restriction map of $\mathcal{F}$ and it is easy to see that $U \mapsto \ker(\phi(U))$ satisfies all the presheaf criterion via this map.

Theorem 3.1.9. *The presheaf kernel of a sheaf morphism* $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ *is a sheaf.*

Proof. Let U be a open set of X and let $\{U_i\}_{i\in I}$ be an open cover of U.
1) Let $s \in \ker(\phi(U)) \subseteq \mathcal{F}(U)$ such that $s|_i = 0\,\forall i$. Then $\mathcal{F}$ is sheaf $\implies s = 0$.
2) Let for each i, let $s_i \in \ker(\phi(U_i))$ such that $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$. Then as above, as $\mathcal{F}$ is a sheaf $\exists s \in \mathcal{F}(U)$ such that $s|_i = s_i$, and $\phi(U)(s) \in \mathcal{G}(U)$. Now see the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker(\phi(U)) \arrow[r] \arrow[d] & \mathcal{F}(U) \arrow[r, "\phi(U)"] \arrow[d, "\rho_{UU_i}"'] & \mathcal{G}(U) \arrow[d, "\rho'_{UU_i}"'] \\
0 \arrow[r] & \ker(\phi(U_i)) \arrow[r] & \mathcal{F}(U_i) \arrow[r, "\phi(U_i)"'] & \mathcal{G}(U_i)
\end{tikzcd}$$

Then for each i

$$\phi(U)(s)|_{U_i} = \rho'_{UU_i} \circ \phi(U)(s) = \phi(U_i) \circ \rho_{UU_i}(s) = \phi(U_i)(s_i) = 0$$

So by sheaf property of $\mathcal{G}$, we have that $\phi(U)(s) = 0 \implies s \in \ker(\phi(U))$ and we are done. $\square$

Sheafification. Here we will define sheaf associated to a presheaf.

Theorem 3.1.10. *Given a presheaf $\mathcal{F}$, there exists a sheaf $\mathcal{F}^+$ and a morphism $\theta : \mathcal{F} \longrightarrow \mathcal{F}^+$, with the following universal property: For any given sheaf $\mathcal{G}$ and any morphism $\gamma : \mathcal{F} \longrightarrow \mathcal{G}$, the following diagram commutes*

$$\begin{tikzcd}
\mathcal{F} \arrow[r, "\gamma"] \arrow[d, "\theta"'] & \mathcal{G} \\
\mathcal{F}^+ \arrow[ur, dotted, "\exists!\psi"'] &
\end{tikzcd}$$

Furthermore the pair $(\mathcal{F}^+, \theta)$ is unique upto unique isomorphism.

Proof. The sheaf $\mathcal{F}^+$ is constructed as follows: For any open subset $U \subseteq X$ define

$$\mathcal{F}^+(U) = \{(s_P) \in \prod_{P\in U} \mathcal{F}_P \text{ such that } (*)\}$$

where $(*)$ is the following condition:
$(*)$ For every $P \in U$, there exists a neighborhood $P \in V \subset U$ and a section $\sigma \in \mathcal{F}(V)$ such that for all $Q \in V$, we have that $s_Q =< V, \sigma >$ in $\mathcal{F}_Q$.

For $V \subset U \subset X$ open, we have the projection map

$$\prod_{P \in U} \mathcal{F}_P \longrightarrow \prod_{Q \in V} \mathcal{F}_Q$$

the above projection map maps the element of $\mathcal{F}^+(U)$ to $\mathcal{F}^+(V)$. Now it is clear that this induced map gives $\mathcal{F}^+$ structure of a presheaf.
Note that the map $\mathcal{F}(U) \longrightarrow \prod_{P \in U} \mathcal{F}_P$ defined in *theorem 3.1.2* has the image in $\mathcal{F}^+(U)$. For open subsets $V \subset U \subset X$ we have the following commutative diagram

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r] \arrow[d] & \mathcal{F}^+(U) \arrow[r] \arrow[d] & \prod_{P \in U} \mathcal{F}_P \arrow[d] \\ \mathcal{F}(V) \arrow[r] & \mathcal{F}^+(V) \arrow[r] & \prod_{Q \in V} \mathcal{F}_Q \end{tikzcd}$$

Here the vertical maps are restriction mappings. Note that thus we have a canonical morphism of presheaves $\mathcal{F} \longrightarrow \mathcal{F}^+$. Now we prove that it is a sheaf as follows(assuming theat $\prod(\mathcal{F})$ is a sheaf.): *first condition.* Let $U = \bigcup_{i \in I} U_i$ be a open cover, and $s = (s_u)_{u \in U} \in \mathcal{F}^+(U)$ such that $s|_{U_i} = (s_u)_{u \in U_i} = 0$ for all i. Now $s \in \prod_{u \in U} \mathcal{F}_u$ as $\mathcal{F}^+(U) \subseteq \prod_{u \in U} \mathcal{F}_u$. As $s|_{U_i} = 0$ in $\prod_{u \in U_i} \mathcal{F}_{u \in U_i}$ and $\prod(\mathcal{F})$ is a sheaf, we have that $s = 0$, and we are done. *Second condition.* Again let $U = \bigcup_{i \in I} U_i$ be an open cover. Suppose we have that $s_i = (s_{i,u})_{u \in U_i} \in \mathcal{F}^+(U_i)$ for each i, and for each i and j, s_i and s_j agree over $U_i \bigcap U_j$. Now as $\prod_{P \in U} \mathcal{F}_P$ is a sheaf, there exists $s = (s_u)_{u \in U} \in \prod_{u \in U} \mathcal{F}_u$ such that $s|_{U_i} = s_i$. We check property $(*)$ defined above for s. Now if $u \in U$, then $u \in U_i$ for some i. Then by $(*)$ for s_i, there exists open subset V, such that $u \in V \subset U_i$ and also $\sigma \in \mathcal{F}(V)$, with the property that for all $v \in V$, $s_{i,v} =< V, \sigma >$ in $\mathcal{F}_v$. Now by the restriction map, we have that $s_v = s_{i,v}$, and thus the $(*)$ is satisfied for s, and so $s \in \mathcal{F}^+(U)$, and second condition for being a sheaf is also satisfied by $\mathcal{F}^+$.
Now let $(\mathcal{F}'^+, \theta')$ be another tuple such that it satifies the condition given in the theorem. Then we have the following two commutative diagrams

