Arithmetic Geometry

Gaurish Korpal

26 April 2018

Outline

Normalization

Given an S-algebra R, the ring of all elements of R integral over S is called the *integral closure*, or *normalization* of S in R.

The following lemma by Nagata gives us general method for finding a subring over which the given ring is integral.

Lemma 1

Let $R = k[r_1, r_2, \ldots, r_n]$ 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 $R = S[r_n]$.

This lets us prove the first main result of normalization, called Noether's normalization lemma.

Theorem 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 integral over $k[t_1, \ldots, t_d]$.

Normalization

Given an S-algebra R, the ring of all elements of R integral over S is called the *integral closure*, or *normalization* of S in R.
The following lemma by Nagata gives us general method for finding a subring over which the given ring is integral.

Lemma 1

Let $R = k[r_1, r_2, \ldots, r_n]$ 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 $R = S[r_n]$.

This lets us prove the first main result of normalization, called Noether's normalization lemma.

Theorem 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 integral over $k[t_1, \ldots, t_d]$.

Normalization

Given an S-algebra R, the ring of all elements of R integral over S is called the *integral closure*, or *normalization* of S in R.
The following lemma by Nagata gives us general method for finding a subring over which the given ring is integral.

Lemma 1

Let $R = k[r_1, r_2, \ldots, r_n]$ 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 $R = S[r_n]$.

This lets us prove the first main result of normalization, called Noether's normalization lemma.

Theorem 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 integral over $k[t_1, \ldots, t_d]$.

Nagata's argument

We can generalize Nagata's argument in the proof of previous lemma, to get the following result.

Lemma 2

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

Hence 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.

Dimension of polynomial ring

The concept of normalization is one of the cornerstone of dimension theory. This can be illustrated by using the previous lemma to find dimension of a polynomial ring. Let's first recall the definition of Krull dimension of a ring:

Krull dimension

The *Krull dimension* of a ring R, $\dim(R)$, is defined as

$$\dim(R) = \sup\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \text{ is prime ideal of } R\}$$

where $\mathrm{ht}(\mathfrak{p}) = \sup\{n : \mathfrak{p}_n \subsetneq \ldots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}, \mathfrak{p}_i \text{ are prime ideals of } R\}$.

Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring. We will proceed by induction on n.

We have the following chain of prime ideals in R:

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots \subsetneq \langle x_1, x_2, \ldots, x_n \rangle$$

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

Dimension of polynomial ring

The concept of normalization is one of the cornerstone of dimension theory. This can be illustrated by using the previous lemma to find dimension of a polynomial ring. Let's first recall the definition of Krull dimension of a ring:

Krull dimension

The *Krull dimension* of a ring R, $\dim(R)$, is defined as

$$\dim(R) = \sup\{\text{ht}(\mathfrak{p}) : \mathfrak{p} \text{ is prime ideal of } R\}$$

where $\text{ht}(\mathfrak{p}) = \sup\{n : \mathfrak{p}_n \subsetneq \ldots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}, \mathfrak{p}_i \text{ are prime ideals of } R\}$.

Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring. We will proceed by induction on n.

We have the following chain of prime ideals in R:

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots \subsetneq \langle x_1, x_2, \ldots, x_n \rangle$$

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

Dimension of polynomial ring

The concept of normalization is one of the cornerstone of dimension theory. This can be illustrated by using the previous lemma to find dimension of a polynomial ring. Let's first recall the definition of Krull dimension of a ring:

Krull dimension

The *Krull dimension* of a ring R, $\dim(R)$, is defined as

$$\dim(R) = \sup\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \text{ is prime ideal of } R\}$$

where $\mathrm{ht}(\mathfrak{p}) = \sup\{n : \mathfrak{p}_n \subsetneq \ldots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}, \mathfrak{p}_i \text{ are prime ideals of } R\}$.

Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring. We will proceed by induction on n.
We have the following chain of prime ideals in R:

$$\langle 0\rangle \subsetneq \langle x_1\rangle \subsetneq \langle x_1, x_2\rangle \subsetneq \cdots \subsetneq \langle x_1, x_2, \ldots, x_n\rangle$$

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

Dimension of polynomial ring

Now consider another chain of prime ideals in R of length ℓ:

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by the previous lemma, there exists a subring $S = k[y_1, \ldots, y_{n-1}, f]$, such that R is integral over S. Now by incomparability of prime ideals under integral extensions, we get the corresponding chain of prime ideals of length ℓ in S.

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f\rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by induction hypothesis $\dim S/\langle f\rangle = n-1$. Since $\langle f\rangle \subseteq \mathfrak{p}_1 \cap S$, we have $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f\rangle$ and hence $\operatorname{ht}(\mathfrak{p}_\ell \cap S) \leq \dim S/\langle f\rangle$, 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 $\dim R = n$.

Dimension of polynomial ring

Now consider another chain of prime ideals in R of length ℓ:

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by the previous lemma, there exists a subring $S = k[y_1, \ldots, y_{n-1}, f]$, such that R is integral over S. Now by incomparability of prime ideals under integral extensions, we get the corresponding chain of prime ideals of length ℓ in S.

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f\rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by induction hypothesis $\dim S/\langle f\rangle = n-1$. Since $\langle f\rangle \subseteq \mathfrak{p}_1 \cap S$, we have $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f\rangle$ and hence $\overline{\text{ht}(\mathfrak{p}_\ell \cap S)} \leq \dim S/\langle f\rangle$, 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 $\dim R = n$.

Dimension of polynomial ring

Now consider another chain of prime ideals in R of length ℓ:

$$\langle 0 \rangle \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by the previous lemma, there exists a subring $S = k[y_1, \ldots, y_{n-1}, f]$, such that R is integral over S. Now by incomparability of prime ideals under integral extensions, we get the corresponding chain of prime ideals of length ℓ in S.

$$\langle 0 \rangle \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f \rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by induction hypothesis $\dim S/\langle f \rangle = n-1$. Since $\langle f \rangle \subseteq \mathfrak{p}_1 \cap S$, we have $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f \rangle$ and hence $\mathrm{ht}(\overline{\mathfrak{p}_\ell \cap S}) \leq \dim S/\langle f \rangle$, 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 $\dim R = n$.

Dimension of polynomial ring

Now consider another chain of prime ideals in R of length ℓ:

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by the previous lemma, there exists a subring $S = k[y_1, \ldots, y_{n-1}, f]$, such that R is integral over S. Now by incomparability of prime ideals under integral extensions, we get the corresponding chain of prime ideals of length ℓ in S.

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f\rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by induction hypothesis $\dim S/\langle f\rangle = n-1$. Since $\langle f\rangle \subseteq \mathfrak{p}_1 \cap S$, we have $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f\rangle$ and hence $\mathrm{ht}(\overline{\mathfrak{p}_\ell \cap S}) \leq \dim S/\langle f\rangle$, 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 $\dim R = n$.

Dimension of polynomial ring

Now consider another chain of prime ideals in R of length ℓ:

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$

Let $f \in \mathfrak{p}_1$ be a non-constant polynomial, then by the previous lemma, there exists a subring $S = k[y_1, \ldots, y_{n-1}, f]$, such that R is integral over S. Now by incomparability of prime ideals under integral extensions, we get the corresponding chain of prime ideals of length ℓ in S.

$$\langle 0\rangle \subsetneq \mathfrak{p}_1 \cap S \subsetneq \mathfrak{p}_2 \cap S \subsetneq \cdots \subsetneq \mathfrak{p}_\ell \cap S$$

But $S/\langle f\rangle$ is isomorphic to a polynomial ring with $n-1$ variables. Hence by induction hypothesis $\dim S/\langle f\rangle = n-1$. Since $\langle f\rangle \subseteq \mathfrak{p}_1 \cap S$, we have $\dim S/(\mathfrak{p}_1 \cap S) \leq \dim S/\langle f\rangle$ and hence $\text{ht}(\overline{\mathfrak{p}_\ell \cap S}) \leq \dim S/\langle f\rangle$, 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 $\dim R = n$.

