National Institute of Science Education and Research

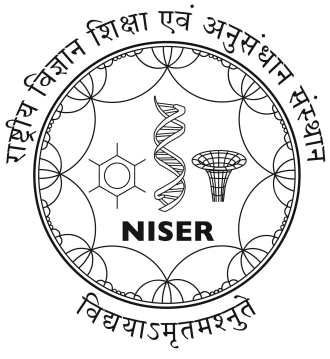
School of Mathematical Sciences

M499: Project-II

# Arithmetic Geometry - II

*Author*
Gaurish Korpal
1411040
gaurish.korpal@niser.ac.in

*Supervisor*
Prof. Brundaban Sahu
Associate Professor
brundaban.sahu@niser.ac.in




April 20, 2018

# Plagiarism statement

I declare that this report is my own work, except where acknowledged, and has not been submitted for academic credit elsewhere.

I acknowledge that the assessor of this report may, for the purpose of assessing it:

- Reproduce it and provide a copy to another member of the Institute; and/or,
- Communicate a copy of it to a plagiarism checking service (which may then retain a copy of it on its database for the purpose of future plagiarism checking).

I certify that I have read and understood the Institute Rules in respect of Student Academic Misconduct[1], and am aware of any potential plagiarism penalties which may apply.

By signing this declaration I am agreeing to the statements and conditions above.

Signed: _____ Date: _____

[1] Disciplinary Rules for Students: http://www.niser.ac.in/notices/2010/Disciplinary%20Rules%20for%20Students.pdf

**Abstract**

In this report we discuss 3 key ideas. Firstly, a generalization of the result used for factorization of prime ideals in number field extensions to any Dedekind domain extension satisfying a very mild condition. Secondly, determining the prime ideals of $\mathbb{Z}[x]$ using geometry. Thirdly, illustrating the application of normalization process to determine the dimension of polynomial ring.

**Acknowledgements**

This report would not have existed in this neat-to-read form without the access to following awesome typesetting tools. I would like to thank the people who created these tools and made them available for free for everyone.

- Donald Knuth for TEX
- Michael Spivak for $\mathcal{AMS}$-TEX
- Sebastian Rahtz for TEX Live
- Leslie Lamport for LATEX
- American Mathematical Society for $\mathcal{AMS}$-LATEX
- Hàn Thê Thành for pdfTEX
  - Heiko Oberdiek for `hyperref` package
  - Steven B. Segletes for `stackengine` package
  - Alan Jeffrey & Frank Mittelbach for `inputenc` package
  - David Carlisle for `graphicx` package
  - Javier Bezos for `enumitem` package
  - Hideo Umeki for `geometry` package
  - Sebastian Rahtz for `textcomp` package
  - Walter Schmidt for `gensymb` package
  - Patrick W. Daly for `natbib` package
- Philipp Kühl & Daniel Kirsch for Detexify (a tool for searching LATEX symbols)
- TeX.StackExchange community for helping me out with LATEX related problems

# Contents

# Introduction

*Arithmetic geometry* can be defined as the part of algebraic geometry connected with the study of algebraic varieties over arbitrary rings, in particular over non-algebraically closed fields. The central problem is to study the solutions in $R^n$ of a system of polynomial equations in $n$ variables with coefficients in a ring $R$ (such as $R = \mathbb{Z}$, $R = \mathbb{Q}$, or $R = \mathbb{Z}/p\mathbb{Z}$). Hence it lies at the intersection between algebraic geometry and number theory.

In the first chapter a generalization of the result used for factorization of prime ideals in number field extensions to any Dedekind domain extension, satisfying a very mild condition, has been discussed. The books by Marcus [Mar77], and Lorenzini [Lor96] were the main references for this chapter.

In the second chapter two main concepts has been discussed. Firstly, determining the prime ideals of $\mathbb{Z}[x]$ using geometry. Secondly, illustrating the application of normalization process to determine the dimension of polynomial ring. Moreover, in the previous report [Kor17] I used two important theorems, namely Noether normalization lemma (that lead to the conclusion that $\dim(K[x_1, \ldots, x_n]) = n$) and Riemann–Roch theorem (while defining genus of algebraic curve) without knowledge of their proofs. In the second chapter, we will see the proof of the former. The books by Liu [Liu02], Eisenbud [Eis04], and Reid [Rei95] were the main references for this chapter.

This report is the second step towards my preparation for the master's thesis to be submitted in May, 2019. Before submitting the final thesis I am expected to write four reports on arithmetic geometry, one each semester, and this is the second one in that series of four reports.

# Chapter 1

# Dedekind domain

We ended the first chapter of our previous report with the definition of Dedekind domain [Kor17, Definition 1.15]. In this chapter we will study some general properties of Dedekind domains. Let's first recall the definition:

**Definition** (Dedekind domain)**.** A Noetherian, integrally closed integral domain in which every non-zero prime ideal is maximal is called a *Dedekind domain.*

## 1.1 Factorization

We know that the rings of algebraic integers do not always have unique factorization property. But since every ring of algebraic integers happens to be a Dedekind domain, every proper ideal admits a unique factorization as a product of prime ideals [Kor16, Remark 12]. In this section we will prove this unique factorization property of Dedekind domains. Though one can deduce this from the general primary decomposition theorems [AM07, Corollary 9.4], we will discuss the direct proof using elementary tools [Mar77, Theorem 16].

**Lemma 1.1.** *In a Dedekind domain $R$ every ideal contains a product of prime ideals.*

*Proof.* On the contrary, assume that there is a non-empty set $\mathcal{A}$ of ideals in $R$ which do not contain any product of prime ideals. Since $R$ is Noetherian, $\mathcal{A}$ has a maximal element $\mathfrak{m}$ [Kor17, Theorem 1.3]. Also, $\mathfrak{m}$ is certainly not prime since $\mathcal{A}$ doesn't contain a product of prime ideals. Hence there exists $r, s \in R\backslash\mathfrak{m}$ such that $rs \in \mathfrak{m}$. Since $\mathfrak{m} + \langle r\rangle$ and $\mathfrak{m} + \langle s\rangle$ are strictly bigger than $\mathfrak{m}$, they must contain a product of prime ideals. But $(\mathfrak{m}+\langle r\rangle)(\mathfrak{m}+\langle s\rangle) \subseteq \mathfrak{m}$, contradicting the fact that $\mathfrak{m}$ didn't contain any product of prime ideals. Hence the set $\mathcal{A}$ is empty, completing the proof. □

**Lemma 1.2.** *Let $\mathfrak{a}$ be a proper ideal in a Dedekind domain $R$ with field of fractions $K$. Then there exists $r \in K\backslash R$ such that $r\mathfrak{a} \subseteq R$.*

*Proof.* Let $a \in \mathfrak{a}$, $a \neq 0$. By Lemma 1.1, $\langle a\rangle$ contains a product of prime ideals, say $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell$ such that $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell \subseteq \langle a\rangle$ and $\ell$ is minimal. Since $R$ is a commutative ring with identity, every proper ideal is contained in a maximal ideal [DF11, Proposition 7.11], let that ideal be $\mathfrak{p}$. Hence we have

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell \subseteq \langle a\rangle \subseteq \mathfrak{a} \subseteq \mathfrak{p}$$

We note that $\mathfrak{p}$ contains a prime ideal $\mathfrak{p}_i$ for some $i$. Since if not, then there exists $a_j \in \mathfrak{p}_j\backslash\mathfrak{p}$ for all $j = 1, \ldots, \ell$ such that $a_1\cdots a_\ell \in \mathfrak{p}$ which will contradict the fact that $\mathfrak{p}$ is a prime ideal. Also since $R$ is a Dedekind domain, every non-zero prime ideal is maximal, i.e. $\mathfrak{p}_i \subset \mathfrak{p}$ implies that $\mathfrak{p}_i = \mathfrak{p}$. Without loss of generality, let $i = 1$. Hence we have

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell \subseteq \langle a\rangle \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1$$

Also by the minimality of $\ell$, there exists $b \in (\mathfrak{p}_2 \cdots \mathfrak{p}_\ell) \backslash \langle a \rangle$. Hence we have found an element $\frac{b}{a} \in K \backslash R$. We observe that since $a \in \mathfrak{p}_1$

$$\frac{b}{a}\ \mathfrak{a} \subseteq \frac{b}{a}\ \mathfrak{p}_1 \subseteq R$$

Hence we have found $r = \frac{b}{a}$, completing the proof. □

**Remark 1.1.** The ideal $\mathfrak{f} = r\mathfrak{a}$ is called *fractional ideal* of the field of fractions $K$ [Kor16, Definition 18].

**Proposition 1.1.** *Let $\mathfrak{a}$ be an ideal in a Dedekind domain $R$. Then there is an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is a principal ideal.*

*Proof.* Fix $a \in \mathfrak{a}$, $a \neq 0$. We claim that $\mathfrak{b} = \{b \in R : b\mathfrak{a} \subseteq \langle a \rangle\}$. We will divide the proof into two steps:

Step 1. *$\mathfrak{b}$ in an ideal in $R$.*

Since $a \in \mathfrak{b}$, $\mathfrak{b} \neq 0$. It's easy to check that $\mathfrak{b}$ is a subgroup of $R$ under addition operation. Finally we note that $rb \in \mathfrak{b}$ for all $r \in R$ and $b \in \mathfrak{b}$. Hence $\mathfrak{b}$ is an ideal in $R$.

Step 2. $\mathfrak{ab} = \langle a \rangle$

Consider the set $\mathfrak{f} = \frac{1}{a}\ \mathfrak{ab}$. Since $\mathfrak{ab} \subseteq \langle a \rangle$, we have $\mathfrak{f} \subseteq R$. Moreover, $\mathfrak{f}$ is an ideal in $R$. Hence it's sufficient to prove that $\mathfrak{f} = R$. On the contrary, let $\mathfrak{f} \subsetneq R$. Then by Lemma 1.2 there exists $r \in K \backslash R$ such that $r\mathfrak{f} \subseteq R$. Since $\mathfrak{b} \subseteq \mathfrak{f}$, we have

$$r\mathfrak{b} \subseteq r\mathfrak{f} \subseteq R$$

From this we conclude that $r\mathfrak{b} \subseteq \mathfrak{b}$, since given any $b \in \mathfrak{b}$ we have $rb \in \mathfrak{b}$ as follows

$$rb \in r\mathfrak{b} \Rightarrow rb \in R \quad \text{and} \quad \frac{r}{a}\ \mathfrak{ab} \subseteq R \Rightarrow rb\mathfrak{a} \subseteq aR = \langle a \rangle$$

Now $R$ is Noetherian since it's a Dedekind domain, hence $\mathfrak{b}$ is finitely generated. Say $\mathfrak{b} = \langle b_1, \ldots, b_m \rangle$, then $r\mathfrak{b} \subseteq \mathfrak{b}$ implies that $rb_i$ for all $i = 1, \ldots, m$ is a linear combination of $b_1, \ldots, b_m$ with coefficients in $R$. Hence we have

$$r \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = M \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \quad \Longrightarrow (rI - M) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = 0$$

for some $m \times m$ matrix $M$ and identity matrix $I$. Hence $\det(rI - M) = 0$, giving us a monic polynomial in $R[X]$ of degree $m$ whose root is $r$. But $R$ is integrally closed since it's a Dedekind domain, hence $r \in R$. This contradicts the assumption that $r \notin R$, hence completing the proof.

□

**Remark 1.2.** Hence we can say that ideal classes in a Dedekind domain form a group with the class of principal ideals being the identity element [Kor16, Theorem 33].