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\theta'"] \arrow[d, "\theta"] & \mathcal{F}'^+ \\ \mathcal{F}^+ \arrow[ur, dotted, "\exists!\, \Psi"'] & \end{tikzcd} \qquad \begin{tikzcd} \mathcal{F} \arrow[r, "\theta"] \arrow[d, "\theta'"] & \mathcal{F}^+ \\ \mathcal{F}'^+ \arrow[ur, dotted, "\exists!\, \Psi'"'] & \end{tikzcd}$$

So we have that $\Psi \circ \theta = \theta'$ and $\Psi' \circ \theta' = \theta$. Thus we have that $\Psi' \circ \Psi = \mathrm{id}_{\mathcal{F}^+}$ and $\Psi \circ \Psi' = \mathrm{id}_{\mathcal{F}'^+}$, and now it is easy to see that the uniqueness condition is satisfied. For any sheaf $\mathcal{G}$, and any morphism $\mathcal{F} \longrightarrow \mathcal{G}$ factors through $\mathcal{F}^+$ uniquely, we will prove after proving *theorem 3.1.6.* $\square$

Sheaf $\mathcal{F}^+$ is call sheaf associated to presheaf $\mathcal{F}$.

Theorem 3.1.11. *Let $\mathcal{F}$ be a presheaf on topological space X, then for any $P \in X$, we have that $\mathcal{F}_P = \mathcal{F}^+_P$. Here $\mathcal{F}^+$ is the sheaf associated to prehseaf $\mathcal{F}$.*

Proof. As the map $\mathcal{F}_P \longrightarrow \prod(\mathcal{F})_P$ is injective, we have that $\mathcal{F}_P \longrightarrow \mathcal{F}^+_P$ is injective. Now we show that this map is surjective. Assume that $\bar{s} \in \mathcal{F}^+_P$, then there exists open neighborhood U with $P \in U$ such that $\bar{s} \equiv < U, s >$ with $s \in \mathcal{F}^+(U)$. Now using property $(*)$, there exists an open neighborhood $P \in V \subset U$, and a section $\sigma \in \mathcal{F}(V)$ such that $s|_V = \sigma$ in $\mathcal{F}^+(V)$. Now equivalence class of $< V, \sigma >$, which is an element of $\mathcal{F}_P$ and it maps to $\bar{s}$. $\square$

Now we prove remaining part of *theorem 3.1.5*, that is if $\mathcal{G}$ is any sheaf, then any morphism $\mathcal{F} \longrightarrow \mathcal{G}$ will factor uniquely as $\mathcal{F} \longrightarrow \mathcal{F}^+ \longrightarrow \mathcal{G}$. For these we have the following commutative diagram:

$$\begin{tikzcd}
\mathcal{F} \arrow[r] \arrow[d] & \mathcal{F}^+ \arrow[r] \arrow[d] & \prod(\mathcal{F}) \arrow[d] \\
\mathcal{G} \arrow[r] & \mathcal{G}^+ \arrow[r] & \prod(\mathcal{G})
\end{tikzcd}$$

If we show that $\mathcal{G} = \mathcal{G}^+$, the we will be done, as that will show that morphism $\mathcal{F} \longrightarrow \mathcal{G}$ factors uniquely through $\mathcal{F}^+$. For this we show $\mathcal{G} \cong \mathcal{G}^+$, and thus using *theorem* 3.1.7, it is enough to show that $\forall x \in X$, $\mathcal{G}_x \cong \mathcal{G}^+_x$. And this follows from *theorem* 3.1.11.

Definition 3.1.12. Subsheaf of a Sheaf. A *subsheaf* of a sheaf $\mathcal{F}$ is a sheaf $\mathcal{F}'$ such that for any open subset $U \subseteq X$, $\mathcal{F}'(U)$ is a subset of $\mathcal{F}(U)$ and the restriction maps of sheaf $\mathcal{F}'$ are induced by those of $\mathcal{F}$.

Note that for a morphism of sheaves $\phi : \mathcal{F} \longrightarrow \mathcal{G}$, we define the *kernel* of ϕ to be the presheaf kernel of ϕ. For the same morphism, we define the *image* of ϕ to be the sheaf associated to the presheaf image of ϕ.

A sequence $\cdots \longrightarrow \mathcal{F}^{i-1} \xrightarrow{\phi^{i-1}} \mathcal{F}^{i} \xrightarrow{\phi^{i}} \mathcal{F}^{i+1} \longrightarrow \cdots$ of sheaves is *exact* if image $\phi^{i-1} = \ker \phi^i$.

Definition 3.1.13. Direct image sheaf, inverse image sheaf. Let $f : X \longrightarrow Y$ be a continuous function and let $\mathcal{F}$ is a sheaf on X. Then *direct image sheaf* $f_*\mathcal{F}$ of $\mathcal{F}$ on Y as follows

$$f_*\mathcal{F}(V) = \mathcal{F}(f^{-1}(V))$$

for any open set $V \subset Y$.
If $\mathcal{G}$ is a given sheaf on Y, we define *inverse image sheaf* $f^{-1}\mathcal{G}$ on X to be the sheaf associated to presheaf $U \mapsto \lim_{f(U)\subset V} \mathcal{G}(V)$, where U is any open set of X and limit is taken over all the open sets of Y which contain $f(U)$.