Dedekind domain

Let's first recall the definition:

Dedekind domain

A *Dedekind domain* is a Noetherian, integrally closed, integral domain of Krull dimension 1.

Examples: Principal ideal domains (except fields), Ring of integers of a number field

Dedekind domain

Let's first recall the definition:

Dedekind domain

A *Dedekind domain* is a Noetherian, integrally closed, integral domain of Krull dimension 1.

Examples: Principal ideal domains (except fields), Ring of integers of a number field

Factorization

We know that the rings of algebraic integers do not always have unique factorization property. For example, $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}[\sqrt{-5}]$, 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. But in a Dedekind domain we have unique factorization of ideals.

Theorem 2

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

Hence our motive is to find prime factorization of ideals in a Dedekind domain.

Factorization

We know that the rings of algebraic integers do not always have unique factorization property. For example, $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}[\sqrt{-5}]$, 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. But in a Dedekind domain we have unique factorization of ideals.

Theorem 2

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

Hence our motive is to find prime factorization of ideals in a Dedekind domain.

Factorization

We know that the rings of algebraic integers do not always have unique factorization property. For example, $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}[\sqrt{-5}]$, 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. But in a Dedekind domain we have unique factorization of ideals.

Theorem 2

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

Hence our motive is to find prime factorization of ideals in a Dedekind domain.

Localization

To prove the result which will help us do ideal factorization in Dedekind domains, we will take help of the technique of localization.

Theorem 3

A Dedekind domain is a Noetherian integral domain R whose localization $R_{\mathfrak{p}}$ at each non-zero prime ideal $\mathfrak{p}$ is a principal ideal domain with non-zero maximal ideal.

Hence we have an alternate definition of Dedekind domain in terms of localization.

Localization

To prove the result which will help us do ideal factorization in Dedekind domains, we will take help of the technique of localization.

Theorem 3

A Dedekind domain is a Noetherian integral domain R whose localization $R_{\mathfrak{p}}$ at each non-zero prime ideal $\mathfrak{p}$ is a principal ideal domain with non-zero maximal ideal.

Hence we have an alternate definition of Dedekind domain in terms of localization.

Localization

To prove the result which will help us do ideal factorization in Dedekind domains, we will take help of the technique of localization.

Theorem 3

A Dedekind domain is a Noetherian integral domain R whose localization $R_{\mathfrak{p}}$ at each non-zero prime ideal $\mathfrak{p}$ is a principal ideal domain with non-zero maximal ideal.

Hence we have an alternate definition of Dedekind domain in terms of localization.

Extension

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.

Lemma 3

$\mathfrak{p}S \neq S$ for any prime ideal $\mathfrak{p}$ in R.

Lemma 4

If S is a finitely generated R-module then S is a Dedekind domain and $\mathfrak{p} \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \mid \mathfrak{p}S$ where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals in R and S respectively.

Combining the above two lemmas we conclude that every prime ideal $\mathfrak{p}$ of R lies under at least one prime $\mathfrak{q}$ of S.

Extension

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.

Lemma 3

$\mathfrak{p}S \neq S$ for any prime ideal $\mathfrak{p}$ in R.

Lemma 4

If S is a finitely generated R-module then S is a Dedekind domain and $\mathfrak{p} \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \mid \mathfrak{p}S$ where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals in R and S respectively.

Combining the above two lemmas we conclude that every prime ideal $\mathfrak{p}$ of R lies under at least one prime $\mathfrak{q}$ of S.

Extension

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.

Lemma 3

$\mathfrak{p}S \neq S$ for any prime ideal $\mathfrak{p}$ in R.

Lemma 4

If S is a finitely generated R-module then S is a Dedekind domain and $\mathfrak{p} \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \mid \mathfrak{p}S$ where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals in R and S respectively.