**Corollary 1.1.** *If $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ are ideals in a Dedekind domain $R$, and $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_3$ then $\mathfrak{a}_2 = \mathfrak{a}_3$.*

*Proof.* By the above proposition there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ba}_1 = \langle a \rangle$ for some $a \in \mathfrak{a}_1$. Then we have

$$\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_3 \Rightarrow \mathfrak{ba}_1\mathfrak{a}_2 = \mathfrak{ba}_1\mathfrak{a}_3 \Rightarrow a\mathfrak{a}_2 = a\mathfrak{a}_3 \Rightarrow \mathfrak{a}_2 = \mathfrak{a}_3$$

since $a \neq 0$ and $R$ is an integral domain. □

**Corollary 1.2.** *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a Dedekind domain $R$, then $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.*

*Proof.* ($\Rightarrow$) By definition, $\mathfrak{a} \mid \mathfrak{b}$ implies that there exists an ideal $\mathfrak{f}$ such that $\mathfrak{af} = \mathfrak{b}$. Hence $\mathfrak{b} \subseteq \mathfrak{a}$ trivially.

($\Leftarrow$) By the above proposition there exists an ideal $\mathfrak{c}$ such that $\mathfrak{ca} = \langle a \rangle$ for some non-zero $a \in \mathfrak{a}$. Then $\mathfrak{b} \subseteq \mathfrak{a}$ implies that $\mathfrak{cb} \subseteq \langle a \rangle$. Hence we have an ideal $\mathfrak{f} = \frac{1}{a}\,\mathfrak{cb}$ of $R$ such that $\mathfrak{af} = \mathfrak{b}$. Thus $\mathfrak{a} \mid \mathfrak{b}$. □

**Theorem 1.1.** *Every proper ideal in a Dedekind domain $R$ is uniquely representable as a product of prime ideals.*

*Proof.* We will prove the existence and uniqueness of factorization in two steps.

Step 1. *Every proper ideal is representable as a product of prime ideals.*

On the contrary, assume that there is a non-empty set $\mathcal{A}$ of ideals in $R$ which are not representable as a product of prime ideals. Since $R$ is Noetherian, $\mathcal{A}$ has a maximal element $\mathfrak{m}$ [Kor17, Theorem 1.3] such that $\mathfrak{m} \neq R$ since it's a proper ideal. Since $R$ is a commutative ring with identity, every proper ideal is contained in a maximal ideal [DF11, Proposition 7.11], let that ideal be $\mathfrak{p}$. Then by Corollary 1.2 we have $\mathfrak{m} = \mathfrak{pa}$ for some ideal $\mathfrak{a}$. Then $\mathfrak{m} \subseteq \mathfrak{a}$. But since prime ideals are proper ideal, $\mathfrak{p} \neq R$ implies that $\mathfrak{m} \neq \mathfrak{a}$. Hence we have the strict containment $\mathfrak{m} \subsetneq \mathfrak{a}$. This implies that $\mathfrak{a} \notin \mathcal{A}$ and hence can be represented as product of prime ideals. But then $\mathfrak{m}$ is also representable as product of prime ideals, contradicting our assumption and completing the proof.

Step 2. *The representation is unique.*

Suppose that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are non-zero prime ideals not necessarily distinct. Then we have

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subseteq \mathfrak{q}_1$$

which implies that $\mathfrak{p}_i \subseteq \mathfrak{q}_1$ for some $i$. Rearranging the $p_i$'s if necessary, we can assume that $p_1 \subseteq q_1$. Since all non-zero prime ideals are maximal ideals in $R$, $p_1 = q_1$. Now by Corollary 1.1, we get

$$\mathfrak{p}_2 \cdots \mathfrak{p}_m = \mathfrak{q}_2 \ldots \mathfrak{q}_n$$

Continuing this way we eventually find that $m = n$ and $p_i = q_i$ for all $i$ (after rearrangement).

□

**Proposition 1.2.** *A Dedekind domain $R$ is a unique factorization domain if and only if it is a principal ideal domain.*

*Proof.* ($\Rightarrow$) Let $\mathfrak{a}$ be an ideal of $R$, then by Proposition 1.1 $\mathfrak{a}$ divides some principal ideal $\langle a \rangle$. Since $R$ is a unique factorization domain, $a$ is a product of prime elements in $R$, say $a = p_1 \cdots p_\ell$. Also, in unique factorization domain prime elements and irreducible elements are same ([DF11, Proposition 8.12]) we conclude that $\mathfrak{a}$ divides a product of principal prime ideals

$$\mathfrak{a} \mid \langle p_1 \rangle \langle p_2 \rangle \cdots \langle p_\ell \rangle$$

Then by Theorem 1.1 it follows that $\mathfrak{a}$ itself is a product of principal prime ideals and therefore a principal ideal.

($\Leftarrow$) This is always true since every principal ideal domain is a unique factorization domain [DF11, Theorem 8.14]. □

**Remark 1.3.** The above proposition is equivalent to Theorem 1.8 of previous report [Kor17] since every unique factorization domain is integrally closed. In that proof, the crucial fact we used was that every prime ideal of a unique factorization domain of dimension 1 is principal. Then it was sufficient to prove that unique factorization domain of dimension 1 is a Bézout domain, which was proved using induction.

**Example 1.1.** We know that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain [Kor15, Theorem 1.7.8], but is not a unique factorization domain since

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

gives two distinct factorizations of 6 into irreducibles [DF11, Propostion 8.11]. We can also directly see that it is not a principal ideal domain since $\mathfrak{a} = \langle 3, 2 + \sqrt{-5} \rangle$ is not a principal ideal [DF11, Example 2, pp. 273]. It is known, but not easy to prove, that $d = -1, -2, -3, -7, -11, -19, -43, -67$ and $-163$ are the only negative values of $d$ for which the ring of integers of $\mathbb{Q}(\sqrt{d})$ is a principal ideal domain [Kor15, Theorem 1.7.9].

## 1.2 Localization

The technique of localization reduces many problems in commutative algebra to problems about local rings. This often turns out to be extremely useful since most of the problems with which commutative algebra has been successful are those that can be reduced to the local case [Eis04, pp. 57]. We will prove an equivalent definition of Dedekind domain in terms of localization at prime ideals [Liu02, Corollary 1.2.14].

**Theorem 1.2.** *A Dedekind domain is a Noetherian integral domain $R$ whose localizations $R_\mathfrak{p}$ at the non-zero prime ideals $\mathfrak{p}$ are principal ideal domains, but not a field*[1].

*Proof.* Given a Noetherian domain $R$, we know that $\dim R = 0$ if and only if $R$ is a field. Hence it is sufficient to prove the equivalence of the following two statements:

(i) For every non-zero prime ideal $\mathfrak{p}$ in $R$ the local ring $R_\mathfrak{p}$ is a principal ideal domain with non-zero maximal ideal.

(ii) The ring $R$ is integrally closed and has dimension 1.

$\boxed{(i) \Rightarrow (ii)}$ We know that the prime ideals of $R_\mathfrak{p}$ are in one-to-one correspondence with the prime ideals of $R$ contained in $\mathfrak{p}$ [AM07, Corollary 3.13]. Hence every chain of prime ideals ending with prime ideal $\mathfrak{p}$ extends to a corresponding chain of same length in $R_\mathfrak{p}$. Thus we have

$$\dim R = \sup\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec} R\} = \sup\{\dim R_\mathfrak{p} : \mathfrak{p} \in \operatorname{Spec} R\} = 1$$

since every principal ideal domain has dimension 1 [Kor17, Lemma 1.4]. Moreover, if $K$ is the field of fractions[2] of $R$, then $K$ is also field of fractions of $R_\mathfrak{p}$ since $R_\mathfrak{p} \subsetneq K$. Also, any element $r \in K$ that is integral over $R$, is also integral over $R_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$ [AM07, Proposition 5.6]. But $R_\mathfrak{p}$ is integrally closed since it is a principal ideal domain [Kor17, Proposition 1.2], hence $r \in \cap_\mathfrak{p} R_\mathfrak{p} = R$ where $\mathfrak{p}$ are all non-zero prime ideals in $R$. Hence $R$ is integrally closed.

$\boxed{(ii) \Rightarrow (i)}$ Since localization preserves the property of $R$ being a Noetherian domain, $R_\mathfrak{p}$ is also a Noetherian domain [AM07, Corollary 7.4] . Also, integral closure is a local property[3],

[1] As in §1.3 of previous report [Kor17], fields are not considered principal ideal domains.
[2] It is the smallest field with respect to the inclusion that contains $R$.
[3] Normalization commutes with localization [Eis04, Proposition 4.13].

hence $R_\mathfrak{p}$ is integrally closed for each prime ideal $\mathfrak{p}$ [AM07, Proposition 5.12]. Moreover, every chain of prime ideals in $R_\mathfrak{p}$ contracts to a chain of at least that length in $R$. Thus we have

$$\dim R_\mathfrak{p} = \sup\{\mathrm{ht}(\mathfrak{q}) : \mathfrak{q} \in \mathrm{Spec}(R_\mathfrak{p})\} = \sup\{\mathrm{ht}(\mathfrak{q}) : \mathfrak{q} \cap R \subseteq \mathfrak{p}\} \leq \dim R = 1$$

Since $R$ is an integral domain, $\dim R_\mathfrak{p} = 0$ if and only if $R$ is a field, i.e. $\dim R = 0$. But we know that $\dim R \neq 0$, hence $\dim R_p = 1$. Hence $R_\mathfrak{p}$ is an integrally closed Noetherian local domain of dimension 1, which is equivalent to saying that $R_\mathfrak{p}$ is a principal ideal domain with non-zero maximal ideal [AM07, Proposition 9.2, (ii)⇔(iii)]. □

## 1.3 Extension

**Lemma 1.3.** *Let $R$ be a Dedekind domain with field of fractions $K$ and $L$ be a finite extension of $K$. If $S$ is the integral closure of $R$ in $L$ then $\mathfrak{p}S \neq S$ for any prime ideal $\mathfrak{p}$ in $R$.*

*Proof.* We will divide the proof into two steps:

Step 1. If $\mathfrak{p} = \langle a \rangle$ is a principal ideal.

On the contrary, let $\mathfrak{p}S = S$. Then there exists $b \in S$ such that $ab = 1$. Also, $b \notin R$ since if not then $\mathfrak{p} = R$ which will be absurd since prime ideals are proper ideals. Since $b$ is an integral element over $R$, there exists a minimal monic polynomial $f(x) \in R[x]$ of degree $n$ such that $f(b) = 0$, that is

$$b^n + r_{n-1}b^{n-1} + \cdots + r_0 = 0$$

But since $ab = 1$, we have

$$b^{n-1} + r_{n-1}b^{n-2} + \cdots + ar_0 = 0$$

Hence we have found an integral relation of $b$ over $R$ of degree less than $n$, contradicting the minimality of $n$. Hence such a $b$ does not exist and $\mathfrak{p}S \neq S$.

Step 2. If $\mathfrak{p}$ is any non-zero prime ideal in $R$.

Let $D = R \backslash \mathfrak{p}$ be the multiplicatively closed subset of $R$. Then we have $D^{-1}\mathfrak{p} = \mathfrak{q}$ a prime ideal in $R_\mathfrak{p}$ [AM07, Corollary 3.13]. Also, $D^{-1}S = S_\mathfrak{p}$ is localization of $S$. Then $\mathfrak{p}S \neq S$ if and only if $\mathfrak{q}S_\mathfrak{p} \neq S_\mathfrak{p}$ [AM07, Proposition 3.8]. But since $R_\mathfrak{p}$ is a principal ideal domain by Theorem 1.2, $\mathfrak{q}$ is a principal ideal. Hence $\mathfrak{q}S_\mathfrak{p} \neq S_\mathfrak{p}$ as in the previous step.