3.2 Schemes

Let A be a given ring. We define Spec$A$ to be the set of all prime ideals of A. Now if $\mathfrak{a} \subset A$ is an ideal of A, we define $V(\mathfrak{a})$ to be set of all prime ideals of A which contain $\mathfrak{a}$.

Theorem 3.2.1. *The set V satisfies the following criterion:*
1) For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A, we have $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \bigcup V(\mathfrak{b})$.
2) For a set $\{\mathfrak{a}_i\}_{i\in I}$ of ideals of A, we have $V(\sum \mathfrak{a}_i) = \bigcap V(\mathfrak{a}_i)$.
3) For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A, $V(\mathfrak{a}) \subseteq V(\mathfrak{b}) \iff \sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$.

Proof. 1) If $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b}) \implies \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Assume that $\mathfrak{b} \not\subseteq \mathfrak{p}$, then $\exists b \in \mathfrak{b}$ and $b \notin \mathfrak{b}$ and $a \in \mathfrak{a}$, then $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \implies a \in \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p} \implies V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a}) \bigcup V(\mathfrak{b})$.
If $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p} \implies \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \implies V(\mathfrak{a}) \bigcup V(\mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$.
2) Let $\sum \mathfrak{a}_\mathfrak{i} \subseteq \mathfrak{p}$, then $\mathfrak{a}_i \subseteq \mathfrak{p}\,\forall i$ as $\sum \mathfrak{a}_i$ is the smallest ideal of A containing all the ideals $\mathfrak{a}_i$. If $\mathfrak{a}_i \subseteq \mathfrak{p}\,\forall i$, then $\sum \mathfrak{a}_\mathfrak{i} \subseteq \mathfrak{p}$.
3) It can be inferred from the fact that radical of an ideal $\mathfrak{a}$ is equal to the intersection of all prime ideals which contain $\mathfrak{a}$. $\square$

Note that we can define a topology on Spec$A$ by taking all the subsets of the form $V(\mathfrak{a})$ to be closed subsets for the topology on Spec$A$. All the axioms of being a topological space follow from the previous theorem.
In the previous section of this chapter we defined the sheaf of abelian groups. In this section we will define the sheaf of rings $\mathcal{O}$ on Spec$A$.

Definition 3.2.2. Sheaf of rings on Spec$A$. For a open set $U \subseteq \mathrm{Spec}A$ define

$$\mathcal{O}(U) = \{\ s : U \longrightarrow \coprod_{\mathfrak{p}\in U} A_{\mathfrak{p}} | s(\mathfrak{p}) \in A_{\mathfrak{p}} \text{ for all } \mathfrak{p} \text{ and } s \text{ is locally a quotient of elements of } A.\ \}$$

Here $A_{\mathfrak{p}}$ is localization of A at $\mathfrak{p}$, and by being locally a quotient of elements of A we mean that $\forall\, \mathfrak{p} \in U$, there exists a neighborhood of $\mathfrak{p}, V$ such that $V \subseteq U$, and elements $a, f \in A$ such that for each $\mathfrak{q} \in V, f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = a/f$ in $A_{\mathfrak{q}}$.

It is obvious that it is a ring and for $V \subseteq U$ with the restriction map $\mathcal{O}(U) \longrightarrow \mathcal{O}(V)$ is the homomorphism of rings, it is a sheaf.

Definition 3.2.3. Spectrum of a ring. Let A be a ring. The *Spectrum of ring* A is topological space Spec$A$ together with the sheaf of rings $\mathcal{O}$ on Spec$A$.

Let $f \in A$, and $D(f)$ denotes the open subset of Spec$A$ defined by complement of $V((f))$. All the open sets of the form $D(f)$, form a base for topology on Spec$A$ defined above.

Theorem 3.2.4. *Let A be a ring and $(SpecA, \mathcal{O})$ its spectrum.*
1) For any $\mathfrak{p} \in SpecA$, $\mathcal{O}_{\mathfrak{p}} \cong A_{\mathfrak{p}}$.
2) For any element $f \in A$, $\mathcal{O}(D(f)) \cong A_f$.
3) $\mathcal{O}(SpecA) \cong A$. □

Definition 3.2.5. Ringed Space. A *ringed space* is a pair $(X, \mathcal{O}_X)$, consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X. A morphism of ringed spaces $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ is a pair of maps $(f, f^{\#})$, where $f : X \longrightarrow Y$ is a continuous map and $f^{\#} : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ is a morphism of sheaves of rings on Y. The ringed space $(X, \mathcal{O}_X)$ is a *locally ringed space* if for each point $P \in X$, the stalk $\mathcal{O}_{X,P}$ is a local ring. A morphism of locally ringed spaces is a morphism $(f, f^{\#})$ of ringed spaces, such that for each point P, the map of local rings $f^{\#}_P : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ is local homomorphism of local rings.

Now we probe into the last condition of above definition. Assume we are given a point $P \in X$, and we have morphism of sheaves $f^{\#} : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$. Thus for every open set $V \subseteq Y$, we have a homomorphism of rings, $\mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(f^{-1}V)$. Now as V ranges over all the neighborhoods of $f(P)$, $f^{-1}(V)$ ranges over a subset of the neighborhoods of P. Thus we have a map:

$$\mathcal{O}_{Y,f(P)} = \varinjlim_{V} \mathcal{O}_Y(V) \longrightarrow \varinjlim_{f^{-1}V} \mathcal{O}_X(f^{-1}V),$$

and the latter limit above maps to the stalk at point P, $\mathcal{O}_{X,P}$. In this way, we have a morphism $f_P^{\#} : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$. We require this morphism to be a local morphism. A morphism $(f, f^{\#})$ is isomorphism if f is a homeomorphism of underlying topological spaces and $f^{\#}$ is isomorphism of sheaves.

