Arithmetic and Algebraic Geometry

Shou-Wu Zhang

April 28, 2015

Contents

1 Rings **7**
- 1.1 Rings and homomorphisms . . . 7
- 1.2 Ideals and quotients . . . 8
- 1.3 Special ideals and rings . . . 9

2 Spectra **13**
- 2.1 Spectra . . . 13
- 2.2 The Zariski Topology . . . 13
- 2.3 Morphisms . . . 15
- 2.4 Localization . . . 17
- 2.5 Neighborhoods . . . 18
- 2.6 Reducibility . . . 19

3 Affine Varieties **21**
- 3.1 Affine varieties . . . 21
- 3.2 Modules . . . 22
- 3.3 Noetherian rings . . . 23
- 3.4 Hilbert Basis Theorem . . . 24
- 3.5 Hillbert Nullstellensatz . . . 25
- 3.6 Dimension . . . 28

4 Projective Varieties **33**
- 4.1 Projective spaces . . . 33
- 4.2 Projective Spectra . . . 34
- 4.3 Hilbet Polynomial . . . 37
- 4.4 Dimensions . . . 40

5 Regularity **45**
- 5.1 Derivatives, tangent spaces, cotangent spaces . . . 45
- 5.2 Regular ring of dimension 1 . . . 48
- 5.3 Dedekind domain . . . 51
- 5.4 Modules over Dedekind domain . . . 56

6 Curves **59**
6.1 Number fields 59
6.2 Function fields 63
6.3 Algebraic curves 67
6.4 Differentials 70

Introduction

Some references for the course:

- Commutative Algebra:
  - Attiyah and McDonlad,*Introduction to Commutative Algebra*
  - Matsumura, *Commutative Rings*
- Algebraic Number Theory:
  - Cohen, *Advanced Number Theory*
  - Cassels and Frohlich,*Algebraic Number Theory*
  - Marcus, *Number Fields*
- Algebraic Geometry:
  - Shafarevich, *Basic Algebraic Geometry*
  - Hartshorne,*Algebraic Geometry*

Note that Szpiro has a course at CUNY that is similar to ours but more specialized in Dedekind Domains.

Explain the title of the course

Arithmetic: This is the study of constants in which the size of the constants is of importance.

Primarily we want to study:

- $\mathbb{N}$: the natural numbers which are closed under addition and multiplication.
- $\mathbb{Z}$: the integers which are closed under addition, subtraction, and multiplication.
- $\mathbb{Q}$: the rational numbers which are closed under addition, subtraction, multiplication and division.

Algebra: Here we study polynomials in $\mathbb{Q}$[T] with variable T. We also want to study these polynomials as a function of T which produce constants.

Geometry: The study of shapes

Algebraic Geometry: This is the study of solution sets defined by polynomials.

Let $f(x) = \sum_{i=1}^{n} a_i x^i$. The solution set is

$$\{\, x \in \mathbb{C} \mid f(x) = 0 \,\} = \{\, p_1, p_2, ..., p_r \,\}$$

with multiplicities. By the fundamental theorem of algebra,

$$\sum_{i=1}^{n} (\text{multiplicities of } p_i) = n.$$

Consider a polynomial function of two variables:

$$f(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} x^i y^j.$$

We want to study all solutions of f(x,y) = 0. That is we want to study the set

$$\{\ (x, y) \in \mathbb{C}^2 \mid \ \text{f(x,y)} = 0 \,\}.$$

This set is generally an infinite set with some sort of shape. Topologically it is a surface which may have some points missing.
Arithmetic Algebraic Geometry: We want to study the properties of the solutions to the polynomial equation f = 0 where f is some polynomial defined over $\mathbb{Z}$ or $\mathbb{Q}$.

We have a hierarchy: Arithmetic Algebraic Geometry is built up through a combination of Algebraic Geometry and Arithmetic. These two areas have commutative algebra, which is the study of commutative rings, as their foundation.

Chapter 1

Rings

1.1 Rings and homomorphisms

Let $\mathcal{R}$ be a ring. We have an object ($\mathcal{R}$,+,-,$\cdot$). This object contains a set with 3 operations. The operations are maps from $\mathcal{R}$x$\mathcal{R} \to \mathcal{R}$. The subset ($\mathcal{R}$,+) is a commutative group, and the subset ($\mathcal{R}$,$\cdot$) is a semi-group or monoid. In the ring there is an element 0 such that 0x = x0 = 0 for all x in $\mathcal{R}$. In the ring there is also an identity element 1, with the property that 1x = x1 = x for all x in $\mathcal{R}$. The ring $\mathcal{R}$ also satisfies a distribution law with respect to the operations of addition and subtraction.

Examples of rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, C (note $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields);
2. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

Definition 1.1.1. If $\mathcal{R}$ is a commutative ring, then $\mathcal{R}[x]$ is the ring of polynomials over $\mathcal{R}$:

$$\mathcal{R}[x] = \{ \sum_{i=1}^{n} a_i x^i \mid a_i \in \mathcal{R}, \text{ with operations } +, -, \text{ and } \cdot \ \}$$

Definition 1.1.2. Let $\mathcal{R}_1$, $\mathcal{R}_2$ be two rings. A homomorphism from $\mathcal{R}_1$ to $\mathcal{R}_2$ is a map

$$\phi : \mathcal{R}_1 \to \mathcal{R}_2$$

which preserves the operations:

$$\phi(x + y) = \phi(x) + \phi(y), \qquad \phi(xy) = \phi(x)\phi(y)$$

Definition 1.1.3. The kernel of a homomorphism $\phi : \mathcal{R}_1 \to \mathcal{R}_2$ is defined to be the preimage of 0 and its denoted by Ker(ϕ).

$$\text{Ker}(\phi) = \phi^{-1}(0) = \{ x \in \mathcal{R} \mid \phi(x) = 0 \}$$

Note that Ker(ϕ) measures the injectivity of ϕ.

Lemma 1.1.4. *The homomorphism ϕ is injective if and only if* ker$\phi = 0$.

Proof. The only if part is obvious. If $\phi(x_1) = \phi(x_2)$ then $\phi(x_1 - x_2) = 0$ so $x_1 - x_2 = 0$. $\square$

The homomorphism ϕ can be factorized as a compoisition of surjective map and an injective map

$$\mathcal{R}_1 \xrightarrow[\text{onto}]{\phi} \phi(\mathcal{R}_1) \hookrightarrow \mathcal{R}_2$$

The image $\phi(\mathcal{R}_1)$ is a *subring* of $\mathcal{R}_2$, while it is a *quotient ring* of $\mathcal{R}_1$.

Some notations

- Surjective map: $\twoheadrightarrow$
- injective map: $\hookrightarrow$ or $\rightarrowtail$

1.2 Ideals and quotients

Now we want to study the structure of kerϕ. Let ker$\phi = I$.
Property 1 *If $x \in I$ and $y \in I$ then $x + y \in I$.* Thus I is an Abelian subgroup of $\mathcal{R}$ under addition.
Property 2 *If $x \in \mathcal{R}$ and $y \in I$ then $xy \in I$.* Indeed

$$\phi(xy) = \phi(x)\phi(y) = 0.$$

Note that if $1 \in I$, then $\phi(1) = 0$ which implies

$$\phi(x) = \phi(x1) = 0$$

for all $x \in \mathcal{R}$. Thus for the most part, we assume
Property 3 *1 is not in I*

Definition 1.2.1. Let I $\hookrightarrow \mathcal{R}$ be a subset. We say I is an ideal if I satisfies two properties:

1. $x \in I, y \in I$ implies $x + y \in I$
2. $x \in I$, $y \in \mathcal{R}$ implies $xy \in I$

Theorem 1.2.2. *A subset I of $\mathcal{R}$ is the kernel of a homomorphism $\phi : \mathcal{R} \to \mathcal{R}'$, if and only if I is an ideal.*

Here is some machinery to start: Let $\mathcal{R}'$ denote the quotient $R/\sim$ of R modulo the relation $\sim$: where

$$x_1 \sim x_2 \quad \text{if and only if} \quad x_1 - x_2 \in I.$$

Step 1. Show this is an equivalence: indeed,

$$x_1 - x_2 \in I, \quad x_2 - x_3 \in I, \quad \text{then} \quad x_1 - x_3 \in I.$$

Notation: let $x \in \mathcal{R}$. The class of x in $\mathcal{R}'$ is denoted by $x + I$ or $x \pmod I$.
Step 2. Define addition and multiplication on $\mathcal{R}'$:

$$(x_1 \pmod I) + (x_2 \pmod I) = (x_1 + x_2) \pmod I$$

$$(x_1 \pmod I)(x_2 \pmod I) = x_1 x_2 \pmod I$$

Step 3. Show $\mathcal{R}'$ is a ring.
Step 4. Define a map

$$\phi : \mathcal{R} \to \mathcal{R}', \quad \phi(x) = x \pmod I.$$

Show ϕ is a homomorphism and $\ker\phi = I$.

1.3 Special ideals and rings

We want to introduce some special ideals and rings through study of examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$[x], $\mathbb{Q}$[x], $\mathbb{R}$[x], $\mathbb{C}$[x].

Fields

Let $I \hookrightarrow \mathbb{Q}$ be an ideal. If I is non-zero, then there is some non-zero element $a \in I$. If $a \in I$, then $a^{-1} \in I$, so $aa^{-1} = 1 \in I$. Thus the only ideal in $\mathbb{Q}$ not containing 1, is the zero ideal. This leads us to the following definition:

Definition 1.3.1. A *Field* is a ring whose only ideal is the zero ideal.

Another definition could be:

Definition 1.3.2. A *Field* is a ring in which every non-zero element is invertible. That is for all $x \in \mathcal{R}$ there exists $y \in \mathcal{R}$ such that $xy = 1$.