□

**Remark 1.4.** Even more is true in the above setting. Krull-Akizuki theorem implies that $S$ is in fact a Dedekind domain [Neu99, Proposition I.12.8]. But we will work on a bit less general setting avoiding the use of more advanced tools from algebra [Lor96, §III.3].

**Proposition 1.3.** *Let $R$ be a Dedekind domain with field of fractions $K$ and $S$ be the integral closure of $R$ in a finite extension $L$ of $K$. Then $S$ is a Dedekind domain if $S$ is a finitely generated $R$-module*

*Proof.* Since $R$ is Noetherian and $S$ is finitely generated $R$-module, $S$ is also Noetherian [Kor17, Corollary 1.5]. Also, since $\dim R = 1$ and $L$ over $K$ is a finite extension, $\dim S = 1$ [Kor17, Corollary 1.6]. Moreover, it is given that $S$ is integrally closed in its field of fractions $L$. Hence $S$ is a Dedekind domain. □

**Lemma 1.4.** *Let $\mathfrak{p}$ be a prime ideal in a Dedekind domain $R$ with field of fractions $K$ and $\mathfrak{q}$ be a prime ideal in the integral closure $S$ of $R$ in a finite extension $L$ of $K$. If $S$ is a finitely generated $R$-module then the following are equivalent:*

*(i)* $\mathfrak{q} \mid \mathfrak{p}S$

*(ii)* $\mathfrak{p}S \subseteq \mathfrak{q}$

*(iii)* $\mathfrak{p} \subseteq \mathfrak{q}$

*(iv)* $\mathfrak{p} = \mathfrak{q} \cap R$

*(v)* $\mathfrak{p} = \mathfrak{q} \cap K$

*where* $\mathfrak{p}S$ *is the extension of* $\mathfrak{p}$ *in* $S$ *under the natural inclusion ring homomorphism.*

*Proof.* By Proposition 1.3 we know that $S$ is a Dedekind domain, hence we can apply Corollary 1.2 to get $(i) \Leftrightarrow (ii)$. Also, $(ii) \Leftrightarrow (iii)$ trivially since $\mathfrak{q}$ is an ideal in $S$. And, $(iv) \Leftrightarrow (v)$ since $R = S \cap K$ and $\mathfrak{q} \subseteq S$. We just need to show that $(iii) \Rightarrow (iv)$, since $(iv) \Rightarrow (iii)$ is trivial. Now for $(iii) \Rightarrow (iv)$, we know that $\mathfrak{p} \subseteq \mathfrak{q} \cap R$ and $\mathfrak{q} \cap R$ is a prime ideal of $R$ [AM07, pp. 9]. Since $R$ is a Dedekind domain, $\mathfrak{p}$ and $\mathfrak{q} \cap R$ are maximal ideals, hence must be equal. □

**Remark 1.5.** This lemma clearly illustrates the fact that extension of a prime ideal need not be a prime ideal [AM07, pp. 10]. In fact, the prime ideals $\mathfrak{q}$'s lying over a given prime ideal $\mathfrak{p}$ are the ones which occur in the prime decomposition of $\mathfrak{p}S$ [Kor16, Definition 14]. Also, by Lemma 1.3 we can conclude that every prime ideal $\mathfrak{p}$ of $R$ lies under at least one prime $\mathfrak{q}$ of $S$ [Mar77, Theorem 20].

**Definition 1.1** (Ramification index)**.** Let $R$ be a Dedekind domain with field of fractions $K$ and $L$ be a finite extension of $K$. Let $S$ be a Dedekind domain which is the integral closure of $R$ in $L$. The exponent with which the prime ideal $\mathfrak{q}$ in $S$ lying over a given non-zero prime ideal $\mathfrak{p}$ in $R$ occur in the prime decomposition of $\mathfrak{p}S$ is called its ramification index. For example, if $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_\ell^{e_\ell}$ then $e_i$ is the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $e(\mathfrak{q}_i/\mathfrak{p})$.

**Remark 1.6.** Due to unique factorization of prime ideals in the Dedekind domain $S$, the value of $e(\mathfrak{q}/\mathfrak{p})$ is unique and hence well defined.

**Definition 1.2** (Residual degree)**.** Let $R$ be a Dedekind domain with field of fractions $K$ and $L$ be a finite extension of $K$. Let $S$ be a Dedekind domain which is the integral closure of $R$ in $L$ and $\mathfrak{q}$ be a prime ideal in $S$ lying over non-zero prime ideal $\mathfrak{p}$ in $R$. Then $R/\mathfrak{p}$ is the residual field of $R$ at $\mathfrak{p}$ and $S/\mathfrak{q}$ is the residual field of $S$ at $\mathfrak{q}$. We define the degree of field extension of $S/\mathfrak{q}$ over $R/\mathfrak{p}$ as the residual degree of $\mathfrak{q}$ over $\mathfrak{p}$. For example, if $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_\ell^{e_\ell}$ then $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}]$ is the residual degree of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $f(\mathfrak{q}_i/\mathfrak{p})$.

**Remark 1.7.** We have the following ring homomorphism

$$\begin{aligned} \psi : R &\hookrightarrow S \to S/\mathfrak{q} \\ x &\mapsto x \mapsto x + \mathfrak{q} \end{aligned}$$

with $\ker \psi = \mathfrak{q} \cap R = \mathfrak{p}$ by Lemma 1.4. Hence we have the embedding

$$\varphi : R/\mathfrak{p} \hookrightarrow S/\mathfrak{q}$$

Moreover, since $S$ is finitely generated $R$-module [Kor17, Theorem 1.6] and $\mathfrak{p} \subseteq \mathfrak{q}$ i.e. $S/\mathfrak{q}$ is annihilated by $\mathfrak{p}$ [DF11, Example 5, pp. 338], we conclude that $S/\mathfrak{q}$ is a finite dimensional $R/\mathfrak{p}$-vector space.

**Theorem 1.3.** *Let* $R$ *be a Dedekind domain with field of fractions* $K$ *and* $S$ *be the integral closure of* $R$ *in a finite extension* $L$ *of* $K$*. If* $S$ *is a finitely generated* $R$*-module then*

$$[L : K] = \sum_{\mathfrak{q} \mid \mathfrak{p}S} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p})$$

*for any non-zero prime ideal* $\mathfrak{p}$ *of* $R$*.*

*Proof.* We will divide our proof into three steps:

Step 1. *Proving the theorem when $R$ and $S$ are principal ideal domains*

By Proposition 1.3 we know that $S$ is a Dedekind domain, hence by Theorem 1.1 we have

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_\ell^{e_\ell} \tag{1.1}$$

for some prime ideals $\mathfrak{q}_i$'s of $S$. Since $q_i$'s are pairwise co-prime ideals in $S$, by Chinese Remainder Theorem [DF11, Theorem 7.6.17] we have

$$S/\mathfrak{p}S \cong S/\mathfrak{q}_1^{e_1} \oplus \cdots \oplus S/\mathfrak{q}_\ell^{e_\ell} \tag{1.2}$$

as rings and also as $R/\mathfrak{p}$-vector spaces since $\mathfrak{p} \subseteq \mathfrak{p}S \subseteq \mathfrak{q}_i^{e_i}$ for all $i = 1, \ldots, \ell$ (as seen in Remark 1.7). Hence we have to show that

$$[L : K] = \sum_{i=1}^{\ell} e_i f_i \tag{1.3}$$

where $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}] = \dim_{R/\mathfrak{p}} S/\mathfrak{q}_i$. Till now we didn't use the fact that $R$ and $S$ are principal ideal domains.

Claim 1. $\dim_{R/\mathfrak{p}} S/\mathfrak{p}S = [L : K]$

Since $R$ is a principal ideal domain and $S$ is a finitely generated $R$-module (under the ring multiplication action), by Structure theorem [Kor17, Proposition 1.7] we know that

$$S \cong R^n \oplus \mathrm{Tor}(S)$$

for some $n \geq 0$ (called rank of $S$ over $R$) and

$$\mathrm{Tor}(S) = \{s \in S : rs = 0 \text{ for some non-zero } r \in R\}$$

Since $S$ is an integral domain, $\mathrm{Tor}(S) = \{0\}$, and hence $S$ is a free $R$-module, i.e. $S \cong R^n$. Since $[L : K]$ is finite and $S$ is integral closure of $R$ in $L$, we conclude that the rank of $S$ over $R$ is equal to $[L : K]$, i.e. $[L : K] = n$ [Kor17, Lemma 1.3].
Since by Lemma 1.4 we know that $R \cap \mathfrak{p}S = \mathfrak{p}$, we have a $R$-module isomorphism[4]

$$S/\mathfrak{p}S \cong (R \oplus \cdots \oplus R)/(\mathfrak{p}R \oplus \cdots \oplus \mathfrak{p}R) = R^n/\mathfrak{p}R^n \tag{1.4}$$

Moreover we have [DF11, Exercise 10.2.12]

$$R^n/\mathfrak{p}R^n \cong R/\mathfrak{p}R \oplus \cdots \oplus R/\mathfrak{p}R = R/\mathfrak{p} \oplus \cdots \oplus R/\mathfrak{p} = (R/\mathfrak{p})^n \tag{1.5}$$

as $R$-modules. But since $\mathfrak{p} \subseteq \mathfrak{p}S$ i.e. $S/\mathfrak{p}S$ is annihilated by $\mathfrak{p}$ [DF11, Example 5, pp. 338], $S/\mathfrak{p}S \cong (R/\mathfrak{p})^n$ as $R/\mathfrak{p}$-vector space (using (1.4) and (1.5)). Hence we have

$$\dim_{R/\mathfrak{p}} S/\mathfrak{p}S = n = [L : K]$$

Claim 2. $\dim_{R/\mathfrak{p}} S/\mathfrak{q}_1^{e_i} = e_i f_i$ *for* $i = 1, \ldots, \ell$.

Without loss of generality, fix $\mathfrak{q}_i = \mathfrak{q}$, $e_i = e$ and $f_i = f = \dim_{R/\mathfrak{p}} S/\mathfrak{q}$. We will prove our claim by induction on $e$. As noted before, $\mathfrak{p} \subseteq \mathfrak{q}^e \subseteq \ldots \subseteq \mathfrak{q}$ and $S/\mathfrak{q}, \ldots, S/\mathfrak{q}^e$ are $R/\mathfrak{p}$-vector spaces. Base case is true since for $e = 1$ we have

$$\dim_{R/\mathfrak{p}} S/\mathfrak{q} = 1 \cdot f$$

[4] This is not always true, since $2\mathbb{Z} \cong 3\mathbb{Z}$ as $\mathbb{Z}$-modules but $\mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/3\mathbb{Z}$ as $\mathbb{Z}$-modules.