Combining the above two lemmas we conclude that every prime ideal $\mathfrak{p}$ of R lies under at least one prime $\mathfrak{q}$ of S.

Extension

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.

Ramification index

The exponent with which the prime ideal $\mathfrak{q}$ occur in the prime decomposition of $\mathfrak{p}S$ is called its *ramification index*.

Residual degree

$R/\mathfrak{p}$ 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 e_i is the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $e(\mathfrak{q}_i/\mathfrak{p})$ and $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}]$ is the *residual degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $f(\mathfrak{q}_i/\mathfrak{p})$.

Extension

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.

Ramification index

The exponent with which the prime ideal $\mathfrak{q}$ occur in the prime decomposition of $\mathfrak{p}S$ is called its *ramification index*.

Residual degree

$R/\mathfrak{p}$ 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 e_i is the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $e(\mathfrak{q}_i/\mathfrak{p})$ and $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}]$ is the *residual degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $f(\mathfrak{q}_i/\mathfrak{p})$.

Extension

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.

Ramification index

The exponent with which the prime ideal $\mathfrak{q}$ occur in the prime decomposition of $\mathfrak{p}S$ is called its *ramification index*.

Residual degree

$R/\mathfrak{p}$ 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 e_i is the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $e(\mathfrak{q}_i/\mathfrak{p})$ and $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}]$ is the *residual degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$, denoted by $f(\mathfrak{q}_i/\mathfrak{p})$.

Extension

The following result will help us find the prime ideal factorization in Dedekind domains:

Theorem 4

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

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

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

Quadratic number field

We can illustrate the application of the result to find factorization of ideals in the ring of integers of a quadratic number field. 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

$$\mathfrak{p}S = \begin{cases} \langle p, \sqrt{m}\rangle^2 & \text{if } p \mid m \\ \langle 2, 1+\sqrt{m}\rangle^2 & \text{if } p = 2, m \equiv 3 \pmod 4 \\ \left\langle 2, \frac{1+\sqrt{m}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{m}}{2}\right\rangle & \text{if } p = 2, m \equiv 1 \pmod 8 \\ \text{prime} & \text{if } p = 2, m \equiv 5 \pmod 8 \\ \langle p, n+\sqrt{m}\rangle\langle p, n-\sqrt{m}\rangle & \text{if } p \neq 2, p \nmid m, m \equiv n^2 \pmod p \\ \text{prime} & \text{if } p \neq 2,\ p \nmid m,\ \left(\frac{m}{p}\right) = -1 \end{cases}$$

Quadratic number field

We can illustrate the application of the result to find factorization of ideals in the ring of integers of a quadratic number field. 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

$$\mathfrak{p}S = \begin{cases} \langle p, \sqrt{m} \rangle^2 & \text{if } p \mid m \\ \langle 2, 1+\sqrt{m} \rangle^2 & \text{if } p = 2, m \equiv 3 \pmod 4 \\ \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle & \text{if } p = 2, m \equiv 1 \pmod 8 \\ \text{prime} & \text{if } p = 2, m \equiv 5 \pmod 8 \\ \langle p, n+\sqrt{m} \rangle \langle p, n-\sqrt{m} \rangle & \text{if } p \neq 2, p \nmid m, m \equiv n^2 \pmod p \\ \text{prime} & \text{if } p \neq 2,\ p \nmid m,\ \left(\frac{m}{p}\right) = -1 \end{cases}$$

Spectrum of ring

Spectrum of a ring is the collection of the primes ideals of that ring. For example, $\operatorname{Spec}\mathbb{Z} = \{\langle 0\rangle\} \cup \{\langle p\rangle : p \text{ is a prime integer}\}$.

Zariski topology

Let R be a commutative ring with identity and $\mathfrak{a}$ be an ideal in 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) $V(R) = \phi$

(iv) $V(0) = \operatorname{Spec} R$

Then we define topology τ 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 $\operatorname{Spec} R$.