The equivalence of these two definitions is easy to see. If there were some non-zero element $x \in \mathcal{R}$ that was not invertible, then (x) will be non-zero and $(x) \neq \mathcal{R}$. If every non-zero element of $\mathcal{R}$ is invertible then clearly the only ideal of $\mathcal{R}$ is the zero ideal.

It is clear that $\mathbb{R}$ and $\mathbb{C}$ are also fields.

PID

In $\mathbb{Z}$, every ideal is generated by one element N.

$$I = (N) = \{\, Nx \mid x \in \mathbb{Z} \,\}.$$

This is easy to see by considering the smallest non-negative element and applying the Euclidean algorithm. Note these ideals are generated by one element. Such ideals are called principle. Similarly, using division algorithm one can show that every ideal is principle in the following rings $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

Definition 1.3.3. A *principle ideal* is an ideal generated by one element.

Definition 1.3.4. A principal ideal domain (PID) is a ring in which every ideal is a principal ideal.

The ring $\mathbb{Z}[x]$ is not a PID. For example the idea $(p, x) = p\mathbb{Z}[x] + f\mathbb{Z}[x]$ is not generated by one element. In fact, it can be proved that every idea of $\mathbb{Z}[x]$ is generated by at most two elements.

Integral domains

Let $\mathcal{R}$ be a ring.

Definition 1.3.5. A *zero divisor* $x \in \mathcal{R}$ is called a zero divisor if there exists a non-zero $y \in \mathcal{R}$ such that $xy = 0$.

Example 1.3.6. Let $\mathcal{R} = \mathbb{Z}/x^2$. Notice that x is non-zero in $\mathcal{R}$ but $x \cdot x = 0$. Thus this ring has non-zero zero divisors.

Definition 1.3.7. We say that $\mathcal{R}$ is an *integral domain* if $\mathcal{R}$ which does not contain any non-zero zero divisors. That is $xy = 0$ impiles $x = 0$ or $y = 0$.

Definition 1.3.8. Let $\mathcal{R}$ be an integral domain. The field of fractions $\mathrm{Frac}(\mathcal{R})$ is the field of *fractions* $\frac{a}{b}$ $(a, b \in R,\ b \neq 0)$ with usual equivalence ($\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$) and operations ($\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$).

Prime ideals

Definition 1.3.9. An ideal $\wp$ of $\mathcal{R}$ is called a *prime ideal* if $\mathcal{R}/\wp$ is an integral domain.

Definition 1.3.10. If $\wp$ is a prime ideal, then the residue field $k(\wp)$ of $\wp$ is defined to be the fraction field $\mathrm{Frac}(\mathcal{R}/\wp)$.

Note that the previous definition is equivalent to the condition that $x, y \notin \wp$ then $xy \notin \wp$.

Definition 1.3.11. An ideal of $\mathcal{R}$ is called a *maximal ideal* if $\mathcal{R}/\mathfrak{m}$ is a field.

Lemma 1.3.12. *The definition of Maximal Ideal is equivalent to the following condition: If* $\mathfrak{m}$ *is not* $\mathcal{R}$ *and there is no ideal* $\mathfrak{a}$ *such that* $\mathfrak{m} \subsetneq \mathfrak{a}$.

Proof. If I is maximal then R/I is a field. If this statement were not true then R/I has a non-zero ideal J. We have a map ϕ from R to R/I. Now $\phi^{-1}(J)$ is an ideal of R, but $\phi^{-1}(J) \supsetneq I$, a contradiction. To prove the other direction, use the same idea as above. □

Example 1.3.13. In the following we want to list all prime ideals of $\mathbb{Z}$, $\mathbb{C}[x]$, $\mathbb{R}[x]$, and $\mathbb{Q}[x]$. All these rings are PID. Thus every ideal has the form (f). This ideal is prime if and only if $f = 0$ or f is irreducible.

1. $\mathbb{Z}$: The only prime ideals are (0) and (p) where p is a prime. The quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a fintie field. denoted $\mathbb{F}_p$.

2. $\mathbb{C}[x]$: The only prime ideals are (0), and $\wp = (f)$ where $(x-a) \in \mathbb{C}[x]$ for some $a \in \mathbb{C}$. The quotient ring $\mathbb{C}[x]/(x-a)$ is isomorphic to $\mathbb{C}$ via the map x $\to a$.

3. $\mathbb{R}[x]$: The prime ideals are: (0), $(x-a)$ for some $a \in \mathbb{R}$ with quotient ring isomorphic to $\mathbb{R}$ via the map x $\to a$, and (x^2+ax+b) for some $a, b \in \mathbb{R}$ with $a^2 - 4b < 0$, with the quotient ring isomorphic to $\mathbb{C}$ via via the map x $\to$ to one of the roots of $x^2 + ax + b$. Their quotient rings have the following

4. $\mathbb{Q}[x]$: The prime ideals are (0) and (f) where f is irreducible over $\mathbb{Q}$ with quotient ring a subring embedded into $\mathbb{C}$ via $x \mapsto$ a root of $f(x) = 0$. The image of the map $\mathbb{Q}[a]$ a *number field*.

Theorem 1.3.14. *If* k *is a field and* $f(x)$ *is irreducible in* $k[x]$ *then the ideal* $(f(x))$ *is maximal and* $k[x]/f(x)$ *is a field*

Exercise 1.3.15. Prove this Theorem.

Remark 1.3.16. Let $k[x]/f(x)$ be denoted as K. Then K contains k and has dimension $n = degf(x)$ as a k-vector space. In the case $k = \mathbb{F}_p$, K is the finite field of with $q := p^n$-elements. The structure of K is determined completely by the cardinality q.

Lets look at prime ideals of $\mathbb{Z}[x]$. Recall that $\mathbb{Z}[x]$ is a unique factorization domain (UFD). Thus 0 is a prime ideal, and so is principal ideal (f) with f irreducible. If $f \in \mathbb{Z}$, then $f = p$ is a prime. We will prove later that all other prime ideals has the form $\wp = (p, f)$ where p is a prime, and f is non-constant polynomial which is irreducible mod p.

Chapter 2

Spectra

2.1 Spectra

We will introduce a topological realization of rings and ideals of a ring A:

$$\begin{aligned}\mathrm{Spec}(A) =&\text{the spectrum of } A\\ =&\text{some topological space in which } A \text{ is}\\ &\text{the ring of ``continuous functions''.}\end{aligned}$$

Definition 2.1.1. Let A be a ring. The spectrum of $\mathrm{Spec}(A)$ is the set of all prime ideals of A.

We also want to develop the notion of a valuation. Let $f \in A$ and $p \in \mathrm{Spec}(A)$. The value $f(p) \in k(p) = \mathrm{Frac}(A/p)$ is defined as the image of f in the composition $A \to A/p \to k(p)$.

Exercise 2.1.2. Let X denote the interval $(0, 1)$. Let $C(X)$ be the space of real valued continuous functions of X. Find all closed prime ideals of $C(x)$. Show that

$$\mathrm{Spec}_{\mathrm{top}} C(X) = X$$

where $\mathrm{Spec}_{\mathrm{top}}$ means take only the topologically closed prime ideals.

Exercise 2.1.3. Show that

$$\mathrm{Spec}\mathbb{C}[x] \cong \mathbb{C} \cup (\text{the zero prime ideal}).$$

Here the isomorphism is viewed as an isomorphism of spaces, $\mathbb{C}$ corresponds to maximal ideals, and (the zero prime ideal) corresponds to zero ideals.

2.2 The Zariski Topology

Now we want to develop the concept of topology for rings such that A becomes the space of continuous functions. In particular, for an $f \in A$, the set $Z(f)$ should be a closed subset.

More generally for an ideal I, let $Z(I)$ denote the zero subset of an ideal I in Spec(A), then $Z(I)$ should be a closed subset. This is because $Z(I)$ is generated by $Z(f)$ by taking intersections:

$$Z(I) = \bigcap_{f \in I} Z(f).$$

Definition 2.2.1. The *Zariski topology* on Spec$A$ is defined such that all closed subsets are of form

$$\begin{aligned} Z(I) &= \{\, \wp \mid f(\wp) = 0, \quad \forall f \in I \,\} \\ &= \{\, \wp \mid \wp \supset I \,\} \end{aligned}$$

To show that the topology just defined makes sense we have to show the finite unions of closet subsets are still subsets:

Lemma 2.2.2. *Let I and J be two ideals in $\mathcal{R}$, then*

$$Z(I) \cup Z(J) = Z(I \cdot J).$$

Proof. As $Z(I \cdot J) \supset Z(I)$ and $Z(I \cdot J) \supset Z(J)$, so $Z(I \cdot J) \supset Z(I) \cup Z(J)$. Let $\wp \in Z(I \cdot J)$, then $\wp \supset I \cdot J$. We want to show that either $\wp \supset I$ or $\wp \supset J$. Suppose $\wp \not\supseteq I$, then there exists $x \in I \backslash \wp$, $\wp \supset x \cdot J$ so $\wp \supset x \cdot y$ for all $y \in J$. So y must be in $\wp$. Thus $\wp \supset J$ and we are done. □

We consider the closed subsets of our topology $Z(I)$, where $Z(I)$ is the zero set of an ideal $I \subset A$. Note that if S is any subset of A, then $Z(S) = Z(I)$ for some ideal I.

Questions

1. *What functions are non-vanishing on all points in* Spec(A)*?*
2. *What functions are vanishing on every point in* Spec(A)*?*

Proposition 2.2.3. *Here are answers to these questions:*

1. *All the invertible elements in A denoted by A^*.*
2. *All the nilpotent elements in A denoted by*

$$\mathrm{Nil}(A) := \sqrt{0} = \{\, f \in A \mid \textit{there exists } n > 0 \textit{ such that } f^n = 0 \,\}.$$

Proof.