Now our induction hypothesis is that

$$\dim_{R/\mathfrak{p}} S/\mathfrak{q}^{e-1} = (e-1)f \tag{1.6}$$

Now we will prove the inductive step. Consider the linear transformation for $R/\mathfrak{p}$-vector spaces

$$\begin{aligned}\varphi : S/\mathfrak{q}^e &\to S/\mathfrak{q}^{e-1} \\ x + \mathfrak{q}^e &\mapsto x + \mathfrak{q}^{e-1}\end{aligned}$$

where $\ker(\varphi) = \mathfrak{q}^{e-1}/\mathfrak{q}^e$. Then by Rank-Nullity Theorem[5] [HK15, Theorem 3.2] we know that

$$\dim_{R/\mathfrak{p}} S/\mathfrak{q}^e = \dim_{R/\mathfrak{p}} S/\mathfrak{q}^{e-1} + \dim_{R/\mathfrak{p}} \mathfrak{q}^{e-1}/\mathfrak{q}^e$$

Then using induction hypothesis (1.6) we get

$$\dim_{R/\mathfrak{p}} S/\mathfrak{q}^e = (e-1)f + \dim_{R/\mathfrak{p}} \mathfrak{q}^{e-1}/\mathfrak{q}^e \tag{1.7}$$

Next we note that since $S$ is a principal ideal domain, $\mathfrak{q} = \langle \beta \rangle$ for some $\beta \in S$ and we have the surjective $S$-module homomorphism

$$\begin{aligned}\psi : S &\hookrightarrow \mathfrak{q}^{e-1}/\mathfrak{q}^e \\ x &\mapsto x\beta^{e-1} + \mathfrak{q}^e\end{aligned}$$

where $\ker(\psi) = \langle \beta \rangle = \mathfrak{q}$. Therefore by first isomorphism theorem we have $S$-module isomorphism

$$S/\mathfrak{q} \cong \mathfrak{q}^{e-1}/\mathfrak{q}^e$$

Since $\mathfrak{q}$ annihilates $\mathfrak{q}^{e-1}/\mathfrak{q}^e$, we have $S/\mathfrak{q} \cong \mathfrak{q}^{e-1}/\mathfrak{q}^e$ as $S/\mathfrak{q}$-vector spaces. Hence we have

$$\dim_{S/\mathfrak{q}} \mathfrak{q}^{e-1}/\mathfrak{q}^e = 1 \tag{1.8}$$

Now we note that we have tower of fields, $R/\mathfrak{p} \hookrightarrow S/\mathfrak{q} \hookrightarrow \mathfrak{q}^{e-1}/\mathfrak{q}^e$, hence we have [DF11, Theorem 13.14]

$$\dim_{R/\mathfrak{p}} \mathfrak{q}^{e-1}/\mathfrak{q}^e = \dim_{R/\mathfrak{p}} S/\mathfrak{q} \cdot \dim_{S/\mathfrak{q}} \mathfrak{q}^{e-1}/\mathfrak{q}^e$$

Now using (1.8) we get

$$\dim_{R/\mathfrak{p}} \mathfrak{q}^{e-1}/\mathfrak{q}^e = f$$

Using this in (1.7) we get the desired result.

Combining the above two claims with (1.2) we get (1.3).

Step 2. *Proving the theorem for the localizations $D^{-1}R$ and $D^{-1}S$ for $D = R\backslash\mathfrak{p}$*

$D = R\backslash\mathfrak{p} \subseteq R \subseteq S$ is a multiplicatively closed subset, hence we can define the ring of fractions of $R$ and $S$ with respect to $D$. Let $D^{-1}R = R_{\mathfrak{p}}$ and $D^{-1}S = S_{\mathfrak{p}}$ be the respective ring of fractions (abuse of notations). Let $\mathfrak{Q}$ and $\mathfrak{P}$ are the extensions of $\mathfrak{q}$ and $\mathfrak{p}$, under the respective ring localization homomorphisms. Since the field of fractions of a ring doesn't change after localization, we wish to prove that

$$[L : K] = \sum_{\mathfrak{Q}|\mathfrak{P}S_{\mathfrak{p}}} e(\mathfrak{Q}/\mathfrak{P}) f(\mathfrak{Q}/\mathfrak{P})$$

[5] This can also be seen as a consequence of Splitting Lemma [DF11, Proposition 10.25]. Since any short exact sequence of vector spaces split, in particular, if $T : V \to W$ is a linear transformation then $V \cong \ker(T) \oplus \mathrm{Im}(T)$ since we have the short exact sequence $0 \to \ker(T) \to V \to V/\ker(T) \to 0$ where $\mathrm{Im}(T) \cong V/\ker(T)$.

By Theorem 1.2 we know that $R_{\mathfrak{p}}$ is a Dedekind domain (integrally closed Noetherian domain of dimension 1) as well as a principal ideal domain (since it is a local ring). To be able to use the previous step, it's sufficient to prove that $S_{\mathfrak{p}}$ is also a Dedekind domain and a principal ideal domain.

Claim 1. *$S_{\mathfrak{p}}$ is a Dedekind domain*

By Proposition 1.3 we know that $S$ is an integrally closed Noetherian domain of dimension 1. Since localization respects integral closure [AM07, Proposition 5.12] and Noetherian condition [AM07, Proposition 7.3], we just need to prove that dimension of $S_{\mathfrak{p}}$ is 1. The prime ideals of $S_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals of $S$ not intersecting $D = R\backslash\mathfrak{p}$. Since $S$ is a Dedekind domain, by (1.1) we know that $q_i$'s are the only primes lying over $\mathfrak{p}$ in $S$. Also, by Lemma 1.4 we know that $\mathfrak{q}_i \cap R = \mathfrak{p}$ for all $i = 1, \dots, \ell$. Hence the only prime ideals $\mathfrak{q}$ of $S$ for which $D \cap \mathfrak{q} = \phi$ are $\mathfrak{q} = \mathfrak{q}_i$ for all $i = 1, \dots, \ell$. Since $\mathfrak{p}$ is non-zero prime ideal, $\ell \geq 1$. Hence $S_{\mathfrak{p}}$ have $\ell$ non-zero prime ideals,

$$\dim S_p \geq 1$$

Moreover, every chain of prime ideals in $S_{\mathfrak{p}}$ contracts to a chain of at least that length in $S$. Thus we have

$$\dim S_{\mathfrak{p}} = \sup\{\mathrm{ht}(\mathfrak{Q}) : \mathfrak{Q} \in \mathrm{Spec}(S_{\mathfrak{p}})\} \leq \dim S = 1$$

Hence $\dim S_p = 1$.

Claim 2. *$S_{\mathfrak{p}}$ is a principal ideal domain*

From previous claim we conclude that $S_{\mathfrak{p}}$ is an integral domain of dimension 1 that has property of unique factorization of ideals by Theorem 1.1. Also, the set of non-zero prime ideals is finite, which is in fact same as the number of prime ideal in $S$ lying over $\mathfrak{p}$. Let the extension of $\mathfrak{q}_i$ in $S_{\mathfrak{p}}$ be $\mathfrak{Q}_i$ for all $i = 1, \dots, \ell$. Without loss of generality fix $i = 1$, i.e. consider the non-zero prime ideal $\mathfrak{Q}_1$. Then by unique factorization of ideals we know that $\mathfrak{Q}_1^2 \neq \mathfrak{Q}_1$, i.e. there exists a non-zero element $x \in \mathfrak{Q}_1\backslash\mathfrak{Q}_1^2$. Also, since dimension is 1, every non-zero prime ideal $\mathfrak{Q}_i$ is a maximal ideal. Hence the ideals $\mathfrak{Q}_1^2, \mathfrak{Q}_2, \dots, \mathfrak{Q}_\ell$ are pairwise co-prime. Hence by Chinese Remainder Theorem [DF11, Theorem 7.6.17] we have the following ring isomorphism

$$\begin{aligned} \chi : S_{\mathfrak{p}}/(\mathfrak{Q}_1^2\mathfrak{Q}_2 \cdots \mathfrak{Q}_\ell) &\to S_{\mathfrak{p}}/\mathfrak{Q}_1^2 \times S_{\mathfrak{p}}/\mathfrak{Q}_2 \cdots \times S_{\mathfrak{p}}/\mathfrak{Q}_\ell \\ r &\mapsto (r + \mathfrak{Q}_1^2, r + \mathfrak{Q}_2, \dots, r + \mathfrak{Q}_\ell) \end{aligned}$$

Hence there exists $y \in S_{\mathfrak{p}}$ such that $\chi(y) = (x+\mathfrak{Q}_1^2, 1+\mathfrak{Q}_2, \dots, 1+\mathfrak{Q}_\ell)$, i.e. $y-x \in \mathfrak{Q}_1^2$ and $y - 1 \in \mathfrak{Q}_i$ for all $i = 2, \dots, \ell$. Since $y - x \in \mathfrak{Q}_1^2 \subsetneq \mathfrak{Q}_1$ and $x \in \mathfrak{Q}_1\backslash\mathfrak{Q}_1^2$, we have $\langle y \rangle \subseteq \mathfrak{Q}_1$ but $\langle y \rangle \nsubseteq \mathfrak{Q}_1^2$. Also, $y - 1 \in \mathfrak{Q}_i$ and $1 \notin \mathfrak{Q}_i$ for all $i = 2, \dots, \ell$ (proper ideals) implies that $\langle y \rangle \nsubseteq \mathfrak{Q}_i$ for all $i = 2, \dots, \ell$. But in a commutative ring every proper ideal must be contained in some maximal ideal [DF11, Proposition 7.11], we conclude that $\langle y \rangle = \mathfrak{Q}_1$. Hence, non-zero prime ideals (maximal ideals) of $S_{\mathfrak{p}}$ are principal ideals. Since number of prime ideals is finite and every proper ideal is a unique product of prime ideals, we conclude that $S_{\mathfrak{p}}$ is a principal ideal domain.

Combining the above two claims with the previous step, we complete the proof of this step.

Step 3. *It is sufficient to prove the theorem for the localizations $R_{\mathfrak{p}}$ and $S_{\mathfrak{p}}$.*

Given a prime ideal $\mathfrak{q}$ in $S$ lying over the non-zero prime ideal $\mathfrak{p}$ in $R$, let $\mathfrak{Q}$ and $\mathfrak{P}$ be the extensions of $\mathfrak{q}$ and $\mathfrak{p}$, under the respective localization ring homomorphisms.

Claim 1. $e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P})$
This follows directly from the Going-up Lemma [AM07, Theorem 5.10] since $R \subseteq S$ and $S$ is integral over $R$.

Claim 2. $f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P})$
This follows from the following general lemma:

> *Given a commutative ring $R$, a maximal ideal $\mathfrak{m} \subset R$ and a multiplicative closed subset $D \subseteq R\backslash\mathfrak{m}$. Then $R/\mathfrak{m} \cong D^{-1}R/D^{-1}\mathfrak{m}$ as fields. Where the ring isomorphism is given by*
>
> $$\sigma : R/\mathfrak{m} \to D^{-1}R/D^{-1}\mathfrak{m}$$
> $$r + \mathfrak{m} \mapsto \frac{r}{1} + D^{-1}\mathfrak{m}$$
>
> The above map is injective because any homomorphism from a field to a non-zero ring is injective ($0 \notin D$ implies that $D^{-1}R$ is a non-zero ring and $\mathfrak{m} \cap D = \phi$ implies that $D^{-1}m$ is a prime ideal). The map is surjective because for any $\frac{a}{d} + D^{-1}\mathfrak{m} \in D^{-1}R/D^{-1}\mathfrak{m}$ there exists $t \in R$ such that $td - 1 \in \mathfrak{m}$ (since $d \notin \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal, i.e. $\langle \mathfrak{m}, d\rangle = R$) and we have
>
> $$\sigma(rt + \mathfrak{m}) = \frac{r}{d} + D^{-1}\mathfrak{m}$$
>
> as per the equivalence relations of localization.