Spectrum of ring

Spectrum of a ring is the collection of the primes ideals of that ring. For example, $\operatorname{Spec}\mathbb{Z} = \{\langle 0\rangle\} \cup \{\langle p\rangle : p \text{ is a prime integer}\}$.

Zariski topology

Let R be a commutative ring with identity and $\mathfrak{a}$ be an ideal in 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) $V(R) = \phi$

(iv) $V(0) = \operatorname{Spec} R$

Then we define topology τ 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 $\operatorname{Spec} R$.

Spectrum of ring

Affine line

Let k be a field, then the we define the affine line $\mathbb{A}_k^1 = \operatorname{Spec} k[x]$ where $k[x]$ is the ring of polynomials with coefficients in the field k. Since $k[x]$ is a principal ideal domain, we have
$\mathbb{A}_k^1 = \{\langle 0\rangle\} \cup \{\langle f(x)\rangle : f(x) \text{ is a monic irreducible polynomial}\}$.

But, in general, determining all the prime ideals of a given ring is not easy. In the above two cases, we were able to write the prime ideals since the ring R was a principal ideal domain. Our motive is to determine the elements of spectrum of given ring R in general. For that we will take help of topological structure of the spectrum.

Spectrum of ring

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

But, in general, determining all the prime ideals of a given ring is not easy. In the above two cases, we were able to write the prime ideals since the ring R was a principal ideal domain. Our motive is to determine the elements of spectrum of given ring R in general. For that we will take help of topological structure of the spectrum.

Homeomorphism

Theorem 5

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

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

which is continuous. Moreover, following properties are true:

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

(ii) If φ is surjective, then φ^* induces a homeomorphism onto the closed subspace $V(\ker(\varphi))$.

Spectrum of $\mathbb{Z}[x]$

We can illustrate the application of the result to find prime ideals of $\mathbb{Z}[x]$. 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, we know that

$$\operatorname{Spec}\mathbb{Z} = \{\langle 0\rangle\} \bigcup \left(\bigcup_p \{p\mathbb{Z}\}\right)$$

By the above result we know that φ^* is a continuous map, and hence

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

Spectrum of $\mathbb{Z}[x]$

We can illustrate the application of the result to find prime ideals of $\mathbb{Z}[x]$. 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, we know that

$$\operatorname{Spec} \mathbb{Z} = \{\langle 0 \rangle\} \bigcup \left(\bigcup_p \{p\mathbb{Z}\} \right)$$

By the above result we know that φ^* is a continuous map, and hence

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

Spectrum of $\mathbb{Z}[x]$

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

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

Now by previous result we know that ψ^* is a homeomorphism from $\mathbb{A}^1_{\mathbb{Q}}$ onto $\varphi^{*-1}(\{\langle 0 \rangle\})$.

Spectrum of $\mathbb{Z}[x]$

We will now analyse the preimage of zero ideal and non-zero prime ideals of $\mathbb{Z}$ under the φ^* map. 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 $D^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$:

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

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 previous result we know that ψ^* is a homeomorphism from $\mathbb{A}^1_{\mathbb{Q}}$ onto $\varphi^{*-1}(\{\langle 0\rangle\})$.

Spectrum of $\mathbb{Z}[x]$

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 previous result we know that σ_p^* is a homeomorphism from $\mathbb{A}^1_{\mathbb{F}_p}$ onto $\varphi^{*-1}(\{p\mathbb{Z}\})$.

Spectrum of $\mathbb{Z}[x]$

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 previous result we know that σ_p^* is a homeomorphism from $\mathbb{A}^1_{\mathbb{F}_p}$ onto $\varphi^{*-1}(\{p\mathbb{Z}\})$.

Spectrum of $\mathbb{Z}[x]$

Now using the above two homeomorphisms (bijection) we get

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

as sets.

Next we note that:

(i) $\psi^{-1}(\langle 0\rangle) = \langle 0\rangle$

(ii) $\psi^{-1}(\langle g(x)\rangle) = \langle f(x)\rangle$ for any monic irreducible polynomial $g(x) \in \mathbb{Q}[x]$, where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{Q}$-irreducible polynomial with 1 as the gcd of the coefficients.