1: For $f \in A$, f is not invertible if and only if $(f) \neq A$. By Zorn's lemma there exists $\mathfrak{m}$ such that $(f) \subset \mathfrak{m}$. Where $\mathfrak{m}$ is a maximal ideal of A. $\mathfrak{m}$ is prime because the quotient $A/\mathfrak{m}$ is field and a field is always an integral domain. If $f \in \mathfrak{m}$ then $f(\mathfrak{m}) = 0$. Clearly if $f \in$ any ideal $\neq A$, then f is not invertible.

2: Assume f is not nilpotent. The set

$$\{ f^n \mid n \in \mathbb{N} \} \cap \{ 0 \} = \emptyset$$

Let I be an ideal such that

$$\{ f^n \mid n \in \mathbb{N} \} \cap I = \emptyset$$

and that I is maximal with respect to this property. Such as set exists because of Zorn's lemma. We need to show that I is a prime ideal. This will imply that $f(I) \neq 0$. This is quite clear. Let $x \in A \backslash I$, $y \in A \backslash I$. We want to show $xy \notin I$. $I + (x) \supsetneq I$, so there exists m such that $f^m \in I + (x)$.

Likewise there exists n such that $f^n \in I + (y)$.

This implies $f^{m+n} \in I + (xy)$.

So $I + (xy) \supsetneq I$. Thus $xy \notin I$, and we are done. □

When does $Z(I) = Z(J)$?

Note that $Z(0) = \mathrm{Spec}(A)$, $Z(f^2) = Z(f)$, and $Z(\mathrm{nil}(A)) = \mathrm{Spec}(A)$. Thus we can't conclude that $Z(I) = Z(J)$ implies $I = J$. $Z(I) = Z(J)$ if and only if there exists $f \in I$, and n such that $f^n \in J$.

Definition 2.2.4. Let I be an ideal of A. We define the nilpotent root of I as

$$\sqrt{I} = \{ f \in A \mid f^n \in I \text{ for some } n > 0 \}.$$

Example 2.2.5. .

1. $\sqrt{0} = nil(A)$
2. $\sqrt{\sqrt{I}} = \sqrt{I}$.

Proposition 2.2.6. $Z(I) = Z(\sqrt{I})$.

Now we are ready to answer the question previously asked: $Z(I) = Z(J)$ when $\sqrt{I} = \sqrt{J}$.

Proof. One could use the method of proof of Proposition 2.2.3. An alternate method would be to show that $f \in A$, $f|_{Z(I)} = 0$ if and only if $f \in \sqrt{I}$. Now examine the ring A/I and finish the rest as an exercise. □

2.3 Morphisms

Morphisms can be roughly described as special maps that preserve some structure under the mapping. If $A \to B$ is a homomorphism, then there is a morphism $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Why is the arrow reversed? Recall that A and B are being viewed as spaces of functions on their perspective spectra.

Definition 2.3.1. For $f : A \to B$ be a ring homomorphism, let $f^* : Spec(B) \to Spec(A)$ be a map so that $f^*(\wp) = f^{-1}(\wp)$.

We need to show that $f^{-1}(\wp)$ is prime otherwise the definition does not make sense. We have the following diagram:

$$\begin{array}{ccc} A & \to & B \\ \downarrow & & \downarrow \\ A/f^{-1}(\wp) & \hookrightarrow & B/\wp \end{array}$$

As $B/\wp$ is integral, the subring $A/f^{-1}(\wp)$ must be integral!

Lemma 2.3.2. *f^* is continuous*

Proof. We want to show that $f^{*-1}(Z(I))$ is closed, that is it is $Z(something)$ where we will determine what that something is. In fact $f^{*-1}(Z(I)) = Z(f(I))$.

$$\begin{aligned} \wp \in f^{*-1}(Z(I)) &\longleftrightarrow f^*(\wp) \in Z(I) \\ &\longleftrightarrow I \subset f^*(\wp) = f^{-1}(\wp) \\ &\longleftrightarrow f(I) \subset \wp \\ &\longleftrightarrow f(I) \cdot B \subset \wp \end{aligned}$$

Here we use B to make the left hand side an ideal. Thus $\wp \in Z(f(I) \cdot B)$. So we have shown that

$$f^{*-1}(Z(I)) = Z(f(I) \cdot B) = Z(f(I)).$$

□

Questions:

We have a map $A \to A/I$, what can be said about the map $\mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$?

Exercise 2.3.3. Show that the map is an injection and its image is $Z(I)$.

Questions

If we have a map $A \hookrightarrow B$ what can be said about the map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$?

Here is an example:

$$\mathbb{R} \hookrightarrow \mathbb{C}, \quad \text{and} \quad \mathrm{Spec}(\mathbb{C}) = \mathrm{Spec}(\mathbb{R}) = \{\,\text{point}\,\}.$$

Another example is to consider the map $\mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$. This induces

$$\mathrm{Spec}(\mathbb{C}[x]) \to \mathrm{Spec}(\mathbb{R}[x]).$$

Now

$$\begin{aligned}\mathrm{Spec}(\mathbb{C}[x]) &= \mathbb{C} \cup \{\, point \,\} \\ &= \{\, (x-a) \mid a \in \mathbb{C} \,\} \cup \{\, 0 \text{ ideal} \,\} \\ &= \{\, (x-a) \mid a \in \mathbb{C} \,\} \cup \mathrm{Spec}(\mathbb{C}(x)).\end{aligned}$$

Now

$$\mathrm{Spec}(\mathbb{R}[x]) = \{\, x-a, x^2+bx+c \,\} \cup \{\, 0 \text{ ideal} \,\}.$$

So

$$\mathrm{Spec}(\mathbb{R}[x]) = \mathrm{Spec}(\mathbb{C}[x])/conjugates.$$

Note that $\mathbb{R}[x]$ is the subring of $\mathbb{C}[x]$ of elements invariant under conjugation.

Definition 2.3.4. Suppose that we have a group G that acts on A (then G also acts on Spec$A$). Then A^G, called the G invariants in A, is the set of elements in A that are left invariant by G. and SpecA^G is called the categoric quotient of Spec$A$

2.4 Localization

Let $S \hookrightarrow Spec(A)$. What are the continuous functions on S? Let

$$T = \{\, f \in A \mid f \text{ is non-vanishing everywhere on } S \,\}.$$

T is multiplicative ($f, g \in T$ implies $fg \in T$) and we should be able to invert $\{\, T \,\}$, f^{-1} should also be a function on S. This process of formally adding inverses to a set is called localization.

Definition 2.4.1. The *localization* of A with respect to the multiplicative system T is a homomorphism $\phi : A \to B$ satisfies the following two properties:

1. For $t \in T$, $\phi(t)$ is invertible in B.

2. For any map $\phi' : A \to B'$ which has property 1, then there is a unique map $\psi B \to B'$ such that
$$\phi' = \psi \circ \phi.$$

Exercise 2.4.2. Show the local lization of A with respect to T is unique up to isomorphism if it does exist. This means that if $\phi_1 : A \to B_1$ and $\phi_2 : A :\to B_2$ both are localization of A w.r.t. T, then there is a "unique" isomorphism $\alpha : B_1 \to B_2$ such that $\phi_2 = \alpha \circ \phi_1$.

Notation 2.4.3. We denote the localization of A w.r.t. by $A[T^{-1}]$, or $T^{-1}A$.

One construction

There are many ways to construct A_T. Here is one way: Let $C = A[x_t : t \in T]$ denote the ring of polynomials of A with indetermines indexed by T. Let $I = (x_t \cdot t - 1 : t \in T)$ denote the ideal of C generated by $x_t \cdot t - 1$. Then we define

$$A[T^{-1}] = C/I.$$

Exercise 2.4.4. Show that the above construction really define a localization of A w.r.t. T as in the above definition.

2.5 Neighborhoods

What are the local neighborhoods around $\wp \in \mathrm{Spec}(A)$? It is easy to see

$$\mathrm{Spec}(A) \setminus Z(I) = \bigcup_{f \in I} \mathrm{Spec}(A) \setminus Z(f).$$

Thus the basis for open sets on $\mathrm{Spec}(A)$ are given by

$$\begin{aligned} D(f) &= \mathrm{Spec}(A) \setminus Z(f). \\ &= \{\, \wp \mid f(\wp) \neq 0 \,\} \end{aligned}$$

Notice that $A[f^{-1}]$ are functions on $D(f)$.

Exercise 2.5.1. Show that $D(f)$ is the image of the morphism

$$\mathrm{Spec}A[f^{-1}] \to \mathrm{Spec}A$$

induced by the homomorphism $A \to A[f^{-1}]$.

Fix on $\wp \in Spec(A)$, $\wp$ has neighborhoods

$$\{D(f) \mid f(\wp) \neq 0 \,\}$$

What are the functions locally defined at $\wp$? They are

$$\bigcup_{f \in D(f) (\longleftrightarrow f \notin \wp)} (\text{functions of D(f)}) = T^{-1}A, \quad T = A \setminus \wp.$$

Notation 2.5.2. Let $\wp$ be an ideal of A. Denote $T^{-1}A = A_{(\wp)}$. where $T = A \setminus \wp$.

Example 2.5.3. .

1. Let $p \in \mathrm{Spec}(\mathbb{Z})$. Functions defined out of p are

$$\begin{aligned} &\mathbb{Z}\left[1/n \mid n \text{ is invertible off } p\right] \\ =&\mathbb{Z}\left[1/n \mid \ell \nmid n \text{for all } \ell \neq p\right] \\ =&\mathbb{Z}\left[1/n \mid n = p^k\right] \\ =&\mathbb{Z}\left[1/p\right] \end{aligned}$$

2. What are functions defined locally at p? Answer: exactly the opposite. That is $\mathbb{Z}_{(p)} = \{ \frac{a}{b} \mid p \nmid b \}$.

3. Now look at

$$\bigcup_f \text{ functions on } D(f) = \text{ functions defined on an open subset}$$
$$= \bigcup_{n \neq 0} \mathbb{Z}[1/n] = \mathbb{Q}$$

We denote (o ideal) as $\eta \in \text{Spec}(\mathbb{Z})$.