Theorem 3.2.6. *We have the following for rings A, B and ring homomorphism $\phi : A \longrightarrow B$:*
1) $(Spec A, \mathcal{O})$ is locally ringed space.
2) ϕ induces a morphism of locally ringed spaces:

$$(f, f^{\#}) : (Spec B, \mathcal{O}_{Spec B}) \longrightarrow (Spec A, \mathcal{O}_{Spec A}) .$$

3) Any morphism of locally ringed spaces is induced by a ring homomorphism $A \longrightarrow B$.

□

Definition 3.2.7. Affine Scheme. An *affine scheme* is a locally ringed space $(X, \mathcal{O}_X)$ which is isomorphic as a locally ringed space to the spectrum of some ring. A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ in which every point has an open neighborhood U such that the topological space U, together with the restricted sheaf $\mathcal{O}_X|_U$, is an affine scheme.

We call X the *underlying topological space* of the scheme, and $\mathcal{O}_X$ is *structure sheaf*. A morphism of schemes is morphism of locally ringed spaces.

3.3 First Properties of Schemes

Definition 3.3.1. Connedted, Irreducible and Reduced Schemes. A scheme is *connected* if the topological space is connected and a scheme is *irreducible* if the underlying topological space is irreducible. A scheme X is *reduced* if for every open set U, the ring $\mathcal{O}_X(U)$ has no nilpotent elements. A scheme X is *integral* if for every open set $U \subseteq X$, the ring $\mathcal{O}_X(U)$ is an integral domain.

Definition 3.3.2. Locally Noetherian Schemes. A scheme X is *locally noetherian* if it can be covered by open affine subsets $Spec\, A_i$, where each A_i is noetherian ring. X is *noetherian* if it is locally noetherian and quasi-compact.

Definition 3.3.3. Morphism of finite type. A morphism $f : X \longrightarrow Y$ of schemes is called locally of finite type if there exists a covering of Y by open affine subsets

$V_i = \mathrm{Spec} B_i$, such that $f^{-1}(V_i)$ can be covered by open affine subsets $U_{ij} = \mathrm{Spec} A_{ij}$ for each i, where A_{ij} is finitely generated B_i-algebra. The morphism f is of finite type for each i, $f^{-1}(V_i)$ can be covered by finite number of U_{ij}.

Definition 3.3.4. Open Subscheme and Open Immersion. An *open subscheme* of a scheme X is a scheme U, whose topological space is an open subset of X, and whose structure sheaf $\mathcal{O}_U$ is isomorphic to the $\mathcal{O}_X|_U$, the restriction of $\mathcal{O}_X$, the structure sheaf of X. An *open immersion* is a morphism $f : X \longrightarrow Y$, such that there exists a isomorphism between X and an open subscheme of Y.

Definition 3.3.5. Closed immersion and Closed Subscheme. A *closed immersion* is a morphism $f : Y \longrightarrow X$ of schemes such that f induces an isomorphism between topological space Y and a closed subset of topological space X and also that the map $f^{\#} : \mathcal{O}_X \longrightarrow f_*\mathcal{O}_Y$ of sheaves is surjective. A *closed subscheme* of a scheme X is a equivalence class of closed immersions, with the following equivalence relation: $f : Y \longrightarrow X \ \sim \ f' : Y \longrightarrow X$ if there exists an isomorphism $i : Y' \longrightarrow Y$ such that the following diagram commutes

$$\begin{tikzcd} Y \arrow[r, "f"] & X \\ Y' \arrow[u, "i"] \arrow[ur, "f'"'] & \end{tikzcd}$$

Definition 3.3.6. Dimension of a Scheme. The *dimension* of a scheme X, denoted dim X, is its dimension as a topological space. If Z is an irreducible closed subset of X, then the *codimension* of Z in X, denoted by $\mathrm{codim}(Z, X)$ is the supremum of the lengths of the chain of following type

$$Z = Z_0 < Z_1 < \cdots < Z_n$$

where Z_i are distinct closed irreducible subsets of X. If Y is any closed subset of X, we define

$$\mathrm{codim}\,(Y, X) = \inf_{Z \subseteq Y} \mathrm{codim}\,(Z, X)$$

here infimum is taken over all closed irreducible subsets of Y.

Definition 3.3.7. Fibred Product. Let X, Y be schemes over another scheme S, then we define *fibred product* of X and Y over S, denoted by $X \times_S Y$, to be a scheme, together with morphisms $p_1 : X \times_S Y \longrightarrow X$ and $p_2 : X \times_S Y \longrightarrow Y$, which make a commutative diagram with the given morphisms $X \longrightarrow S$ and $Y \longrightarrow S$, such that given any scheme Z over S, and given morphisms $f : Z \longrightarrow X$ and $g : Z \longrightarrow Y$ which make a commutative diagram with the given morphism $X \longrightarrow S$ and $Y \longrightarrow S$, then there exists unique morphism $\theta : Z \longrightarrow X \times_S Y$ such that $f = p_1 \circ \theta$ and $g = p_2 \circ \theta$.

$$\begin{tikzcd}
Z \arrow[rr, dotted] \arrow[dr] \arrow[drrr] & & X \times_S Y \arrow[dl] \arrow[dr] & \\
& X \arrow[dr] & & Y \arrow[dl] \\
& & S &
\end{tikzcd}$$

3.4 Separated and Proper Morphisms

Definition 3.4.1. Seprated Morphism. Let $f : X \longrightarrow Y$ be a morphism of schemes. The *diagonal* morphism is the unique morphism $\Delta : X \longrightarrow X \times_Y X$, whose composition with the projection maps $p_1, p_2 : X \times_Y X \longrightarrow X$ is the identity map of $X \longrightarrow X$. Then morphism f is separated if Δ is a closed immersion. In that case X is said to be separated over Y. A scheme Y is called separated if it is separated over $\operatorname{Spec} \mathbb{Z}$.