(iii) $\sigma_p^{-1}(\langle 0\rangle) = \langle p\rangle$

(iv) $\sigma_p^{-1}(\langle g(x)\rangle) = \langle p, f(x)\rangle$ for any monic irreducible polynomial $g(x) \in \mathbb{F}_p[x]$, where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{F}_p$-irreducible polynomial such that $g(x) \equiv f(x) \mod p$.

Spectrum of $\mathbb{Z}[x]$

Now using the above two homeomorphisms (bijection) we get

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

as sets.

Next we note that:

(i) $\psi^{-1}(\langle 0\rangle) = \langle 0\rangle$

(ii) $\psi^{-1}(\langle g(x)\rangle) = \langle f(x)\rangle$ for any monic irreducible polynomial $g(x) \in \mathbb{Q}[x]$, where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{Q}$-irreducible polynomial with 1 as the gcd of the coefficients.

(iii) $\sigma_p^{-1}(\langle 0\rangle) = \langle p\rangle$

(iv) $\sigma_p^{-1}(\langle g(x)\rangle) = \langle p, f(x)\rangle$ for any monic irreducible polynomial $g(x) \in \mathbb{F}_p[x]$, where $f(x) \in \mathbb{Z}[x]$ is $\mathbb{F}_p$-irreducible polynomial such that $g(x) \equiv f(x) \mod p$.

Spectrum of $\mathbb{Z}[x]$

Hence we conclude that the prime ideals in $\mathbb{Z}[x]$ are:

(i) principal prime ideal $\langle f \rangle$, where f is either 0, a prime integer p, or a $\mathbb{Q}$-irreducible polynomial written so that its coefficients have gcd 1

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

This illustrates a real mixing of arithmetic and geometric properties; $\operatorname{Spec} \mathbb{Z}[x]$ can be seen as a family of affine lines, parametrized by the points of $\operatorname{Spec} \mathbb{Z}$, and over fields of different characteristics.

Spectrum of $\mathbb{Z}[x]$

Hence we conclude that the prime ideals in $\mathbb{Z}[x]$ are:

(i) principal prime ideal $\langle f \rangle$, where f is either 0, a prime integer p, or a $\mathbb{Q}$-irreducible polynomial written so that its coefficients have gcd 1

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

This illustrates a real mixing of arithmetic and geometric properties; $\operatorname{Spec} \mathbb{Z}[x]$ can be seen as a family of affine lines, parametrized by the points of $\operatorname{Spec} \mathbb{Z}$, and over fields of different characteristics.

References I

- Michael F. Atiyah and Ian G. MacDonald. *Introduction to Commutative Algebra.* Levant Books, Howrah, 2007.
- David S. Dummit and Richard M. Foote. *Abstract Algebra.* Wiley India Pvt. Ltd., New Delhi, 3 rd edition, 2011.
- David Eisenbud. *Commutative Algebra,* volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2004.
- Kenneth Hoffman and Ray Kunze. *Linear Algebra.* Pearson India Education Services Pvt. Ltd., New Delhi, Indian edition, 2015.
- Gaurish Korpal. Diophantine equations. Summer internship project report, Bhaskaracharya Pratishthana, Pune, June 2015.
- Gaurish Korpal. Number fields. Summer internship project report, Indian Statistical Institute, Bangalore, June 2016.
- Gaurish Korpal. Arithmetic Geometry - I. Course M498 project report, NISER, Bhubaneswar, November 2017.

References II

- Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 1 st edition, 2002.
- Dino Lorenzini. *An Invitation to Arithmetic Geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island, 1996.
- Daniel A. Marcus. *Number Fields.* Universitext. Springer-Verlag, New York, 1 st edition, 1977.
- Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin-Heidelberg, 1 st edition, 1999.
- Miles Reid. *Undergraduate Commutative Algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1 st edition, 1995.