By Lemma 1.4 we know that $\mathfrak{q} \cap R = \mathfrak{p}$, hence $R \subseteq S$ implies that $R\backslash\mathfrak{p} = R\backslash(\mathfrak{q} \cap R) \subseteq S\backslash(\mathfrak{q} \cap S) = S\backslash\mathfrak{q}$. Thus by the above lemma, $R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{P}$ and $S/\mathfrak{q} \cong S_{\mathfrak{p}}/\mathfrak{Q}$. Thus we have

$$\dim_{R/\mathfrak{p}} S/\mathfrak{q} = \dim_{R_{\mathfrak{p}}/\mathfrak{P}} S_{\mathfrak{p}}/\mathfrak{Q}$$

Hence completing the proof of our claim.

Combining the above three steps, we complete the proof of the theorem. □

**Remark 1.8.** We know a direct proof of the above theorem when $R$ and $S$ are ring of integers of number fields [Kor16, Theorem 18]. The key difference between that proof and the proof given above is that there we could use the concept of embeddings in $\mathbb{C}$ [Kor16, Definition 4] and here we had to take help of localization [Lor96, Theorem III.3.5]. Moreover, additional assumption of the field extension $L$ over $K$ being separable allows us to write a simpler proof involving linear algebra instead of localization [Neu99, Proposition 8.2].

**Example 1.2.** We can find prime ideal factorization of ring of integers of quadratic number fields. That is, we set $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{m})$ for some square free integer $m$, and

$$S = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

Then for $\mathfrak{p} = \langle p\rangle$ where $p$ is some prime integer, we get [Kor16, Theorem 28].

$$\mathfrak{p}S = \begin{cases} \langle p, \sqrt{m}\rangle^2 & \text{if } p \mid m \\ \langle 2, 1 + \sqrt{m}\rangle^2 & \text{if } p = 2, m \equiv 3 \pmod 4 \\ \left\langle 2, \frac{1+\sqrt{m}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{m}}{2}\right\rangle & \text{if } p = 2, m \equiv 1 \pmod 8 \\ \text{prime} & \text{if } p = 2, m \equiv 5 \pmod 8 \\ \langle p, n + \sqrt{m}\rangle\langle p, n - \sqrt{m}\rangle & \text{if } p \neq 2, p \nmid m, m \equiv n^2 \pmod p \\ \text{prime} & \text{if } p \nmid m \text{ and } m \text{ is not a quadratic residue mod } p \end{cases}$$

# Chapter 2

# Motivation for scheme theory

In the second chapter of our previous report we tried to illustrate the relationship between arithmetic and geometry using the specific example of elliptic curves. In this chapter we wish to explore foundations of these geometric relations. Our aim is to introduce few ideas which will help us develop the general geometric machinery (scheme theory) needed for further investigations. We won't define what is meant by scheme in this report.

## 2.1 Spectrum of a ring

As seen in Theorem 1.2, spectrum of a ring is the collection of the primes ideals of that ring. But we can give it a topological structure using subsets of the spectrum which behave like closed sets.

**Lemma 2.1.** *Let $R$ be a commutative ring with identity and $\mathfrak{a}$ be an ideal of $R$. We define*

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{a} \subseteq \mathfrak{p}\} \subseteq \operatorname{Spec} R$$

*Then the following properties hold:*

*(i)* $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$

*(ii)* $\bigcap_\lambda V(\mathfrak{a}_\lambda) = V\left(\sum_\lambda \mathfrak{a}_\lambda\right)$

*(iii)* $V(R) = \phi$ *and* $V(0) = \operatorname{Spec} R$

*Proof.* (i) We will show both side set containment.

($\subseteq$) This is trivial.

($\supseteq$) For this we need to use the fact that prime ideals are irreducible ideals [AM07, Proposition 1.11(ii)].

$$\begin{aligned}
\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b}) &\Rightarrow \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p} \\
&\Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p} && \text{(irreducible ideal)} \\
&\Rightarrow \mathfrak{p} \in V(\mathfrak{a}) \text{ or } \mathfrak{p} \in V(\mathfrak{b}) \\
&\Rightarrow \mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})
\end{aligned}$$

(ii) This follows from the fact that $\sum_\lambda \mathfrak{a}_\lambda$ is the smallest ideal containing all $\mathfrak{a}_\lambda$'s.

$$\begin{aligned}
\mathfrak{p} \in \bigcap_\lambda V(\mathfrak{a}_\lambda) &\iff \mathfrak{p} \in V(\mathfrak{a}_\lambda)\ \forall \lambda \\
&\iff \mathfrak{a}_\lambda \subseteq \mathfrak{p}\ \forall \lambda
\end{aligned}$$

$$\iff \sum_{\lambda} \mathfrak{a}_\lambda \subseteq \mathfrak{p}$$
$$\iff \mathfrak{p} \in V\left(\sum_{\lambda} \mathfrak{a}_\lambda\right)$$

(iii) True since there is no prime ideal containing whole ring (prime ideals are proper ideals) and every prime ideal contains the zero ideal.

□

**Definition 2.1** (Zariski topology)**.** Let $X = \operatorname{Spec} R$, then we define topology $\tau$ on $X$ such that the closed subsets are of the form $V(\mathfrak{a})$. Moreover, the sets of the form $D(r) = \operatorname{Spec} R \backslash V(\langle r \rangle)$ for all $r \in R$ constitute a base of open subsets of $\operatorname{Spec} R$.

**Lemma 2.2.** *The singleton $\{\mathfrak{p}\} \subset \operatorname{Spec} R$ is closed in the Zariski topology if and only if $\mathfrak{p}$ is a maximal ideal of $R$.*

*Proof.* ($\Rightarrow$) Since $\{\mathfrak{p}\}$ is closed, $\{\mathfrak{p}\} = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ in $R$. Since $\mathfrak{p}$ is the only prime ideal containing $\mathfrak{a}$ and every proper ideal of a commutative ring with identity should be contained in a maximal ideal [DF11, Proposition 7.11], $\mathfrak{p}$ is a maximal ideal.

($\Leftarrow$) If $\mathfrak{p}$ is a maximal ideal then $V(\mathfrak{p}) = \{\mathfrak{p}\}$ and hence $\{\mathfrak{p}\}$ is a closed set. □

**Definition 2.2** (Closed point)**.** A prime ideal $\mathfrak{p}$ in $R$ is said to be a closed point of $\operatorname{Spec} R$ if $\{\mathfrak{p}\}$ is a closed set of $\operatorname{Spec} A$ under the Zariski topology.

**Example 2.1.** Since $\mathbb{Z}$ is a principal ideal domain [DF11, Proposition 8.1], we have

$$\operatorname{Spec} \mathbb{Z} = \{\langle 0 \rangle\} \cup \{\langle p \rangle : p \text{ is a prime integer}\}$$

Here every non-zero prime ideal is a maximal ideal. Hence all prime ideals except the zero ideal, represent closed points of $\operatorname{Spec} \mathbb{Z}$.

**Definition 2.3** (Affine line)**.** Let $k$ be a field, then the we define the affine line $\mathbb{A}^1_k = \operatorname{Spec} k[x]$ where $k[x]$ is the ring of polynomials with coefficients in the field $k$. Since $k[x]$ is a principal ideal domain [DF11, Corollary 9.4], we have

$$\mathbb{A}^1_k = \{\langle 0 \rangle\} \cup \{\langle f(x) \rangle : f(x) \text{ is a monic irreducible polynomial}\}$$

**Remark 2.1.** Here every non-zero prime ideal is a maximal ideal. Hence all prime ideals except the zero ideal, represent closed points of $\mathbb{A}^1_k$. Moreover, all proper closed subsets of $\mathbb{A}^1_k$ are finite sets since any polynomial is a product of finitely many irreducible polynomials.

**Proposition 2.1.** *Let $\varphi : R \to S$ be a ring homomorphism, where $R$ and $S$ are commutative rings with identity. We define the map of sets*

$$\varphi^* : \operatorname{Spec} S \to \operatorname{Spec} R$$
$$\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$$

*Then the following properties are true:*

*(i) The map $\varphi^*$ is continuous.*

*(ii) If $\varphi$ is a localization morphism, i.e. $S = D^{-1}R$ for some multiplicatively closed subset $D$ of $R$, then $\varphi^*$ is a homemorphism onto the subspace $\{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{p} \cap D = \phi\}$ of $\operatorname{Spec} R$.*

*(iii) If $\varphi$ is surjective, then $\varphi^*$ induces a homeomorphism onto the closed subset $V(\ker(\varphi))$ of $\operatorname{Spec} R$.*

*Proof.* The map $\varphi^*$ is well defined since contraction of a prime ideal is again a prime ideal [AM07, pp. 9].

(i) We need to show that inverse image of a closed set of Spec $R$ is a closed set in Spec $S$. Let $V(\mathfrak{a}) \subset \operatorname{Spec} R$ be a closed set where $\mathfrak{a}$ is an ideal in $R$. Hence it is sufficient to prove the following

`Claim:` $\varphi^{*-1}(V(\mathfrak{a})) = V(\varphi(\mathfrak{a})S)$, where $\varphi(\mathfrak{a})S$ is the ideal in $S$ generated by $\varphi(\mathfrak{a})$.

We will show both side set containment simultaneously.

$$\begin{aligned} \mathfrak{q} \in \varphi^{*-1}(V(\mathfrak{a})) &\iff \varphi^*(\mathfrak{q}) \in V(\mathfrak{a}) \\ &\iff \varphi^{-1}(\mathfrak{q}) \in V(\mathfrak{a}) \\ &\iff \mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q}) \\ &\iff \varphi(\mathfrak{a}) \subseteq \mathfrak{q} \\ &\iff S\varphi(\mathfrak{a}) \subseteq \mathfrak{q} \\ &\iff \mathfrak{q} \in V(S\varphi(\mathfrak{a})) \end{aligned}$$

(ii) We know that $\varphi^*$ is a bijection onto $\{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{p} \cap D = \phi\}$ [AM07, Proposition 3.11(iv)] and continuity follows from previous part. We just need to show that $\varphi^{*-1}$ is continuous. Hence it's sufficient to show that $\varphi^*$ is a closed map. Let $V(\mathfrak{b}) \subset \operatorname{Spec} D^{-1}R$ be a closed set, where $\mathfrak{b}$ is an ideal in $D^{-1}R$.

`Claim:` $\varphi^*(V(\mathfrak{b})) = V(\varphi^{-1}(\mathfrak{b})) \cap \operatorname{Im}(\varphi^*)$, where $\varphi^{-1}(\mathfrak{b})$ is the ideal in $R$ [AM07, pp. 9].

($\subseteq$) $V(\mathfrak{b}) \subset \operatorname{Spec} D^{-1}R$ implies that $\varphi^*(V(\mathfrak{b})) \subseteq \operatorname{Im}(\varphi^*)$. Also, we have

$$\begin{aligned} \mathfrak{p} \in \varphi^*(V(\mathfrak{b})) &\Rightarrow \mathfrak{p} = \varphi^{-1}(\mathfrak{q}) && \text{for some } \mathfrak{q} \in V(\mathfrak{b}) \\ &\Rightarrow \mathfrak{p} = \varphi^{-1}(\mathfrak{q}) && \text{such that } \mathfrak{b} \subseteq \mathfrak{q} \\ &\Rightarrow \varphi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p} \\ &\Rightarrow \mathfrak{p} \in V(\varphi^{-1}(\mathfrak{b})) \end{aligned}$$

($\supseteq$) Let $\mathfrak{p} \in V(\varphi^{-1}(\mathfrak{b})) \cap \operatorname{Im}(\varphi^*) \subseteq \operatorname{Im}(\varphi^*)$. Since $\varphi^*$ is a bijection onto $\operatorname{Im}(\varphi^*)$, there exists $\mathfrak{q} \in \operatorname{Spec} D^{-1}R$ such that $p = \varphi^{-1}(\mathfrak{q})$. But since $\varphi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p}$, we have $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q})$, i.e. $\mathfrak{b} \subseteq \mathfrak{q}$. Hence $\mathfrak{q} \in V(\mathfrak{b})$ which is equivalent to saying $\mathfrak{p} \in \varphi^*(V(\mathfrak{b}))$.