Exercise 2.5.4. Prove that

$$\{ \eta \} = \bigcap (\text{all non-empty open sets}),$$

and that the Zariski closure is the whole plane, and finally that

$$\{ \eta \} = \text{ image of } \text{Spec}(\mathbb{Q}) \in \text{Spec}(\mathbb{Z}).$$

2.6 Reducibility

Recall also that $\sqrt{0} = \text{nil}(A)$ and $\text{Spec}(A) = \text{Spec}(A/\text{nil}(A))$. Look at the following example: $\mathbb{Z}/p^n\mathbb{Z}$ has nontrivial nilpotent radical for all n fixed. However $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ which has trivial nilpotent.

Definition 2.6.1. A ring A is called reduced if $\text{nil}(A) = 0$.

Questions:

1. *When is* $\text{Spec}(A) = X$ *connected? That is to say:*

$$X \neq X_1 \coprod X_2$$

where X_1 *and* X_2 *are closed and non-empty*

2. *When is* $\text{Spec}(A)$ *irreducible? That is to say:*

$$X \neq X_1 \cup X_2$$

Example 2.6.2. $X = \text{Spec}\mathbb{C}[x] = \mathbb{C} \cup \{ \text{the 0 ideal} \}$. Let $\eta = \{ \text{the 0 ideal} \}$. Lets look at the toplogy of toplogy of $\text{Spec}\mathbb{C}[x]$ The open subsets are

$$\mathbb{C} - \{ X_1, X_2, ..., X_n \} \cup \{ \eta \},$$

so this is irreducible.

Replace A by $A/\mathrm{nil}(A)$ which does not change the space $\mathrm{Spec}(A)$ and its topology, we may assume that A is reduced. Recall $\mathrm{nil}(A) = \bigcap_{P:\mathrm{primes}} P$. Let $X_i = Z(I_i)$ with $Z(I_i) \neq \mathrm{Spec}A$. Then above two conditions are equivalent to the following conditions for every prime P:

1. $P \supset I_1$ or $P \supset I_2$
2. But not both ($P \supsetneq I_1 + I_2$)

Condition 1 implies $P \supset I_1 \cdot I_2$ for every P. Thus $I_1 \cdot I_2 \subset \mathrm{nil}(A) = 0$. Condition 2 implies $P \supsetneq I_1 + I_2$ for every P. Thus $I_1 + I_2 = A$. We have $I_1 \cdot I_2 = 0$ and $I_1 + I_2 = 0$.

Exercise

1. Chinese Remainder Theorem: let A, I_1, and I_2 be as above, then the canonical projection gives an isomorphism
$$A \cong A/I_1 \oplus A/I_2$$
2. If $A = A_1 \oplus A_2$, then
$$\mathrm{Spec}(A) = \mathrm{Spec}(A_1) \coprod \mathrm{Spec}(A_2).$$
3. A has no two nonzero ideals I_1 and I_2 such that $I_1 \cdot I_2 = 0$ if and only if A is an integral.

Thus we have the following:

Proposition 2.6.3. $\mathrm{Spec}(A)$ *is connected if and only if* A *is indecomposible.* $\mathrm{Spec}(A)$ *is irreducible if and only if* A *is integral.*

Chapter 3

Affine Varieties

3.1 Affine varieties

Let k be a field. Then k is algebraicly closed if and only if Spec$k[x] \cong k \cup \eta$ where each $a \in k$ corresponds to the maximal ideal $(x-a)$ and where η corresponding to the 0 ideal. We call η a generic point.

Now we assume that k an algebraicly closed field, for example $k = \mathbb{C}$. Consider the n-dimensional affine space $k^n = \mathbb{A}^n(k)$ which has coordinate ring $A = k[x_1, \cdots, x_n]$. In an affine space we can define the Zariski topology such that closed subsets are of form

$$V(I) = \{\, (a_1, a_2, ..., a_n) \in k^n \mid f(a_1, a_2, ..., a_n) = 0 \text{ for all } f \in I \,\}.$$

where I is an ideal of $k[x_1, x_2, ..., x_n]$.

We can talk about irreducibilty and connectivity for closed subsets. If $k = \mathbb{C}$, the Zariski topology is different than the usual archimedean topology.

Definition 3.1.1. Let $V \subset k^n$ be an algebraic set. We say V is a closed subvariety if V is irreducible.

We can define a map $\mathbb{A}^n(k) \hookrightarrow \text{Spec}(k[x_1, x_2, ..., x_n])$ via $x \in (a_1, a_2, ..., a_n) \to$ a maximal ideal, $x_x = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$. This map is a topological embedding.

Theorem 3.1.2 (Hilbert Nullstellensatz)**.** *The images of the previously defined map are the set of maximal ideals.*

More generally, let I be an ideal of $k[_1, \cdots, x_n]$ which defines an algebraic set $X = V(I)$ of zeros of all polynomials in I. Then have a map: $i : X \to \text{Spec}(A/I)$ by

$$(x_1, x_2, ..., x_n) \to (x_1 - a_1, x_2 - a_2, ..., x_n - a_n).$$

This leads us to two questions:

1) How does X determine I?

Answer: There is a 1 to 1 correspondence between the algebraic sets X and set of the radical ideals $\sqrt{I} = I$.

2) What is the image of $i(X)$?

Answer: $i(X)$ is the set of the maximal ideals of $\mathrm{Spec}(A/I)$. The key fact for these answers is that A is a finitely generated algebra over k. This would not be true if A were not finitely generated over k.

We will prove these answers in next few classes.

3.2 Modules

Let M be an abelian group. Let $\mathrm{End}(M)$ denote the set of homomorphisms of M. Then $\mathrm{End}(M)$ is a ring with operations

$$(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x)$$

$$(\phi_1 \cdot \phi_2)(x) = \phi_1(\phi_2(x)).$$

The ring $\mathrm{End}(M)$ is in general noncommutative.

Definition 3.2.1. Let R be a ring. By a R-module M we mean an abelian group M with a homomorphism from $R \to END(M)$. Equivalently there is a map

$$R \times M \to M \quad \text{via} \quad (a, x) \mapsto a \cdot x$$

that satisfies:

1. $1 \cdot x = x$
2. $a(x + y) = ax + ay$
3. $(ab)x = a(bx)$

Example 3.2.2. .

1. If R is a field then an R-module is a vector space over R.
2. Let I be an ideal. If $I \hookrightarrow R$ then I is an R-module. In particular R is an R-module. The ideals are the R-submodules of R.

Definition 3.2.3. Let M be an R-module, $N \subset M$ a subgroup. N is a R-submodule if $R \cdot N \subseteq N$.

Example 3.2.4. If $R \to R'$ is a homomorphism, then R' is a R-module.

Definition 3.2.5. Let R be a ring. By an algebra A over R we mean a ring homomorphism from R to A.

Definition 3.2.6. Let R be a ring. Then $R[x_1, x_2, ..., x_n]$ is called the polynomial algebra of n-variables over R.

Example 3.2.7. Every ring R is an algebra over $\mathbb{Z}$ via natural morphism $n \mapsto n1_R$, e.g., $\mathbb{Z} \to \mathbb{Z}[\sqrt{-1}]$ or $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Exercise 3.2.8. Construct a counter example to the Nullstallensatz when $n = \infty$. Let $R = \mathbb{C}[x_t \mid t \in \mathbb{C}(y)]$. Define a map $\phi : R \twoheadrightarrow \mathbb{C}(y)$ via $x_t \to t$. Show that Kerϕ is a maximal ideal not given by $(..., x_t - a_t, ...)$ for $a_t \in \mathbb{C}$. Explain why this is a counter example.

Finitely generated Modules

Definition 3.2.9. Let $S \subset M$ be a subset of M. A submodule N generated by S is the set of all elements of the type $N = \{ \sum_{i=1}^{n} a_i x_i \mid x_i \in S \}$

Definition 3.2.10. We say M is finitely generated over R if there exists $x_1, x_2, ..., x_n \in M$ such that M is generated by $x_1, x_2, ..., x_n$. Equivalently M is a quotient of R^n.

Exercise 3.2.11. A module M is finitely generated if and only if there is a surjective homomorphism from a free module R^n of finite rank onto M.

3.3 Noetherian rings

Definition 3.3.1. Let R be a ring. We say R is Noetherian if the following is satisfied: Let M be a R-module and N be a R-module of M with $N \hookrightarrow M$, then if M is finitely generated then N is finitely generated.

Example 3.3.2. .

1. If R a field then R is Noetherian, this is obvious as finitely generated modules are finite dimensional vector spaces.

2. If $R = \mathbb{Z}$ then R is Northerian, this is less obvious but follows easily from the next lemma.

Theorem 3.3.3. *R is Noetherian if and only if every ideal is finitely generated.*

Proof. If R is Noetherian, R as an R-module is finitely generated. Every ideal of R is an R-submodule so clearly the ideals are finitely generated. Now assume every ideal of R is finitely generated. We want to show that every sub-module N of every finitely generated module M is finitely generated.

Step 1: Reduce M to a free module R^n of finite rank.

Indeed, as M is finitely generated, there is a surjective homomorphism $\phi : R^n \to M$. Let $N' = \phi^{-1}(N)$. Then the restriction of ϕ on N' is surjective onto N. Thus if N' is finitely generated then N is finitely generated. So we reduce to the case where $M = R^n$ and N is a submodule.

Step 2: Induction on n

It is trivial if $n = 1$ as then N is an ideal of R. Now assume that $n > 1$ and that every submodule of R^{n-1} is finitely generated. Let $\phi : R^n \to R$ be the projection onto the last factor. Then we have the following

- $\ker(\phi) = R^{n-1}$, the first $n-1$ factors.
- Let $N' = N \cap R^{n-1}$ then N' is the kernel of the homomorphism $N \to \phi(N)$. As N' is a submodule of R^{n-1}, by induction assumption, N' is finitely generated. Let $x_1, \cdots, x_m$ be generaters of N'.
- $\phi(N)$ is finitely generated, as $\phi(N)$ is an ideal of R. Let $y_1, \cdots, y_n$ be generators of $\phi(N)$.