A morphism is closed if the image of any closed subset is closed.

Definition 3.4.2. Universally Closed Morphism. A morphism $f : X \longrightarrow Y$ is universally closed if it is closed, and for any morphism $Y' \longrightarrow Y$, the corresponding morphism $f' : X' \longrightarrow Y'$ obtained by base extension is also closed.

Definition 3.4.3. Proper Morphism. A morphism $f : X \longrightarrow Y$ is proper if it is separated, of finite type and universally closed.

3.5 Differentials

Let A be a commutative ring with 1, and let B be an $A-$algebra, and let M be a $B-$module.

Definition 3.5.1. A-derivation of B. An $A-$ *derivation* of B into M is a map $d : B \longrightarrow M$ such that 1) $d(a_1b_1 + a_2b_2) = a_1d(b_1) + a_2d(b_2)$, 2) $d(b_1b_2) = b_1d(b_2) + b_2d(b_1)$.

Note that $d(a) = 0$ for all $a \in A$ as follows: $d(1_B) = d(1_B.1_B) = 1_B d(1_B) + 1_B d(1_B) \implies d(1_B) = 0$. Now $d(a) = ad(1_B) = 0$.

Definition 3.5.2. Module of Relative Differential Forms. The *module of relative differential forms* of B over A is a $B-$module $\Omega_{B/A}$, together with $A-$derivation $d : B \longrightarrow \Omega_{B/A}$, which satifies the following universal property: for any $B-$module M, and any given $A-$derivation $d' : B \longrightarrow M$, there exists a unique $B-$module homomorphism $f : \Omega_{B/A} \longrightarrow M$ such that the following diagram commutes:

$$\begin{tikzcd} B \arrow[r, "d'"] \arrow[d, "d"'] & M \\ \Omega_{B/A} \arrow[ur, dotted, "\exists! f"'] & \end{tikzcd}$$

Let B be an $A-$algebra. Now consider the homomorphism $f : B \otimes_A B \longrightarrow B$ defined by $b \otimes b' \longmapsto bb'$ and let I be its kernel. Now we give $B \otimes_A B$ an $B-$module structure by multiplication on left as follows: $b(b_1 \otimes b_2) \longmapsto bb_1 \otimes b_2$. This gives I/I^2 a $B-$module structure. Now we say that $\Omega_{B/A} = I/I^2$ and define $A-$derivation of B into $\Omega_{B/A}$ by $d : B \longrightarrow \Omega_{B/A}$ by $b \longmapsto 1 \otimes b - b \otimes 1 \pmod{I^2}$. Now we prove that d satisfies all the condition of being an $A-$derivation as follows:

1) $d(a_1b_1 + a_2b_2) = 1 \otimes (a_1b_1 + a_2b_2) - (a_1b_1 + a_2b_2) \otimes 1 = 1 \otimes a_1b_1 + 1 \otimes a_2b_2 - a_1b_1 \otimes 1 - a_2b_2 \otimes 1 = a_1(1 \otimes b_1 - b_1 \otimes 1) + a_2(1 \otimes b_2 - b_2 \otimes 1) = a_1d(b_1) + a_2d(b_2)$.

2) *Lebiniz Rule.* $d(bb') = 1 \otimes bb' - bb' \otimes 1 = 1 \otimes bb' - b \otimes b' + b \otimes b' - bb' \otimes 1$. Now we have that $b \otimes b' - bb' \otimes 1 = b(1 \otimes b' - b' \otimes 1) = bd(b')$. Now we will try prove that $1 \otimes bb' - b \otimes b' - b'd(b) \in I^2$. Note that $1 \otimes bb' - b \otimes b' - b'(1 \otimes b - b \otimes 1) = (1 \otimes b - b \otimes 1)(1 \otimes b' - b' \otimes 1) \in I.I = I^2$. And so $d(bb') = bd(b') + b'd(b)$, and we are done.

Now we prove define a map $f : \Omega_{B/A} \longrightarrow M$ given by $\sum_i (b_i \otimes b'_i) \mapsto \sum_i b_i d'(b'_i)$, where d' is $A-$derivation from B to M. It is easy to prove that this map f satisfies the universal property defined in *definition* 3.5.2.

3.6 Abelian Categories

Definition 3.6.1. Monomorphism, Epimorphism, Isomorphism. Let $\mathfrak{U}$ be a category and $A, B, C \in \mathrm{Ob}\,\mathfrak{U}$. A morphism $f \in \mathrm{Hom}_{\mathfrak{U}}(B, C)$ is called a monomorphism if $\forall g, h \in \mathrm{Hom}_{\mathfrak{U}}(A, B)$ with $f \circ g = f \circ h \implies g = h$. $f \in \mathrm{Hom}_{\mathfrak{U}}(A, B)$ is called an epimorphism if $\forall g, h \in \mathrm{Hom}_{\mathfrak{U}}(B, C)$ with $g \circ f = h \circ f \implies g = h$. $f \in \mathrm{Hom}_{\mathfrak{U}}(A, B)$ is called an isomorphism if there is morphism $g \in \mathrm{Hom}_{\mathfrak{U}}(B, A)$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.