(iii) Consider the following lemma:

*If $\varphi : R \to S$ is a surjective ring homomorphism between commutative rings with identity, with an ideal $\mathfrak{a}$ in $R$ and an ideal $\mathfrak{b}$ in $S$ such that $\ker\varphi \subset \mathfrak{a}$. Then the following properties hold:*

(1) $\mathfrak{a}^{ec} = \mathfrak{a}$ *and* $\mathfrak{b}^{ce} = \mathfrak{b}$

(2) $\mathfrak{a}$ *is a prime ideal in $R$ if and only if $\mathfrak{a}^e$ is a prime ideal in $S$.*

*where $\mathfrak{a}^e = S\varphi(\mathfrak{a})$ is the extension ideal of $\mathfrak{a}$ in $S$ and $\mathfrak{b}^c = \varphi^{-1}(\mathfrak{b})$ is the contraction ideal of $\mathfrak{b}$ in $R$.*

We know that there exists a bijection between the set of contracted ideals in $R$ and extended ideals in $S$ [AM07, Proposition 1.17]: $\{\mathfrak{a} : \mathfrak{a}^{ec} = \mathfrak{a}\} \longleftrightarrow \{\mathfrak{b} : \mathfrak{b}^{ce} = \mathfrak{b}\}$. For (1) note that since $\varphi$ is surjective, every ideal $\mathfrak{b}$ of $S$ is an extension ideal, i.e. $\mathfrak{b} = \mathfrak{a}^e$ for some ideal $\mathfrak{a}$ in $R$. For (2), non-trivial fact is that the extension ideal is again a prime ideal. Here we use the fact that $\ker\varphi \subseteq \mathfrak{a}$. Suppose $x, y \in S$ such that $xy \in \mathfrak{a}^e$ where $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in R$ (surjection). Now choose $c \in \mathfrak{a}$ such that $\varphi(c) = xy$) (possible due to previous part). Then $ab - c \in \ker\varphi \subseteq \mathfrak{a}$, i.e. $ab \in \mathfrak{a}$. Since $\mathfrak{a}$ is a prime ideal, $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$. Hence we have $x \in \mathfrak{a}^e$ or $y \in \mathfrak{a}^e$.

Hence $\varphi^*$ is a bijection onto the set of prime ideals containing $\ker\varphi$, i.e. $V(\ker\varphi)$. We already know that $\varphi^*$ is a continuous map. Hence it's enough to show that $\varphi^*$ is a closed map, i.e. $\varphi^{*-1}$ is continuous. Let $V(\mathfrak{b}) \subset \operatorname{Spec} S$ be a closed set, where $\mathfrak{b}$ is an ideal in $S$.

`Claim:` $\varphi^*(V(\mathfrak{b})) = V(\varphi^{-1}(\mathfrak{b}))$, where $\varphi^{-1}(\mathfrak{b})$ is the ideal in $R$ [AM07, pp. 9].

We will show both side set containment.

($\subseteq$) This containment is same as that for the previous part.

($\supseteq$) Let $\mathfrak{p} \in V(\varphi^{-1}(\mathfrak{b}))$, then $\varphi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p}$. Since $\langle 0\rangle \subseteq \mathfrak{b}$, we have $\varphi^{-1}(\langle 0\rangle) \subseteq \varphi^{-1}(\mathfrak{b})$. Hence we have $\ker\varphi \subseteq \varphi^{-1}(\mathfrak{b})$, i.e. $V(\varphi^{-1}(\mathfrak{b})) \subseteq V(\ker\varphi)$. Since $\varphi^*$ is a bijection onto $V(\ker\varphi)$, there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) \in V(\varphi^{-1}(\mathfrak{b}))$. Therefore, $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q})$, i.e. $\mathfrak{b} \subseteq \mathfrak{q}$. Hence $\mathfrak{q} \in V(\mathfrak{b})$, i.e. $\mathfrak{p} \in \varphi^*(V(\mathfrak{b}))$.

□

**Theorem 2.1.** *The prime ideals in $\mathbb{Z}[x]$ are:*

*(i)* $\langle 0\rangle$

*(ii) principal prime ideal $\langle f\rangle$, where $f$ is either a prime integer $p$, or a $\mathbb{Q}$-irreducible polynomial written so that its coefficients have* gcd *1*

*(iii) maximal ideals $\langle p, f\rangle$, where $p$ is a prime integer and $f$ is a monic integral polynomial irreducible modulo $p$.*

*Proof.* Our goal is to determine the $\operatorname{Spec}\mathbb{Z}[x]$, and we will use the previous theorem to achieve this goal. Consider the canonical ring homomorphism:

$$\begin{aligned}\varphi :&\mathbb{Z} \hookrightarrow \mathbb{Z}[x]\\ &n \mapsto n\end{aligned}$$

Then we have the following corresponding map of the sets:

$$\begin{aligned}\varphi^* : \operatorname{Spec}\mathbb{Z}[x] &\to \operatorname{Spec}\mathbb{Z}\\ \mathfrak{p} &\mapsto \varphi^{-1}(\mathfrak{p})\end{aligned}$$

where $\varphi^{-1}(\mathfrak{p}) = \mathfrak{p} \cap \mathbb{Z}$. Also, by Example 2.1 we know that $\operatorname{Spec}\mathbb{Z} = \{\langle 0\rangle\} \bigcup \left(\bigcup_p \{p\mathbb{Z}\}\right)$. Now by Proposition 2.1(i) we know that $\varphi^*$ is a continuous map, and hence

$$\operatorname{Spec}\mathbb{Z}[x] = \varphi^{*-1}(\{\langle 0\rangle\}) \bigcup \left(\bigcup_p \varphi^{*-1}(\{p\mathbb{Z}\})\right) \tag{2.1}$$

We will now analyse the preimage of zero ideal and non-zero prime ideals of $\mathbb{Z}$ under the $\varphi^*$ map.

Claim 1. $\varphi^{*-1}(\{\langle 0\rangle\})$ *is homeomorphic to* $\mathbb{A}^1_{\mathbb{Q}}$.

Consider the multiplicative closed subset $D = \mathbb{Z}\backslash\{0\}$ of $\mathbb{Z}[x]$. Then we have the canonical ring homomorphism between $\mathbb{Z}[x]$ and $D^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$:

$$\begin{aligned}\psi : \mathbb{Z}[x] &\to \mathbb{Q}[x]\\ f(x) &\mapsto \frac{f(x)}{1}\end{aligned}$$

Then we have the following map of sets:

$$\psi^* : \mathbb{A}^1_{\mathbb{Q}} \to \operatorname{Spec}\mathbb{Z}[x]$$

$$\mathfrak{q} \mapsto \psi^{-1}(\mathfrak{q})$$

Now by Proposition 2.1(ii) we know that $\psi^*$ is a homeomorphism onto the subspace

$$\begin{aligned}\{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \mathfrak{p} \cap D = \phi\} &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \mathfrak{p} \cap \mathbb{Z} = \{0\}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \varphi^{-1}(\mathfrak{p}) = \langle 0\rangle\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \varphi^*(\mathfrak{p}) = \langle 0\rangle\} \\ &= \varphi^{*-1}(\langle 0\rangle)\end{aligned}$$

Claim 2. *$\varphi^{*-1}(\{p\mathbb{Z}\})$ is homeomorphic to $\mathbb{A}^1_{\mathbb{F}_p}$.*

Consider the natural surjective ring homomorphism between $\mathbb{Z}[x]$ and $\mathbb{Z}[x]/\langle p\rangle = \mathbb{F}_p[x]$:

$$\begin{aligned}\sigma_p : \mathbb{Z}[x] &\to \mathbb{F}_p[x] \\ f(x) &\mapsto f(x) \mod p\end{aligned}$$

where $f(x) \mod p = f(x) + \langle p\rangle$. Then we have the following map of sets

$$\begin{aligned}\sigma_p^* : \mathbb{A}^1_{\mathbb{F}_p} &\to \operatorname{Spec} \mathbb{Z}[x] \\ \mathfrak{q} &\mapsto \sigma_p^{-1}(\mathfrak{q})\end{aligned}$$

Now by Proposition 2.1(iii) we know that $\sigma_p^*$ is a homeomorphism onto the subspace

$$\begin{aligned}V(\ker \sigma_p) &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \ker \sigma_p \subseteq \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \langle p\rangle \subseteq \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}\} \qquad (\mathbb{Z} \text{ is a Dedekind domain, Lemma 1.4}) \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \varphi^{-1}(\mathfrak{p}) = p\mathbb{Z}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[x] : \varphi^*(\mathfrak{p}) = p\mathbb{Z}\} \\ &= \varphi^{*-1}(p\mathbb{Z})\end{aligned}$$

Now using the above two claims in (2.1) we get

$$\operatorname{Spec} \mathbb{Z}[x] = \psi^*\left(\mathbb{A}^1_{\mathbb{Q}}\right) \bigcup \left(\bigcup_p \sigma_p^*(\mathbb{A}^1_{\mathbb{F}_p})\right)$$

Also, from Definition 2.3 we know the elements of $\mathbb{A}^1_{\mathbb{Q}}$ and $\mathbb{A}^1_{\mathbb{F}_p}$. Hence we have

$$\begin{aligned}\operatorname{Spec} \mathbb{Z}[x] =& \{\langle 0\rangle\} \bigcup \{\psi^{-1}(\langle g(x)\rangle) : g(x) \text{ is a monic irreducible polynomial in } \mathbb{Q}[x]\} \bigcup \\ & \left(\bigcup_p \langle p\rangle\right) \bigcup \left(\bigcup_p \{\sigma_p^{-1}(\langle g(x)\rangle) : g(x) \text{ is a monic irreducible polynomial in } \mathbb{F}_p[x]\}\right)\end{aligned} \tag{2.2}$$

since $\psi^{-1}(\langle 0\rangle) = \langle 0\rangle$ and $\sigma_p^{-1}(\langle 0\rangle) = \langle p\rangle$. Now we will analyse the inverse images of $\psi$ and $\sigma_p$ separately.