Lift $y_1, y_2, ..., y_n$ to $y_1^{'}, y_2^{'}, ..., y_n^{'} \in N$. Claim: $x_1, x_2, ..., x_m, y_1^{'}, y_2^{'}, ..., y_n^{'}$ generate N. Proof of Claim: Let $x \in N$. Then $\phi(x)$ is a linear combination of y_j's: $\phi(x) = \sum a_j y_j$. This implies $\phi(x - \sum a_j y_j^{'}) = 0$. So the element $x - \sum a_i y_i^{'}$ is in N' and therefore is a linear combination of x_i's: $x - \sum a_j y_j^{'} = \sum b_i x_i$. Thus x is a linear combination of $x_i's$ and y_j's. So N is finitely generated. □

3.4 Hilbert Basis Theorem

Theorem 3.4.1. *If R is Noetherian then $R[x]$ is Noetherian.*

Proof. Let I be an ideal of $R[x]$. We want to prove that I is finitely generated. Let $J \hookrightarrow R$ be an ideal of leading coefficients of polynomials in I. Since R is Noetherian, J is finitely generated. Let $f_1, f_2, ..., f_n \in I$ be elements whose leading coefficients generate J. We write $f_i = c_i x^{n_i} + ...$ with n_i the degree of f_i and a_i the leading coefficient of f_i.

Let $f \in I$. We can write $f = a_n x^n + ... + a_0$ with a_n non-zero. As $a_n \in J$, we can write $a_n = \sum b_i \cdot c_i$. If $n \geqq n_i$ for every i we can write $g = f - \sum b_i f_i x^{n-n_i}$ where the n-th coefficient of g is zero. By induction on n, we have proved that every polynomial $f \in I$ can be written as $f = \sum_{i=1}^{n} g_i f_i + f^{'}$ where $\deg(f^{'}) \leqq \max(n_i)$.

Let $m = \max(n_i)$ and

$$I^{'} = \{\, f \in I \text{ where } \deg(f) \leqq m \,\}.$$

Then $I^{'}$ is not an $R[x]$ but it is a R-submodule of $\sum_{i=1}^{n} R_i x^i \cong R^m$. Since R is Noetherian, $I^{'}$ is finitely generated. There are elements $f_1^{'}, f_2^{'}, ..., f_\ell^{'}$ in $I^{'}$ generating $I^{'}$ as an R-module. Thus $f_1, f_2, ..., f_l, f_1^{'}, f_2^{'}, ..., f_\ell^{'}$ generating I. □

Exercise 3.4.2. An equivalent statement of the theorem is: If R is Noetherian then every finitely generated R-algebra is Noetherian.

Exercise 3.4.3. Let T be a multiplicative system of R. Prove $R[\frac{1}{T}]$ is Noetherian if R is Noetherian.

3.5 Hillbert Nullstellensatz

Let $k = \overline{k}$ be algebraicly closed. Let $\mathbb{A}^n_k = k^n$ be the affine space. We have a map $\mathbb{A}^n_k \to \text{Spec}k[x_1, \ldots, x_n]$ via

$$(a_1, \ldots, a_n) \longmapsto m_x = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$$

a maximal ideal.

Theorem 3.5.1. *The image of this map is the set of maximal ideals.*

Equivalently:

Theorem 3.5.2. *Let K be a field containing k such that K is finitely generated as a k-algebra. Then $k = K$.*

Proof of the equivalence. Theorem 3.5.1 implies Theorem 3.5.2: $K = k[t_1, \ldots, t_n]$ where $t_i \in K$. We have a map $Q\colon k[x_1, \ldots, x_n] \twoheadrightarrow K$ via $x_i \mapsto t_i$. Clearly, Q is a homomorphism and $\ker Q$ is a maximal ideal of $k[x_1, \ldots, x_n]$. By Theorem 3.5.1, $\ker Q$ is generated by $x - a_i$, $a_i \in k$. Thus

$$K \cong \frac{k[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} = k.$$

Theorem 3.5.2 implies Theorem 3.5.1: If m is a maximal ideal of $k[x_1, \ldots, x_n]$ then $K[x_1, \ldots, x_n]/m$ is a field and it is finitel generated over k. Therefore, $K = k$ by Theorem 3.5.2. We obtain $k = k[x_1, \ldots, x_n]/m$, which implies $x_i \equiv a_i \pmod{m}$, so $x_i - a_i \in m$. Thus $(x_1 - a_1, \ldots, x_n - a_n) \subset m$. So since m is maximal, $(x_1 - a_1, \ldots, x_n - a_n) = m$. □

Example 3.5.3. Let $K = k(x)$ be the field of fractions in $K[x]$. Then K is not finitely generated as a k-algebra.

Proof. Assume that K is finitely generated over k: $K = k\left[\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\right]$. This implies that every fraction in K has a denominator of the form $g_1^{t_1} \ldots g_n^{t_n}$. Thus there are only finitely many irreducible polynomials, say, $P_1, \ldots, P_r$. Then $(1 + P_1 \cdot \ldots \cdot P_n)$ will have a prime factor P_i. But it is prime to $P_1, \ldots, P_r$ so we have a contradiction. □

Exercise 3.5.4. $\mathbb{Q}$ is not finitely generated over $\mathbb{Z}$ as an algebra.

Proof of Theorem 3.5.2. Suppose Theorem 2 is false. Suppose $K = k[t_1, \ldots, t_n]$ and there is a $t_i \notin k$, so t_i must be transcendental over k.

Definition 3.5.5. Let $K_1 \hookrightarrow K_2$ be an extension of fields. Let $x \in K_2$. We say x is *algebraic in* K_1 if x satisfies an equation $a_n x^n + \ldots + a_0 = 0$ with $a_n \neq 0$, $a_0, \ldots, a_n \in K_1$, otherwise we say x is transcendental over K_1.

Back to the proof of Theorem 3.5.2. After rearranging the order of $t_1, \ldots, t_n$ we may assume that

- t_i is transcendental over $k[t_1, \ldots, t_{i-1}]$ for $1 \leq i \leq r$ but
- t_i is algebraic over $k[t_1, \ldots, t_r]$ if $i > r$.

We have

$$\begin{array}{ccccc} k & \hookrightarrow & k(t_1, \ldots, t_r) & \hookrightarrow & k[t_1, \ldots, t_n] \\ & & \| & & \| \\ & & L & & k(t_1, \ldots, t_n) \quad = \quad K \end{array}$$

1. L/k is not finitely generated as an algebra by Example 3.5.3.
2. K/k is finitely generated as an algebra.
3. K is a L-vector space of finite dimension by the following lemma.

Lemma 3.5.6. *Let $K_1 \hookrightarrow K_2$ be a field extension. Let $x \in K_2$, then x is algebraic over K_1 if and only if $K_1(x)$ is a K_1 vector space of finite dimension.*

Proof. The " $\Longleftarrow$ " part is obvious. To prove the " $\Longrightarrow$ " part note that $K_1[x] = \sum_{n=0}^{\infty} K_1 x^n$. Since $a_n x^n + \ldots + a_0 = 0$ and $a_n \neq 0$ it follows that $K_1[x]$ is finite dimensional. □

So we have reduced the proof of Theorem 3.5.2 to the following lemma:

Lemma 3.5.7. *Let $A \subset B \subset C$ be extensions of rings with A noetherian such that*

1) C is a finitely generated A algebra;

2) C is finitely generated as a B-module.

Then B is finitely generated as an A-algebra.

Proof. Strategy: let us construct $B' \subset B$ such that

1) B' is finitely generated as an A-algebra.

2) C is finitely generated as a B'-module.

This will imply

3) B' is Noetherian.

4) B is finitely generated as a B'-module (consider B as a B' submodule of C).

Then 1) and 4) imply B is finitely generated as an A-algebra.

Write $C = A[x_1, \ldots, x_n]$, $C = \sum_{j=1}^{m} By_i$ with x_i, y_j in C. Let b_{ijk}'s be elements of B such that

$$x_i y_j = \sum_{k=0}^{m} b_{ijk} y_k.$$

where $y_0 = 1$.

Claim: *Let $B' = A[b_{ijk}]$. Then B' satisfies 1) and 2).*

Obviously, B' satisfies 1). For 2) we need only show that C is generated by y_j's as a B'-module. Let C' denote this B'-module: $C' = \sum_{k=0}^{m} B' y_k$. Then

$$x_i C' = \sum_{k=0}^{m} B' x_i y_k \subset C'.$$

In other words, C' is closed under multiplication by x_i's. As C is generated by x_i's, C' is closed under multiplication by C. Since C contains $y_0 = 1$, it follows that $C \subset C'$. This concludes the proof of Lemma 3.5.7. □

Theorem 3.5.2 is proved.

□

What happens if $k \neq \overline{k}$? For example, let $A = k[x]$, and m a maximal ideal in A. Then $m = (f(x))$ with $f(x)$ irreducible and $A/m = k[x]\Big/(f(x))$ may not be equal to k but is algebraic over k. The above proof will give the following:

Theorem 3.5.8 (Hilbert Nullstellensatz)**.** *Let k be a field (not necessarily equal to $\overline{k}$). Let A/k be an algebra of finite type. Let $m \subset A$ be a maximal ideal, then $K \subseteq A/m$ is algebraic over k.*

Assume again that $k = \bar{k}$. Let $X \hookrightarrow \mathbb{A}_k^n$ be an algebraic closed set defined by an ideal $\mathfrak{a}$ of $k[x_1, \ldots, x_n]$. Let $I(x) = \{\text{functions that vanish on } x\}$.