Definition 3.6.2. Products, Coproducts, Biproducts. Let $\mathfrak{U}$ be a category and let $\{\mathfrak{U}_i | i \in I\}$ be a collection of objects in $\mathfrak{U}$.
• A product of the family $\{\mathfrak{U}_i | i \in I\}$ is an object P (often denoted $\prod_i \mathfrak{U}_i$) is an object of $\mathfrak{U}$ together with a family of morphisms $\{\pi_i : P \longrightarrow \mathfrak{U}_i | i \in I\}$ such that for any object Q and any collection of morphisms $\{\phi_i : Q \longrightarrow \mathfrak{U}_i | i \in I\}$, there is a unique morphism $\psi : Q \longrightarrow P$ such that $\pi_i \circ \psi = \phi_i$. For $I = \{1, 2\}$ this looks like

$$\begin{tikzcd}
 & Q \arrow[dl, "\phi_1"'] \arrow[d, "\exists!\,\psi"'] \arrow[dr, "\phi_2"] & \\
\mathfrak{U}_1 & \mathfrak{U}_1 \times \mathfrak{U}_2 \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & \mathfrak{U}_2
\end{tikzcd}$$

• A coproduct for the family $\{\mathfrak{U}_i | i \in I\}$ is an object C (often denoted $\sum_i \mathfrak{U}_i$)in the category $\mathfrak{U}$ together with a family of morphisms $\{c_i : \mathfrak{U}_i \longrightarrow C | i \in I\}$, such that for any object D and family of morphisms $\{d_i : \mathfrak{U}_i \longrightarrow D | i \in I\}$, there exists a unique homomorphism $d : C \longrightarrow D$ such that $d \circ c_i = d_i$. This can be shown in the diagram for $I = \{1, 2\}$ as

$$\begin{tikzcd}
\mathfrak{U}_1 \arrow[r, "c_1"] \arrow[dr, "d_1"'] & \mathfrak{U}_1 + \mathfrak{U}_2 \arrow[d, "\exists!\,d"'] & \mathfrak{U}_2 \arrow[l, "c_2"'] \arrow[dl, "d_2"] \\
 & D &
\end{tikzcd}$$

• Suppose now that $\mathfrak{U}$ has a zero object. A biproduct of the family $\{\mathfrak{U}_i | i = 1, 2, \cdots, n\}$ is an object B (often denoted $\bigoplus_i \mathfrak{U}_i$) of $\mathfrak{U}$ which is both product and coproduct of the family and for which the collection of morphisms π_i and c_j satisfy

$$\pi_i \circ c_j = \begin{cases} \mathrm{id}_{\mathfrak{U}_i}, & i = j \\ 0, & i \neq j \end{cases}$$

Definition 3.6.3. Kernels/co-kernels and Image/co-image. Let $\mathfrak{U}$ be a category with zero objects. Then, $\forall A, B \in \mathrm{Ob}\,\mathfrak{U}$ and $\forall f \in \mathrm{Hom}_{\mathfrak{U}}(A, B)$,
• the ***kernel*** of $f : A \longrightarrow B$ is pair (K, k) with $K \in \mathrm{Ob}\,\mathfrak{U}$ and $k : K \longrightarrow A$ such

that $f \circ k = 0$ and if there is a $g \in \mathrm{Hom}_{\mathfrak{U}}(P, A)$ such that $f \circ g = 0$, there exists a unique $h \in \mathrm{Hom}_{\mathfrak{U}}(P, K)$ such that $g = k \circ h$, that is

$$\begin{tikzcd} K \arrow[r, "k"] & A \arrow[r, "f"] & B \\ & P \arrow[ul, "\exists ! h"] \arrow[u, "g"'] & \end{tikzcd}$$

Equivalently the kernel of $f : A \longrightarrow B$ given by the following pullback diagram

$$\begin{tikzcd} K \arrow[r] \arrow[d, "k"] & 0 \arrow[d] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

• The cokernel of f is a pair (C, c) where $C \in \mathrm{Ob}\,\mathfrak{U}$ and $c : B \longrightarrow C$ such that $c \circ f = 0$ and if there is a $q \in \mathrm{Hom}_{\mathfrak{U}}(B, Q)$ such that $q \circ f = 0$, then $\exists ! d \in \mathrm{Hom}_{\mathfrak{U}}(C, Q)$ such that $d \circ c = q$, that is

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "c"] \arrow[d, "q"'] & C \arrow[dl, "\exists !\, d"] \\ & Q & \end{tikzcd}$$

• The image of f is kernel of its cokernel and coimage of f is the cokernel of its kernel.

Theorem 3.6.4. *The kernel of an monomorphism is isomorphic to 0, and the cokernel of an epimorphism is isomorphic to 0.* □

Definition 3.6.5. Pull Back or Fibred Product. Let $\mathfrak{M}$ be a metacategory. Let $f : A \longrightarrow C$ and $f : B \longrightarrow C$ be two morphisms with common codomain. The pullback of the morphisms f and g consists of an object P and two morphisms $p_1 : P \longrightarrow A$ and $p_2 : P \longrightarrow B$ for which the following diagram

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

commutes subject to the following universal mapping property:

For any commutative diagram

$$\begin{tikzcd} Q \arrow[r, "q_2"] \arrow[d, "q_1"'] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

there is a unique morphism $u : Q \longrightarrow P$ making the following diagram commute:

$$\begin{tikzcd} Q \arrow[dr, dotted, "u"] \arrow[drr, bend left, "q_2"] \arrow[ddr, bend right, "q_1"'] & & \\ & P \arrow[r, "p_2"] \arrow[d, "p_1"] & B \arrow[d, "g"] \\ & A \arrow[r, "f"'] & C \end{tikzcd}$$

Note that pullback P is also denoted by $A \times_C B$.