Claim 1. *Given a monic irreducible polynomial $g(x) \in \mathbb{Q}[x]$, we have $\psi^{-1}(\langle g(x)\rangle) = \langle f(x)\rangle$ where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{Q}$-irreducible polynomial with 1 as the* gcd *of the coefficients.*

By $\psi^{-1}(g(x))$ we mean to clear the denominators of coefficients, i.e. multiply the polynomial with the least common multiple of denominators of the coefficients. We observe that

$f(x)$ so obtained has 1 as the greatest common divisor of all the coefficients. This can be proved as follows.

$$g(x) = x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \ldots + \frac{a_0}{b_0}; \qquad \gcd(a_i, b_i) = 1 \ \forall \ i$$

Then for $\ell = \operatorname{lcm}(b_{n-1}, \ldots, b_0)$ we have

$$f(x) = \ell g(x) = \ell x^n + \ell\frac{a_{n-1}}{b_{n-1}}x^{n-1} + \ldots + \ell\frac{a_0}{b_0} \in \mathbb{Z}[x]$$

by clearing the denominators. Let $\gcd\left(\ell, \frac{\ell a_{n-1}}{b_{n-1}}, \ldots, \frac{\ell a_0}{b_0}\right) = d$. Now there exist $m_i \in \mathbb{Z}$ for $i = 0, \ldots, n$ such that $dm_n = \ell$ and $dm_i = \frac{\ell a_i}{b_i}$. Hence we have $m_n a_i = m_i b_i$, which implies that $b_i \mid m_n$ for all $i = 0, \ldots, n-1$ since $\gcd(a_i, b_i) = 1$. But then $\ell \mid m_n$ and hence $d = 1$.

Now we need to show both side set containment. This trivially follows from the fact that $\psi^{-1}(g(x)) = \ell g(x) = f(x) \in \langle f(x)\rangle$ and $\psi(f(x)) = \frac{f(x)}{1} = \frac{\ell g(x)}{1} \in \langle g(x)\rangle$.

Claim 2. *Given a monic irreducible polynomial $g(x) \in \mathbb{F}_p[x]$, we have $\sigma_p^{-1}(\langle g(x)\rangle) = \langle p, f(x)\rangle$ where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{F}_p$-irreducible polynomial such that $g(x) \equiv f(x) \mod p$.*

By $\sigma_p^{-1}(g(x))$ we mean to find a $f(x) \in \mathbb{Z}[x]$ such that $g(x) \equiv f(x) \mod p$, i.e $g(x) = f(x) + \langle p\rangle$. Hence we just need to prove both side set containment[1].

($\subseteq$) Let $r(x) \in \sigma_p^{-1}(\langle g(x)\rangle)$, then $\sigma_p(r(x)) = g(x)h(x)$ for some $h(x) \in \mathbb{F}_p[x]$. Now we have

$$r(x) + \langle p\rangle = (f(x) + \langle p\rangle)(s(x) + \langle p\rangle)$$

since $h(x) = s(x) + \langle p\rangle$ for some $s(x) \in \mathbb{Z}[x]$ (due to surjection). Hence we have

$$r(x) + \langle p\rangle = f(x)s(x) + \langle p\rangle$$

Thus we conclude that $r(x) - f(x)s(x) \in \langle p\rangle$, i.e. $r(x) - f(x)s(x) = pt(x)$ for some $t(x) \in \mathbb{Z}[x]$. We can rearrange the terms to get

$$r(x) = f(x)s(x) + pt(x) \in \langle p, f(x)\rangle$$

($\supseteq$) We have $p \in \sigma_p^{-1}(\langle g(x)\rangle)$ since $0 \in \langle g(x)\rangle$. Also, $f(x) \in \sigma_p^{-1}(\langle g(x)\rangle)$ since $\sigma_p(f(x)) = g(x)$.

Combining the above two claims with (2.2) we complete the proof. □

**Remark 2.2.** We followed the geometric approach for the above proof [Liu02, Example 2.1.8]. This illustrates a real mixing of arithmetic and geometric properties; $\operatorname{Spec}\mathbb{Z}[x]$ can be seen as a family of affine line, parametrized by the points of $\operatorname{Spec}\mathbb{Z}$, and over fields of different characteristics. We can also give a purely algebraic proof of this theorem but it won't give us much insights into the geometry [Rei95, Proposition 1.5].

[1] In the previous case, Gauss's lemma says that converse is also true, i.e. $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if $f(x)$ is irreducible in $\mathbb{Q}[x]$ where $f(x) \in \mathbb{Z}[x]$ such that the gcd of coefficients is 1 [DF11, Corollary 9.6]. But in this case, though irreducibility in $\mathbb{Z}/p\mathbb{Z}[x]$ implies irreducibility in $\mathbb{Z}[x]$, the converse is not true [DF11, Proposition 9.12].

## 2.2 Normalization

Given an $R$-algebra $S$, the ring of all elements of $S$ integral over $R$ is called the *integral closure*, or *normalization* of $R$ in $S$. The most important examples occur when $R$ is an integral domain and $S$ is its field of fractions. In this case the subalgebra of elements of $S$ integral over $R$ is simply called the *normalization of* $R$ [Eis04, pp. 118]. For example, consider a one-dimensional Noethrian integral domain $R$ which is not a Dedekind domain. Passing to the normalization of $R$, in geometric terms means taking the *resolution* of singularities in the scheme $X = \mathrm{Spec}(R)$ [Neu99, pp. 91]. We will explain the example once we introduce the definition of schemes.

**Definition 2.4** ($R$-algebra)**.** Let $R$ and $S$ be two commutative rings, then $S$ is an $R$-algebra if $S$ has a $R$-module structure with scalar multiplication defined by a ring homomorphism $\varphi : R \to S$ as $r \cdot s = \varphi(r)s$ for all $r \in R$ and $s \in S$.

**Remark 2.3.** If $R$ is a field $k$ and $S \neq 0$, then $\varphi$ is injective [AM07, Proposition 1.2] and therefore $k$ can be canonically identified with its image in $S$. Thus a $k$-algebra is effectively a ring containing $k$ as a subring, i.e. $\varphi(a) = a$ for all $a \in k$ (inclusion map).

**Definition 2.5** (Finite $R$-algebra)**.** $S$ is said to be finite $R$-algebra is $S$ is a finitely generated $R$-module.

**Definition 2.6** (Finitely generated $R$-algebra)**.** $S$ is said to be finitely generated $R$-algebra if there exists a finite set of elements $s_1, \ldots, s_n \in S$ such that every element of $S$ can be written as a polynomial in $s_1, \ldots, s_n$ with coefficients in $\varphi(R)$, i.e. $S = \varphi(R)[s_1, \ldots, s_n]$.

**Remark 2.4.** Finitely generated $R$-algebra is isomorphic to quotient of a polynomial ring over $\varphi(R)$. Consider the following ring homomorphism

$$\begin{aligned} \psi : \varphi(R)[x_1, x_2, \ldots, x_n] &\to \varphi(R)[s_1, s_2, \ldots, s_n] \\ f(x_1, x_2, \ldots, x_n) &\mapsto f(s_1, s_2, \ldots, s_n) \end{aligned}$$

where $\psi$ is surjective since every element of $S$ can be written as a polynomial in $s_1, \ldots, s_n$ with coefficients in $\varphi(R)$. Then by first isomorphism theorem we have $S \cong \varphi(R)[x_1, x_2, \ldots, x_n]/\ker\psi$.

**Definition 2.7** (Algebraically independent)**.** The elements $t_1, \ldots, t_m$ of an $R$-algebra are said to be algebraically independent if there doesn't exist a non-zero polynomial relation between $t_1, \ldots, t_m$ with coefficients in $\varphi(R)$.

**Remark 2.5.** If $S$ is a finitely generated $R$-algebra and all elements of $S$ are algebraically independent then $\ker\psi = \{0\}$ and $S$ is isomorphic to a polynomial ring.

**Lemma 2.3.** *Consider a finite set* $\{m^{(j)}\}_{j\in\{1,\ldots,\ell\}}$ *of* $n$*-tuples* $m^{(j)} = \left(m_1^{(j)}, m_2^{(j)}, \ldots, m_n^{(j)}\right)$ *where* $m_i^{(j)} \in \mathbb{Z}_{>0}$*. Then for two distinct tuples,* $m^{(j_1)} \neq m^{(j_2)}$*, there exists a system of positive integers* $w_1, \ldots, w_{n-1}, w_n = 1$ *such that*

$$\sum_{i=1}^{n} w_i m_i^{(j_1)} \neq \sum_{i=1}^{n} w_i m_i^{(j_2)}$$

*Proof.* We will proceed by induction on $n$. For $n = 1$ the statement is trivially true. Let $n > 1$, and the statement be true for upto $(n-1)$-tuples. Now consider $n$-tuples

$$\left(m_1^{(j_1)}, m_2^{(j_1)}, \ldots, m_n^{(j_1)}\right) \neq \left(m_1^{(j_2)}, m_2^{(j_2)}, \ldots, m_n^{(j_2)}\right)$$

Then we have two cases (without loss of generality):

Case 1. *When the* $(n-1)$*-tuples are equal, i.e.* $\left(m_2^{(j_1)},\ldots,m_n^{(j_1)}\right)=\left(m_2^{(j_2)},\ldots,m_n^{(j_2)}\right)$

Then we set $w_1=w_2=\ldots=w_n=1$ so as to ensure that

$$\sum_{i=1}^{n} w_i m_i^{(j_1)} \neq \sum_{i=1}^{n} w_i m_i^{(j_2)}$$

since $m_1^{(j_1)} \neq m_1^{(j_2)}$.

Case 2. *When the* $(n-1)$*-tuples are not equal, i.e.* $\left(m_2^{(j_1)},\ldots,m_n^{(j_1)}\right)\neq\left(m_2^{(j_2)},\ldots,m_n^{(j_2)}\right)$

Then by inductive hypothesis there exists $w_2,w_3,\ldots,w_{n-1},w_n=1$ such that

$$\sum_{i=2}^{n} w_i m_i^{(j_1)} \neq \sum_{i=2}^{n} w_i m_i^{(j_2)}$$

Now if $m_1^{(j_1)}=m_1^{(j_2)}$, then any choice of $w_1$ will work. Otherwise, we can choose sufficiently large $w_1$. For example,

$$w_1 > \max_j \left(\sum_{i=2}^{n} w_i m_i^{(j)}\right)$$

ensures that the inequality holds.

□

**Lemma 2.4** (Nagata's normalization)**.** *Suppose that* $R=k[r_1,r_2,\ldots,r_n]$ *be a finitely generated* $k$*-algebra and* $f\in k[x_1,x_2,\ldots,x_n]$ *be a non-zero polynomial such that* $f(r_1,r_2,\ldots,r_n)=0$*. Then there exist* $s_1,s_2,\ldots,s_{n-1}\in R$ *such that* $r_n$ *is integral over* $S=k[s_1,s_2,\ldots,s_{n-1}]$ *and* $R=S[r_n]$*.*

*Proof.* We have

$$f(x_1,x_2,\ldots,x_n)=\sum_{j=1}^{\ell}\alpha_{m^{(j)}}x^{m^{(j)}}=\sum_{j=1}^{\ell}\alpha_{m^{(j)}}\prod_{i=1}^{n}x_i^{m_i^{(j)}}$$

where $m^{(j)}=\left(m_1^{(j)},\ldots,m_n^{(j)}\right)$ and $\alpha_{m^{(j)}}\neq 0$ for all $n$-tuples $m^{(j)}$. As in Lemma 2.3, we can choose positive $w_1,w_2,\ldots,w_{n-1},w_n=1$ such that $\sum_{i=1}^{n} w_i m_i^{(j_1)} \neq \sum_{i=1}^{n} w_i m_i^{(j_2)}$ for $m^{(j_1)}\neq m^{(j_2)}$.

`Claim:` $s_i=r_i-r_n^{w_i}$ for $i=1,\ldots,n-1$.