Theorem 3.5.9. $I(x) = \sqrt{\mathfrak{a}}$

Let $A = k[x_1, \ldots, x_n]/\mathfrak{a}$. This is equivalent to

Theorem 3.5.10. *Let $f \in A$ be an element that vanishes at every closed point in* Spec$A$*, then $f \in \mathrm{Nil}(A)$.*

Proof of Theorem 2. We know $\mathrm{Nil}(A) = \bigcap_{p \text{ prime}} p$. We want $\mathrm{Nil}(A) = \bigcap_{m \text{ maximal}} m$. It is clear that "$\subset$" holds. Let $f \in A$, and $f \notin \mathrm{Nil}(A)$. Then there exists $\mathfrak{p}$ prime such that $f \notin \mathfrak{p}$. We have the maps:

$$A \longrightarrow A/\mathfrak{p} = B \longrightarrow B\left[\frac{1}{\overline{f}}\right] = C,$$

where $A \ni f \longmapsto \overline{f} \in B$, $\overline{f} \neq 0$. Let m be a maximal ideal of C, then $C/m = k$ by Hilbert's Nullstellensatz. Let $\phi : C \to k$ be the composition:

$$\phi : A \longrightarrow C \longrightarrow C/m = k$$

Then $\phi\colon A \to k$ is surjective, $\phi(f) \neq 0$, $f \notin \ker \phi$ but $\ker \phi$ is maximal and we are done. $\square$

Example 3.5.11. Note the above theorem is only true when A is a k-algebra of finite type. Consider the following:

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \;\middle|\; p \nmid n \right\}.$$

Then $\mathbb{Z}_{(p)}$ has a single non-zero ideal $p \cdot \mathbb{Z}_{(p)}$, $\mathbb{Z}_{(p)}/p \cdot \mathbb{Z}_{(p)} = \mathbb{F}_p$ and $\mathrm{Nil}(A)$ is not equal to the intersection of maximal ideals m.

Exercise 3.5.12. Let $f_1, \ldots, f_m$ be polynomials in $k[x_1, \ldots, x_n]$. Assume that the equations $f_1 = 0, \ldots, f_m = 0$ have no common solutions, then $f_1, \ldots, f_m$ generate $k[x_1, \ldots, x_n]$.

3.6 Dimension

We have our usual notion of dimension:

- a line is 1-dimensional
- a plane is 2-dimensional
- a space is 3-dimensional.
- $\dim \mathbb{A}^n_k = n$.

The dimension measures how much freedom do you have, or equivalntly, how many constrains you may have. If a space X has dimension n, then for generic $n+1$ functions $f_1, \ldots, f_{n+1}$ the system $f_1 = f_2 = \ldots = 0$ should not have solutions, but any n of them will have solutions. If an irreducible space X has dimension n then consider the chain of subvarieties

$$Y_1 \supsetneq Y_2 \supsetneq \ldots \supsetneq Y_m,$$

where Y_i are integral (irreducible), $Y_i \neq X$, the maximal length of chains is n.

Definition 3.6.1. Let X be a topological space. We say X is Noetherian if any descending chain of closed subsets of X is finite. Equivalently for any chain

$$Y_1 \supseteq Y_2 \supseteq \ldots \supseteq Y_n \supseteq \ldots,$$

there is a N such that $Y_m = Y_N$ for $m \geq N$.

Exercise 3.6.2. Spec$A$ is Noetherian if A is Noetherian.
Hint: Since $Y_i = Z(I_i)$ and $I_i = \sqrt{I_i}$, then $Y_1 \supset Y_2 \supset \dots$ if and only if $I_1 \subsetneq I_2 \subsetneq I_3 \dots$. But one can find $n < \infty$ such that

$$\bigcup_{i=1}^{\infty} I_i = \bigcup_{i=1}^{n} I_i.$$

Proposition 3.6.3. *Let X be a Noetherian space. Let $Y \subset X$ be a closed subset, then Y is a finite union of irreducible closed subsets Y_i, $i = 1, \dots, m$. This union is unique if we require $Y_i \subsetneq Y_j$ for $i \neq j$.*

Proof. Let S be the set of closed subsets of X which cannot be written as a finite union of irreducible closed proper subsets. We want to show $S = \emptyset$. Assume $S \neq \emptyset$, then since X is Noetherian, S will have a minimal element Y. If Y is irreducible we are done. If not $Y = Y_1 \cup Y_2$ where $Y_1 \subsetneq Y \supsetneq Y_2$, so either Y_1 or Y_2 must be in S, so either Y_1 or Y_2 gives an element in S which is smaller than Y. This contradiction concludes the proof. □

Definition 3.6.4. Let X be a space which is finite union of irreducible subspaces X_i ($i = 1, \cdot, n$) such that $X_i \subsetneq X_j$ if $i \neq j$. Then we call X_i the irreducible components of X.

Definition 3.6.5. Let X be a Noetherian space. The *dimension* $\dim X$ of X is the maximal length of chains of irreducible closed subsets which are not irreducible components of X.

Proposition 3.6.6. *Let $X = \mathrm{Spec}A$ where A is Noetherian. Then $\dim X$ is equal to the maximal length of chains $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots \supseteq \mathfrak{p}_m$, where $\mathfrak{p}_i$ is a non-maximal prime ideal of A.*

Proof. The proof is left to the reader as an exercise. □

Example 3.6.7. We have $\dim \mathrm{Spec}\,\mathbb{Z} = 1$. If k is a field, we obtain $\dim \mathrm{Spec}\,k = 0$, $\dim \mathrm{Spec}\,k[x] = 1$, $\dim \mathrm{Spec}\,k[x_1, \dots, x_n] = n$, and $\dim \mathrm{Spec}\,\mathbb{Z}[x_1, \dots, x_{n-1}] = n$. The case where $n \geq 2$ is tricky and we will examine this in the next lecture.

Now let k be an algebraically closed field and let A be an integral domain of finite type over k. Let

$$K = \text{the fractions of } A = k\left[\frac{1}{A - \{0\}}\right],$$

then K/k is a field extension of finite type.

Definition 3.6.8. The transcendental dimension of $X = \mathrm{Spec}(A)$ relative to k is the transcendental degree tr_A of (K/k) which is the cardinality r of any subset $\{x_1, \cdots, x_r\}$ of K with the following properties:

1. $x_1, \dots, x_r$ are algebraically independent.
2. every element $x \in K$ is algebraic over $k(x_1, \cdots, x_r)$.

This definition makes sense because r does not depend on the choice of $x_1, \dots, x_r$.

Theorem 3.6.9. $\dim X = \mathrm{tr}_K \dim X$.

Proof. Step 0: If one side equals 0 *then the other side also equals* 0.

a) If $\dim X = 0$, 0 is the only ideal of A, so A is a field. Thus from the Hilbert Nullstellensatz A is an algebraic extension of k, so $A = k$. Therefore $\mathrm{tr}_k \deg K = \mathrm{tr}_k \deg k = 0$.

b) If $\mathrm{tr}_k \dim X = 0$ (K/k is algebraic) then $K = k$, $k \subset A \subset k = \overline{k}$, so $A = k$.

Step 1: $\dim X \leq \mathrm{tr} \dim X$

$$X = \mathrm{Spec} A, \qquad 0 \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

. We have $A \twoheadrightarrow A/\mathfrak{p}_0 \twoheadrightarrow A/\mathfrak{p}_1 \twoheadrightarrow \ldots$. Thus $\mathrm{tr}\deg A_i \geq \mathrm{tr}\deg A_{i+1}$, where $A_i = A/\mathfrak{p}_i$. We need only to show that $\mathrm{tr}\deg A_i \neq \mathrm{tr}\deg A_{i+1}$. So the first step is reduced to the following

Lemma 3.6.10. *Let A be an integral k-algebra of finite type. Let $\mathfrak{p} \subseteq A$ be a non-zero prime ideal. Then* $\mathrm{tr}\deg A \neq \mathrm{tr}\deg A/\mathfrak{p}$.

Proof. Assume $\mathrm{tr}\deg A = \mathrm{tr}\deg A/\mathfrak{p} = r$. Write $A = k[x_1, \ldots, x_n]$ with $x_1, \ldots, x_r$ algebraically independent over k. Let $S = k[x_1, \ldots, x_r] - (0)$. The assumption implies $S \cap \mathfrak{p} = \emptyset$. Therefore

$$S^{-1}A \overset{\neq}{\twoheadrightarrow} S^{-1}\big(A/\mathfrak{p}\big), \qquad S^{-1}A = k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n].$$

Claim: $S^{-1}A$ is a field.

Lemma 3.6.11. *Let L be a field with A/L an integral algebra which is finite dimensional as an L-vector space. Then A is a field*

Proof. Let $X \in A - \{0\}$. The set $\{1, x, x^2, \ldots, x^n, \ldots\}$ must be linearly dependent so $\sum_{n=0}^{m} a_n x^n = 0$ for some $m > 0$ and $a_n \in L$ which are not all 0. By eliminating x's we may assume $a_0 \neq 0$. We have

$$a_0 + x(a_1 + a_2 x + \ldots) = 0 \qquad \text{or} \qquad \frac{x(a_1 + a_2 x + \ldots)}{-a_0} = 1.$$

Therefore x is invertible so A is a field. Now since $S^{-1}A$ is a field, the homomorphism to $S^{-1}(A/\mathfrak{p})$ must be injective as it is nonzero, so must be bijective as it is already surjective. This is a contradiction! □

Exercise 3.6.12. Let S be a multiplicative system of R. Let $\mathfrak{p}$ be a prime ideal of R such that $S \cap \mathfrak{p} = 0$. Prove that

1) $S^{-1}\mathfrak{p}$ is a prime in $S^{-1}A$;

2) $S^{-1}(A/\mathfrak{p}) = S^{-1}A/S^{-1}\mathfrak{p}$;

3) $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$.