Definition 3.6.6. Abelian Category. An *abelian category* is a category $\mathfrak{U}$ such that:
1) For each $A, B \in \mathrm{Ob}\,\mathfrak{U}, \mathrm{Hom}\,(A, B)$ has structure of an abelian group, and the composition law is linear.
2) Finite direct sums exits.
3) Every morphism has kernel and cokernel.
4) Every monomorphism is the kernel of its cokernel, every epimorphism is the cokernel of its kernel.
5) Every morphism can be factored into an epimorphism followed by a monomorphism.

Following are the examples of abelian categories:
1) $\mathfrak{Ab}$, the category of abelian groups.

Theorem 3.6.7. *Let $\mathfrak{U}$ be an abelian category.Then a morphism which is both a monomorphism and an epimorphism is an isomorphism.* □

Theorem 3.6.8. *The kernel of an monomorphism is isomorphic to 0, and the cokernel of an epimorphism is isomorphic to 0.* □

Definition 3.6.9. Injective Object: An object I in abelian category $\mathfrak{U}$ is injective if for every injective morphism $A \longrightarrow B$ and for every morphism $A \longrightarrow I$ there exists a morphism $g : B \longrightarrow I$ which makes the following diagram commute:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[dl, "\exists g"] \\ & I & \end{tikzcd}$$

Equivalently an object I in $\mathfrak{U}$ is injective if functor $\mathrm{Hom}\,(\cdot, I)$ is exact. In an abelian category $\{0\}$ is an injective object.

Definition 3.6.10. Short Exact Sequence. We say a sequence

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

is a short exact sequence if $A \xrightarrow{\phi} B$ is isomorphic to kernel of ψ and $B \xrightarrow{\psi} C$ is isomorphic to the cokernel of ϕ.

Definition 3.6.11. Chain Complex. A complex $A^{\cdot}$ in a abelian category $\mathfrak{U}$ is a collection of objects $A^i, i \in \mathbb{Z}$ and morphisms $d^i : A^i \longrightarrow A^{i+1}$

$$\cdots \xrightarrow{d^{-3}} A^{-2} \xrightarrow{d^{-2}} A^{-1} \xrightarrow{d^{-1}} A^0 \xrightarrow{d^0} A^1 \xrightarrow{d^1} \cdots$$

such that $d^{i+1} \circ d^i = 0 \, \forall i$. A morphism of complexes $f : A^{\cdot} \longrightarrow B^{\cdot}$ is a set of morphisms $f^i : A^i \longrightarrow B^i$ for each i, which commutes with the co-boundary maps d^i.

Definition 3.6.12. The ith degree cohomology object. The ith degree cohomology object $h^i(A^{\cdot})$ of the complex $A^{\cdot}$ is defined as following

$$h^i(A^{\cdot}) = \frac{\ker d^i}{\mathrm{image}\, d^{i-1}}$$

A morphism of complexs $f^{\cdot} : A^{\cdot} \longrightarrow B^{\cdot}$ induces a morphism $h^i(f) : h^i(A^{\cdot}) \longrightarrow h^i(B^{\cdot})$.

Definition 3.6.13. Homotopy. Let $f, g : (A^{\cdot}, d_A) \longrightarrow (B^{\cdot}, d_B)$ be two morphisms of two complexs. A homotopy between f, g is a collection of morphisms $k^i : A^i \longrightarrow B^{i-1}$

for each i such that in the following diagram

$$\begin{tikzcd}
\cdots \arrow[r] & A^{i-1} \arrow[r] \arrow[d] & A^i \arrow[r, "d_A^i"] \arrow[d] \arrow[dl, "k^i"'] & A^{i+1} \arrow[r] \arrow[d] \arrow[dl, "k^{i+1}"'] & \cdots \\
\cdots \arrow[r] & B^{i-1} \arrow[r, "d_B^{i-1}"'] & B^i \arrow[r] & B^{i+1} \arrow[r] & \cdots
\end{tikzcd}$$

We have $f^i - g^i = k^{i+1} \circ d_A^i - d_B^{i-1} \circ k^i$.

Definition 3.6.14. Functors in an abelian category: A covariant functor $F : \mathfrak{U} \longrightarrow \mathfrak{B}$ from one abelian category to another is *additive* if for any two objects $A, A' \in \operatorname{Ob} \mathfrak{U}$, the induced map $\operatorname{Hom}(A, A') \longrightarrow \operatorname{Hom}(FA, FA')$ is a homomorphism of abelian groups. F is *left exact* if it is additive and for every short exact sequence

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

in $\mathfrak{U}$, the sequence

$$0 \longrightarrow FA' \longrightarrow FA \longrightarrow F''$$

is exact in $\mathfrak{B}$. Similarly we can define *right exact*.

Definition 3.6.15. Injective Resolution: A resolution of an object A of $\mathfrak{U}$ is a complex $I^{\cdot}$, defined in degrees $i \geq 0$, together with an injective morphism $\epsilon : A \longrightarrow I^0$, such that I^i is a object of $\mathfrak{U}$ for each $i \geq 0$, and such the sequence

$$0 \longrightarrow A \xrightarrow{\epsilon} I^0 \longrightarrow I^1 \longrightarrow \cdots$$

is exact. If I^i is injective object of $\mathfrak{U}$ $\forall i \geq 0$, then the resolution is called injective resolution.