We just need to check that $r_n$ is integral over $S=k[s_1,s_2,\ldots,s_{n-1}]$. Then $R=S[r_n]$ trivially follows due to the definition of $s_i$'s. We have

$$\begin{aligned} f(r_1,\ldots,r_{n-1},r_n) &= f(s_1+r_n^{w_1},\ldots,s_{n-1}+r_n^{w_{n-1}},r_n) \\ &= \sum_{j=1}^{\ell}\alpha_{m^{(j)}}\prod_{i=1}^{n-1}(s_i+r_n^{w_i})^{m_i^{(j)}}\ r_n^{m_n^{(j)}} \end{aligned}$$

where in $j^{th}$ summand the highest degree of $r_n$ is given by $\sum_{i=1}^{n} w_i m_i^{(j)}$. Due to our choice of $w_i$'s, all the $\ell$ sums $\sum_{i=1}^{n} w_i m_i^{(j)}$ are distinct. Hence we obtain a maximum value of $\sum_{i=1}^{n} w_i m_i^{(j)}$ for a unique $m^{(j)}$, let's call that unique $n$-tuple to be $m$. Hence we have

$$0=f(r_1,\ldots,r_{n-1},r_n)=\alpha_m g(r_n)$$

where $g(x)\in k[s_1,s_2,\ldots,s_{n-1}][x]$ is a monic polynomial. Thus $r_n$ is integral over $S=k[s_1,s_2,\ldots,s_{n-1}]$. □

**Remark 2.6.** Since $R = S[r_n]$ and $r_n$ is integral over $S$, we can also conclude that $R$ is a finite $S$-algebra [Kor17, Theorem 1.1].

**Theorem 2.2** (Noether's normalization)**.** *Let $k$ be a field and $R$ be a non-zero finitely generated $k$-algebra. Then there exist elements $t_1, \ldots, t_d \in R$ which are algebraically independent over $k$ and such that $R$ is integral over $k[t_1, \ldots, t_d]$.*

*Proof.* Let $R = k[r_1, \ldots, r_n]$, we now proceed by induction on the number of generators $n$ of $R$. If $n = 0$, then the statement trivially holds. If $n > 0$ and $r_1, \ldots, r_n$ are algebraically independent over $k$, then again nothing to prove since we have $R = k[t_1, \ldots, t_d]$, i.e. $r_i = t_i$ and $d = n$.

Now suppose that $n > 0$ and $r_1, \ldots, r_n$ are algebraically dependent, i.e. there exists non-zero polynomial $f \in k[x_1, \ldots, x_n]$ such that $f(r_1, \ldots, r_n) = 0$. Then by Lemma 2.4 we know that there exist $s_1, s_2, \ldots, s_{n-1} \in R$ such that $r_n$ is integral over $S = k[s_1, s_2, \ldots, s_{n-1}]$ and $R = S[r_n]$. Since by inductive hypothesis the statement is true for any finitely generated $k$-algebra with $(n-1)$ generators, there exist elements $t_1, \ldots, t_d \in S$ which are algebraically independent over $k$ and such that $S$ is integral over $T = k[t_1, \ldots, t_d]$. Hence we have $T \subseteq S \subseteq R$ such that $R$ is integral over $S$ and $S$ is integral over $T$. Thus we can conclude that $R$ is integral over $T$ [Kor17, Proposition 1.4]. Hence completing the proof. □

**Remark 2.7.** The proof discussed above is due to Nagata in the 1950s [Rei95, Theorem 4.6]. There is an alternative proof traditional in algebraic geometry, which works if the field $k$ is infinite [AM07, Exercise 5.16].

**Corollary 2.1.** *Let $k$ be a field and $R$ be a non-zero finitely generated $k$-algebra. Then there exist elements $t_1, \ldots, t_d \in R$ which are algebraically independent over $k$ and such that $R$ is a finite $k[t_1, \ldots, t_d]$-algebra.*

*Proof.* Since $k[t_1, \ldots, t_d] \subseteq R$, $R$ is a finite $k[t_1, \ldots, t_d]$-algebra if and only if $R$ is a finitely generated $k[t_1, \ldots, t_d]$-algebra and is integral over $k[t_1, \ldots, t_d]$ [AM07, pp. 60]. By the above theorem we already know that $R$ is integral over $k[t_1, \ldots, t_d]$. Since $k \subseteq k[t_1, \ldots, t_d] \subseteq R$ and $R$ is finitely generated $k$-algebra, we conclude that $R$ is a finitely generated $k[t_1, \ldots, t_d]$-algebra. □

**Lemma 2.5.** *Let $R = k[x_1, \ldots, x_n]$ be a ring of polynomials and $f \in R$ be a non-constant polynomial. Then there exists $y_1, \ldots, y_{n-1} \in R$ such that $x_n$ is integral over $S = k[y_1, \ldots, y_{n-1}, f]$ and $R = S[x_n]$.*

*Proof.* We have

$$f(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{\ell} \alpha_{m^{(j)}} x^{m^{(j)}} = \sum_{j=1}^{\ell} \alpha_{m^{(j)}} \prod_{i=1}^{n} x_i^{m_i^{(j)}}$$

where $m^{(j)} = \left(m_1^{(j)}, \ldots, m_n^{(j)}\right)$ and $\alpha_{m^{(j)}} \neq 0$ for all $n$-tuples $m^{(j)}$. As in Lemma 2.3, we can choose positive $w_1, w_2, \ldots, w_{n-1}, w_n = 1$ such that $\sum_{i=1}^{n} w_i m_i^{(j_1)} \neq \sum_{i=1}^{n} w_i m_i^{(j_2)}$ for $m^{(j_1)} \neq m^{(j_2)}$.

`Claim:` $y_i = x_i - x_n^{w_i}$ for $i = 1, \ldots, n-1$.

We just need to check that $x_n$ is integral over $S = k[y_1, y_2, \ldots, y_{n-1}, f]$. Then $R = S[x_n]$ trivially follows due to the definition of $y_i$'s. We have

$$\begin{aligned} f(x_1, \ldots, x_{n-1}, x_n) &= f(y_1 + x_n^{w_1}, \ldots, y_{n-1} + x_n^{w_{n-1}}, x_n) \\ &= \sum_{j=1}^{\ell} \alpha_{m^{(j)}} \prod_{i=1}^{n-1} (y_i + x_n^{w_i})^{m_i^{(j)}} \, x_n^{m_n^{(j)}} \end{aligned}$$

where in $j^{th}$ summand the highest degree of $x_n$ is given by $\sum_{i=1}^{n} w_i m_i^{(j)}$. Due to our choice of $w_i$'s, all the $\ell$ sums $\sum_{i=1}^{n} w_i m_i^{(j)}$ are distinct. Hence we obtain a maximum value of $\sum_{i=1}^{n} w_i m_i^{(j)}$ for a unique $m^{(j)}$, let's call that unique $n$-tuple to be $m$. Hence we have

$$f(x_1, \ldots, x_{n-1}, x_n) = \alpha_m g(x_n)$$

where $g \in k[y_1, \ldots, y_{n-1}][y]$ is a monic polynomial. Then $g(y) - \frac{f}{\alpha_m} \in S = k[y_1, \ldots, y_{n-1}, f][y]$ is a monic polynomial with $x_n$ as a root. Thus $x_n$ is integral over $S = k[y_1, y_2, \ldots, y_{n-1}, f]$. □

**Remark 2.8.** This lemma illustrates the power of Nagata's normalization process [Eis04, Lemma 13.2(a)]. Given a non-constant polynomial in a ring of polynomials $R$, we can find a subring $S \subseteq R$ such that $R$ is integral over $S$.

**Lemma 2.6.** *Let $R$ be a commutative ring and $\mathfrak{a} \subseteq \mathfrak{b}$ be ideals in $R$, then* $\dim(R/\mathfrak{b}) \leq \dim(R/\mathfrak{a})$.

*Proof.* If $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain of prime ideals containing $\mathfrak{b}$, then it is also a chain of prime ideals containing $\mathfrak{a}$. The result follows from the definition of Krull dimension. □

**Theorem 2.3.** *The Krull dimension of polynomial ring $k[x_1, x_2, \ldots, x_n]$ is $n$.*

*Proof.* Given to us is the polynomial ring $R = k[x_1, x_2, \ldots, x_n]$. We will proceed by induction on $n$.

`Base case`: For $n = 0$, we have $R = k$ which is of dimension 0 since $(0)$ is the only prime ideal, i.e. supremum of height of all prime ideals of $k$ is 0.

`Inductive hypothesis`: Krull dimension of any polynomial ring with less than $n$ variables is equal to the number of variables.

`Induction`: We have the following chain of prime ideals in $R = k[x_1, \ldots, x_n]$:

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_n)$$

Since this is a chain of length $n$, we have $\boxed{\dim R \geq n}$.

Now consider another chain of prime ideals in $R$ of length $\ell$:

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by Lemma 2.5 there exists $y_1, \ldots, y_{n-1} \in R$ such that $x_n$ is integral over $S = k[y_1, \ldots, y_{n-1}, f]$ and $R = S[x_n]$. Hence $R$ is integral over $S$. Now by incomparability of prime ideals under integral extensions [AM07, Corollary 5.9], we get the corresponding chain of prime ideals of length $\ell$ in $S$.

$$(0) \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f \rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by inductive hypothesis $\dim S/\langle f \rangle = n-1$. Since $\langle f \rangle \subseteq \mathfrak{p}_1 \cap S$, by Lemma 2.6 we know that $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f \rangle$, i.e. $\ell - 1 \leq n - 1$, equivalently $\ell \leq n$. Now by taking supremum of both sides we conclude that $\boxed{\dim R \leq n}$.

Combining both the inequalities we get that $\dim R = n$, hence completing the proof. □

**Remark 2.9.** This theorem introduces the technique of the normalization theorem in a simple setting [Eis04, Theorem 13.1]. We can give a second proof of this theorem using going-down lemma and the theory of primary decomposition [Eis04, Corollary 10.13a].

# Conclusion

In this report the stage for the introduction of scheme theory has been set. The idea of scheme can be used in algebraic number theory to deal with the rings like $R = \frac{\mathbb{Z}[x,y,z]}{\langle x^n+y^n-z^n \rangle}$. Considering Spec($R$) leads us towards Wile's celebrated proof of Fermat's Last Theorem. In future reports, the theory of schemes will be discussed.

# Bibliography


[AM07] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Levant Books, Howrah, West Bengal, indian edition, 2007.

[DF11] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley India Pvt. Ltd., New Delhi, 3 rd edition, 2011.

[Eis04] David Eisenbud. *Commutative Algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1 st edition, 2004.

[HK15] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Pearson India Education Services Pvt. Ltd., New Delhi, indian edition, 2015.

[Kor15] Gaurish Korpal. Diophantine equations. Summer internship project report, Bhaskaracharya Pratishthana, Pune, June 2015. https://gaurish4math.files.wordpress.com/2015/12/diophantine-equations-gaurish-rev4.pdf.

[Kor16] Gaurish Korpal. Number fields. Summer internship project report, Indian Statistical Institute, Bangalore, June 2016. https://gaurish4math.files.wordpress.com/2015/12/number-fields_gaurish_rev5.pdf.

[Kor17] Gaurish Korpal. Arithmetic Geometry - I. Course M498 project report, National Institute of Science Education and Research, Bhubaneswar, November 2017. https://gaurish4math.files.wordpress.com/2018/02/arithmetic-geometry-1-gaurish-rev.pdf.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 1 st edition, 2002.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island, 1996.

[Mar77] Daniel A. Marcus. *Number Fields*. Universitext. Springer-Verlag, New York, 1 st edition, 1977.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin-Heidelberg, 1 st edition, 1999.

[Rei95] Miles Reid. *Undergraduate Commutative Algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1 st edition, 1995.