Step 2: $\dim X \geq \operatorname{tr}\dim X$. We will do this by induction on $\operatorname{tr}\dim X$. If $\dim X = 0$ then we are done from Step 0. Assume $\operatorname{tr}\dim X = n > 0$ and $\operatorname{tr}\dim X \leq \dim X$ is true for varieties with dimension less than n. $A = k[x_1, \ldots, x_m]$. Assume x_1 is transcendental over k. $S = k[x_1] - (0)$. Let $k' = k(x_1)$, let

$$B = S^{-1}A = k'[x_2, \ldots, x_m],$$

then

$$\operatorname{tr}_{k'}\dim B = \operatorname{tr}_{k'}\dim B - 1 = n - 1.$$

By the induction hypothesis there is a chain of primes in B of length $n-1$

$$0 \subsetneq Q_1 \subsetneq Q_2 \subsetneq \ldots \subsetneq Q_{n-1}$$

Intersect this chain with A:

$$0 \subsetneq P_1 \subsetneq P_2 \subsetneq \ldots \subsetneq P_{n-1}, \qquad P_i = Q_i \cap A.$$

Exercise 3.6.13. Show that $P_i \neq P_{i+1}$, $S^{-1}P_i = Q_i$, $P_i \cap S = \emptyset$.

Claim: P_{n-1} is not maximal (This will imply $\dim X \geq n$). Otherwise, A/P_{n-1} is a field then by the Hilbert Nullstellensatz $A/P_{n-1} = k$. By the above exercise, $P_{n-1} \cap S = \emptyset$, thus the composition map

$$k[x_1] \longrightarrow A \longrightarrow A/\mathfrak{p} = k$$

is injective. This is impossible as x_1 is transendental over k. The second step is proved. □

The Theorem is proved. □

Exercise 3.6.14. $\dim \mathbb{A}^n_k = n$. Moreover any maximal chain of non-zero ideals in A will have length n. Proved this fact as an exercise. (*Hint*: Look the proof of Theorem 3.6.9)

Example 3.6.15. Non-zero prime ideals in $k[x_1, x_2]$ are of two types:

1. $(f(x_1, x_2))$, where $f(x_1, x_2) \neq 0$ ireeducible;
2. $(x_1 - a_1, x_2 - a_2)$.

Remark 3.6.16. If $k \neq \overline{k}$ Theorem 1 is still true by the same proof.

Remark 3.6.17. Let A be an integral algebra over $\mathbb{Z}$ of finite type

$$\mathbb{Z} \xrightarrow{i} A, \quad \text{where} \quad i(\mathbb{Z}) = \begin{cases} \mathbb{Z}, & \text{case 1} \\ \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p & \text{case 2} \end{cases}$$

If k is the fractions of A then either $\mathbb{Q} \subseteq k$ or $\mathbb{F}_p \subseteq k$.

Exercise 3.6.18. If $i(\mathbb{Z}) = \mathbb{Z}$ then $\dim X = 1 + \mathrm{tr}_{\mathbb{Q}} \dim k$. (Hint: First try to prove the identity when one side equals 1. You will need the following exercise)

Exercise 3.6.19. Let B be Noetherian and integral domain. Let A be an integral algebra over B which is of finite type as an A-module. Then B is a field if and only if A is a field.

Exercise 3.6.20. Let A be an integral algebra of finite type over a field or over $\mathbb{Z}$. Let $f \in A$ an non invertible element. Then

$$\dim A/fA = \dim A - 1.$$

Chapter 4

Projective Varieties

4.1 Projective spaces

1. We know that $\mathbb{C}$ is not compact and it can be compactified by adding a point ∞ to the plane $\mathbb{C}$ to obtain the Riemann sphere $\widehat{\mathbb{C}}$. One good thing about Riemann sphere is the "summation formula" and "degree formula": if $\psi(z) = \dfrac{f(z)}{g(z)}$ then

$$\sum_P \mathrm{ord}_P \psi = 0, \qquad \deg \psi = -\mathrm{ord}_\infty \psi.$$

Riemann sphere is the projective line over complex numbers. It is can be considered as the set of lines in $\mathbb{C}^2$ passing through the origin. Let x_0, x_1 be the coordinates of $\mathbb{C}^2$ then a point $z \in \mathbb{C}$ corresponds to the line $zx_0 - x_1 = 0$ while ∞ corresponds to the line $x_0 = 0$. We may replace $\mathbb{C}$ by any algebraically closed field k to define projective line $\mathbb{P}^1_k$ over k.

2. Let k be an algebraically closed field k. The projective plane $\mathbb{P}^2_k$ is a sort of compactification of affine plane (there are more than one way to compactify affine plane, unlike the case of affine line):

$$\mathbb{A}^2_k \hookrightarrow \mathbb{P}^2_k, \qquad \mathbb{P}^2_k = \mathbb{A}^2_k \cup \mathbb{P}^1_k = \mathbb{A}^2_k \cup \mathbb{A}^1_k \cup \mathbb{A}^0_k.$$

More precisely, the projective plane $\mathbb{P}^2_k$ is defined to be the set of lines in $\mathbb{A}^3_k$ passing through the origin. Let $P = (x_0, x_1, x_2)$ be a nonzero point in $\mathbb{A}^3_k$ then it defines a line $[P]$ in $\mathbb{P}^2_k$ passing through both P and origin. We call (x_0, x_1, x_2) the homogenuous coordinate of $[P]$. Of course the homogenuous coordinates for a point in projective line is not unique but they are propotional by elements by nonzero elements in k. In the above decomposition,

- $\mathbb{A}^2_k$ corresponds to $x_0 \neq 0$,
- $\mathbb{A}^1_k$ coresponds to $x_0 = 0$ but $x_1 \neq 0$,
- A^0_k corresponds to $x_0 = x_1 = 0$ but $x_3 \neq 0$,
- $\mathbb{P}^1_k$ corresponds to $x_0 = 0$.

One advantage for projective plane than affine plane is to solve system of equations. Let $f(x,y)$ and $g(x,y)$ are two polynomials over a field k. Then the system of equations

$$\begin{cases} f(x,y)=0, \\ g(x,y)=0 \end{cases}$$

has the number of common solutions $\leq \deg f \cdot \deg g$ in affine plane $\mathbb{A}_k^2$.

If you introduce homogeneous coordinates $x = x_1/x_0$, $y = x_2/x_0$. We have homohenuous polynomials

$$F(x_0,x_1,x_2) = f\left(\frac{x_1}{x_0},\frac{x_2}{x_0}\right)\cdot x_0^{\deg f}, \quad G(x_0,x_1,x_2) = g\left(\frac{x_1}{x_0},\frac{x_2}{x_0}\right)\cdot x_0^{\deg g}.$$

and new system of equations

$$F(x_0,x_1,x_2)=0 \ \text{ and } \ G(x_0,x_1,x_2)=0.$$

This system has same set of solutions on $\mathbb{A}_k^2$ as that of $f=g=0$ but this new set of solutions has cardinality exactly equal to $\deg f \cdot \deg g$.

Definition 4.1.1. Let n be a nonnegative integer and let k be an algebraically closed field. The n-dimensional projective space $\mathbb{P}_k^n$ is defined to be the set of lines in $\mathbb{A}_k^{n+1}$ passing through the orign.

The only good functions on $\mathbb{P}_k^2$ are constants, but $\mathbb{P}_k^2$ has a lot of homogeneous "functions" $F(x,y,z)$ which are polynomials whose nonzero monomilas have same degree. The polynomial $F(x,y,z)$ is not really a function unless is a constant, but $F(x,y,z)/G(x,y,z)$ is a meromorphic function if $\deg F = \deg G$. All homogeneous functions form a graded algebra

$$A = k[x,y,z] = k \oplus (kx \oplus ky \oplus kz) \oplus A_2 \oplus A_3 \oplus \ldots,$$

where A_n = homogeneous polynomials of degree n. There is a map $\mathbb{P}_k^2 \longrightarrow$ "ideals of A",

$$[a_0 : a_1 : a_2] \longrightarrow (a_1x_0 - a_0x_1, a_2x_0 - a_0x_2, a_2x_1 - a_1x_2).$$

4.2 Projective Spectra

Definition 4.2.1. By a graded algebra over R we mean an R-algebra with a decomposition $A = \bigoplus_{n\geq 0} A_n$, such that $R \subset A_0 = R$ and that $A_i \cdot A_j \hookrightarrow A_{i+j}$. We write $A_+ = \bigoplus_{n\geq 1} A_n$ which is an ideal of A.

Definition 4.2.2. Let A be a graded algebra over R. By a homogeneous ideal of A we mean an ideal $\mathfrak{p}$ of A which can be decomposed as $\mathfrak{p} = \bigoplus_{n\geq 0} P_n$ and $P_n \subseteq A_n$. Or equivalent $\mathfrak{p}$ is an ideal with the following property:

$$\begin{cases} f = \sum_n f_n \in \mathfrak{p}, \\ f_n \in A_n \end{cases} \quad \Longrightarrow f_n \in \mathfrak{p}$$

Definition 4.2.3. Let A be a graded ring over R. The *projective spectrum of* A is defined to be the set of homogeneous prime ideals in A which do not contain A_+, and is denoted by $\mathrm{Proj}A$.

Example 4.2.4. $A = R \oplus 0$ then $\mathrm{Proj}A = \emptyset$.

Example 4.2.5. $\mathrm{Proj}k[T] = \{0-\text{ideal}\}$.

Example 4.2.6.

$$\mathrm{Proj}\mathbb{C}[T_0, T_1] = \{0 - \text{ideal}\} \cup \left\{(aT_0 + bT_1) \colon a, b \in \mathbb{C}^2, a, b \neq 0\right\} = \mathbb{A}^1 \cup \{\infty\}$$

Indeed, every prime ideal in $\mathbb{C}[T_0, T_1]$ has the one of following three forms:

1. (0),
2. (f), where f is nonzero and irreducible,
3. $(T_0 - a, T_1 - b)$, where $a, b \in k$.

The first one is of course homogeneous. The second one is homogeneous only if $f = aT_0 - bT_1$. The third one is homogeneous only if $a, b = 0$. But then it contains A_+ so its not acceptable.