Definition 3.6.16. Sufficiently many injective objects: An abelian category $\mathfrak{U}$ is said to have sufficiently many injectives if for each $A \in \operatorname{Ob} \mathfrak{U}$, there exists an injective object I and a morphism $j : A \longrightarrow I$ which is injective.

Theorem 3.6.17. *If $\mathfrak{U}$ has sufficiently many injectives, then every object has an injective resolution.*

Proof. Let A be an object in $\mathfrak{U}$. As $\mathfrak{U}$ has sufficiently many injective objects, there exists an injective object I^0 with injective morphism $j : A \longrightarrow I^0$. Suppose that we have the following sequence

$$0 \longrightarrow A \xrightarrow{j} I^0 \xrightarrow{d^0} I^1 \longrightarrow \cdots \xrightarrow{d^{k-1}} I^k$$

Now we can find an injective object I^{k+1} such that $\operatorname{coker} d^{k-1} \longrightarrow I^{k+1}$ is injective. And using this injective map we can extend the above exact sequence as follows

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "j"] & I^0 \arrow[r, "d^0"] & I^1 \arrow[r] & \cdots \arrow[r, "d^{k-1}"] & I^k \arrow[r, dotted, "d^k"] \arrow[d] & I^{k+1} \\
 & & & & & \operatorname{coker} d^{k-1} \arrow[ur] &
\end{tikzcd}$$

and here $d^k \circ d^{k-1} = 0$ $\square$

Theorem 3.6.18. *Let* $I^\cdot$, $i : A \hookrightarrow I^0$ *be a resolution of* A *and let* $J^\cdot$, $j : B \hookrightarrow J^0$ *be a resolution of* B *and let* $\phi : A \longrightarrow B$ *be a morphism. Then if the second resolution is injective, there exists a morphism of complexes* $\phi^\cdot : I^\cdot \longrightarrow J^\cdot$ *satisfying* $\phi^0 \circ i = j \circ \phi$. *Moreover if we have two such morphisms* $\phi^\cdot$ *and* $\psi^\cdot$, *there exists a homotopy* $H^\cdot$ *between* $\phi^\cdot$ *and* $\psi^\cdot$. $\square$

Chapter 4

Curves

4.1 Riemann-Roch Theorem

In this section we will assume *the Serre duality theorem*, and then state *the Riemann-Roch theorem.*

Theorem 4.1.1. *The Serre Duality Theorem. Let X be a projective variety of dimension n over algebraically closed field k, and let $\Omega_{X/k}$ be the canonical sheaf, then there exists a natural homomorphism*

$$H^i(X, \mathcal{F}) \longrightarrow H^{i-1}(X, \mathcal{F}^\vee \otimes \Omega_{X/k})$$

Here $\mathcal{F}^\vee$ is the dual of sheaf $\mathcal{F}$.

Let X be non-singular, projective and complete curve. Note that now as X has dimension 1, then the sheaf of relative differentials of X over k, $\Omega_{X/k}$ it is an invertible sheaf. Now let K be divisor such that line bundle corresponding to K is $\Omega_{X/k}$. If D is a divisor, then

$$l(D) = \dim_k \Gamma(X, \mathcal{O}_X(D))$$

which is a positive integer.

Theorem 4.1.2. *Riemann Roch. Let X be a projective curve of genus g and let D be a divisor on X, then*

$$l(D) - l(K - D) = deg\, D + 1 - g$$

□

The 'Riemann-Roch' theorem enables us to solve 'Riemann-Roch' problem for a divisor D on a curve on a curve X. Let D be a divisor on curve X. Then for any $n > 0$ consider the complete linear system $|nD|$. Then the 'Riemann-Roch' problem is to determine $\dim |nD|$ as a function of n and it's behavior as $n \gg 0$.

Thus according to 'Riemann-Roch' theorem it follows that: If $\deg D < 0$, then $|nD|$ is empty for all $n > 0$. If $\deg D = 0$, then if nD is linearly equivalent to 0, then $\dim |nD| = 1$, otherwise $|nD|$ is empty. And for the last case, if $\deg D > 0$, then if $n.\deg\ D > \deg\ K$, then we will have $l(K - nD) = 0$, and thus for $n \gg 0$ we will have

$$\dim |nD| = n.\deg D - g.$$

Bibliography

[Hartshorne 1977] HARTSHORNE, R.: *Algebraic Geometry*. Springer, 1977 (Graduate Texts in Mathematics). – URL https://books.google.co.in/books?id=3rtX9t-nnvwC. – ISBN 9780387902449

[Macdonald 2007] MACDONALD, M.F.A.A.I.G.: *Introduction To Commutative Algebra*. Sarat Book House, 2007. – URL https://books.google.co.in/books?id=fCXnSD9KGUcC. – ISBN 9788187169871

[Matsumura und Reid 1989] MATSUMURA, H. ; REID, M.: *Commutative Ring Theory*. Cambridge University Press, 1989 (Cambridge Studies in Advanced Mathematics). – URL https://books.google.co.in/books?id=yJwNrABugDEC. – ISBN 9780521367646

[Reid 1995] REID, M.: *Undergraduate Commutative Algebra*. Cambridge University Press, 1995 (London Mathematical Society Student Texts). – URL https://books.google.co.in/books?id=mUL1us0mRrAC. – ISBN 9780521458894

[Stacks Project Authors 2016] STACKS PROJECT AUTHORS, The: *Stacks Project*. http://stacks.math.columbia.edu. 2016

[Voisin und Schneps 2002] VOISIN, C. ; SCHNEPS, L.: *Hodge Theory and Complex Algebraic Geometry I:*. Cambridge University Press, 2002 (Cambridge Studies in Advanced Mathematics v. 1). – URL https://books.google.co.in/books?id=dAHEXVcmDWYC. – ISBN 9781139437691