Since $\mathrm{Proj}A \subset \mathrm{Spec}A$ we can define the *Zariski Topology*: let I be homogeneous

$$Z(I) = \{\mathfrak{p} \in \mathrm{Proj}A \colon \mathfrak{p} \supseteq I\}$$
$$Z(I) = \{\text{the zeroes of functions in } I\}$$

Exercise 4.2.7. Prove that the above defined map from $\mathbb{P}^2_k$ to the set of ideals of $A = k[x_0, x_1, x_2]$ actually defined a map to $\mathrm{Proj}A$. Show that the image of this map is the set of closed point in $\mathrm{Proj}A$. (Recall that a point p in a topological space X is called closed if the subset $\{p\}$ is closed.)

Proposition 4.2.8. *If A is Noetherian then $\mathrm{Proj}A$ is Noetherian.*

The proof is left to the reader as an exercise.

Proposition 4.2.9. *Let A be a graded algebra over R ($A_0 = R$) then A is Noetherian if and only if the following two conditions are verified:*

1. *R is Noetherian;*
2. *A is finitely generated over R.*

Proof. The *if* part is clear by the Hilbertbasis theorem. Now assume A is Noetherian. A_+ is an ideal in A and is finitely generated as an A-module, so $A/A_+ \cong R$ must be Noetherian, $A_+ = \sum_{i=1}^{n} Ax_i$, where x_i are homogeneous, $\deg x_i \geq 1$.

Claim: $A = R[x_1, \ldots, x_n]$. It is suffice to show $A_m \subset R[x_1, \ldots, x_n]$ for every m. One then proceed by induction on m. It is clear if $m = 0$. Now assume that $m > 0$ and that $A_\ell \subset R[x_1, \cdots, x_n]$ for $\ell < m$. Since $A_+ = \sum_{i=1}^{\infty} Ax_i$, then

$$A_m = \sum_{i=1}^{n} A_{m-\deg x_i}\, x_i \subset \sum_{i=1}^{m} R[x_1, \ldots, x_n]x_i \subset R[x_1, \ldots, x_n]$$

where $A_n = 0$ if $n < 0$. □

Exercise 4.2.10. Let A be a graded algebra and $\mathfrak{m}$ is a homogenous ideal not including A_+. Then $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m} \cong k[t]$ where k is a field and $k \cong A_0/(A_0 \cap \mathfrak{m})$.

Assume $A_0 = k = \overline{k}$, then we have a map $\mathbb{P}^n(k) \to \mathrm{Proj}k[x_0, \ldots, x_n]$ via

$$(a_0, \ldots, a_n) \longrightarrow (a_j x_i - a_i x_j,\ i, j = 0, \ldots, n).$$

Exercise 4.2.11. Show this map is continuous with image the set of closed points.

Affine decomposition of $\mathrm{Proj}A$

For $f \in A$, f homogeneous, define

$$D(f) = \{\mathfrak{p} \in \mathrm{Proj}A\colon f(\mathfrak{p}) \neq 0 \text{ where } f(\mathfrak{p}) = \text{the image of } f \text{ in } A/\mathfrak{p}\,\}.$$

Then we have $\mathrm{Proj}A = \bigcup D(f)$ where $f \in A_+$, f homogeneous. Now $A[1/f]$ is a homogeneous ring. Let $A_{(f)}$ be the degree 0 part of $A[1/f]$,

$$A_{(f)} = \left\{ \frac{g}{f^n},\ \deg g = n \deg f \right\}.$$

Exercise 4.2.12. $D(f) \cong \mathrm{Spec}A_{(f)}$.

Example 4.2.13. Let $S = k[x_0, \cdots, x_n]$. Then S_+ is generated by $x_0, \cdots, x_n$.

$$\mathrm{Proj}S = \bigcup_{i=0}^{n} D(x_i), \quad \text{where} \quad D(x_i) = \mathrm{Spec}k\left[\frac{x_j}{x_i},\ 0 \leq j \leq n\right].$$

We may also have the similar decomposition for the projective space of dimension n:

$$\mathbb{P}^n(k) = \left(k^{n+1} - \{0\}\right) / \sim\ = \bigcup_{i=0}^{n} D(x_i),$$

where

$$D(x_i) = \{(a_0, \ldots, a_n)\colon a_i \neq 0\}/\sim\ = \{(a_0, \ldots, a_n)\colon a_i = 1\}/\sim\ \simeq \mathbb{A}_k^n.$$

4.3 Hilbet Polynomial

Assume that $A = \bigoplus_{n\geq 0} A_n$ is Noetherian and that $A_0 = k$ is a field. Then A is generated by homogeneous elements and each A_n is finite dimensional vector space over k. Consider the following formal series

$$Q(T) = \sum_{m\geq 0} \dim_k A_m T^m.$$

Theorem 4.3.1. *Assume $x_1, \ldots, x_n$ has degree $d_0, \ldots, d_n$ where $d_i = \deg x_i$, then we have the following identity of the formal power series*

$$Q(T) = \frac{R(T)}{\prod_{i=1}^{n}(1 - T^{d_i})}$$

where $R(T)$ is a polynomial.

Example 4.3.2.

1) In the case $n = 0$ we have $\dim A_n = 1$ if $n = 0$ and $\dim A_n = 0$ if $n > 0$. Thus

$$A = k \oplus 0 \oplus 0 \oplus 0 \oplus \ldots, \qquad Q(T) = 1.$$

2) In the case $n = 1$, $A = \sum_{m\geq 0} kx^m$, assume that $x^m \neq 0$ for all m, then

$$Q(T) = \sum_{n=0}^{\infty} T^n = \frac{1}{1-T}.$$

3) If $A = k[x_1, \ldots, x_n]$ is a polynomial ring of variable of x_i, then,

$$\begin{aligned} Q(T) = \sum \dim A_m \cdot T^m &= \sum_m \sum_{i_1 i_2 \ldots i_n = m} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \cdot T^n \Big|_{x_1 = x_2 = \ldots = x_n = 1} \\ &= \sum_{i_1, \ldots, i_n} (x_1 T)^{i_1} \ldots (x_n T)^{i_n} \Big|_{x_i = 1} = \prod_{j=1}^{n} \frac{1}{1 - x_j T} \Big|_{x_j = 1} = \frac{1}{(1-T)^n}. \end{aligned}$$

By looking at $\dfrac{1}{1-T} = \sum_{i\geq 0} T^i$ and differentiating both sides $n-1$-times we get

$$\dim A_m = \binom{m+n-1}{n-1}$$

.

Now we go back to the proof of Theorem 1. First let us generalize the Theorem to modules:

Theorem 4.3.3. *Let M be a graded A-module of finite type. Write $Q_M(T) = \sum \dim M_n \cdot T^n$. Then*

$$Q_M(T) = \frac{R_M(T)}{\prod_{i=1}^{n}(1 - T^{d_i})}$$

where $R_M(T)$ is a polynomial.

We are going to prove the theorem on the number n of generators of A. Write $A = k[x_1, \ldots, x_n]$. If $n = 0$ then $A = k$. As $M = \bigoplus_{i=0}^{\infty} M_i$ is finite dimensional space, $M_i = 0$ for $i \gg 0$. It follows that $Q_M(T)$ is a polynomial. Assume $n > 0$ and the above theorem is true for modules over a graded ring with less than n homogeneous elements. We have a map which gives the exact sequence:

$$0 \longrightarrow \ker x_0 \longrightarrow M \xrightarrow{x_0} M \longrightarrow M/x_0M \longrightarrow 0. \tag{4.3.1}$$

What do we mean by exact sequence?

Definition 4.3.4. A sequence is chain of modules and homomorphisms:

$$M_0 \xrightarrow{d_0} M_1 \xrightarrow{d_1} \ldots \xrightarrow{d_n} M_{n+1},$$

which is called exact if $\ker(d_i) = \mathrm{im}(d_{i-1})$ for every $i \geq 1$.

Example 4.3.5. If $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact if and only if the following are satisfied:

1. $M_1 \to M_2$ is injective, thus we may consider M_1 as a submodule;
2. $M_2 \to M_3$ is surjective, thus we may consider M_3 as a quotient module of M_2;
3. $M_2/M_1 = M_3$.

This sequence is called a *short exact sequence*. Assume now that M_i are k-vector spaces, show that $\dim M_2 = \dim M_1 + \dim M_3$.

Exercise 4.3.6. For a long exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \ldots \longrightarrow M_n \longrightarrow 0$$

prove that $\sum_i (-1)^i \dim M_i = 0$.

Back to the proof of the above theorem. Taking homogeneous components of formula (1) and applying the inclusion $A_m \cdot M_n \subset M_{n+m}$, we obtain for each n the following exact sequence

$$0 \longrightarrow \ker(x_1)_n \longrightarrow M_n \longrightarrow M_{n+d_1} \longrightarrow \Big(M \Big/ x_1M\Big)_{n+d_1} \longrightarrow 0,$$
$$\dim(\ker(x_1))_n - \dim M_n + \dim M_{n+d_1} - \dim\Big(M \Big/ x_1M\Big)_{n+d_1} = 0.$$

By multiplying this by T^{n+d_1} and summong over n we get

$$T^{d_1}Q_{\ker x_1}(T) \quad - \quad T^{d_1}Q_M(T) \quad + \quad Q_M(T) \quad - \quad Q_{M/x_1M}(T) \quad - \quad R_1(T) \qquad = \qquad 0,$$

where

$$R_1(T) = \sum_{i=1}^{d_1-1} (\dim M_i - \dim(M/x_1M)_i) \cdot T^i.$$

Solving $Q_M(T)$, we obtain

$$Q_M(T) = (1 - T^{d_1})^{-1} \left[-Q_{\ker x_1}(T) + Q_{M/x_1M}(T) + R_1(T) \right]. \tag{4.3.2}$$

Now $\ker(x_1)$ is a module of $k[x_1, \ldots, x_n]/(x_1) = k[x_2, \ldots, x_n]$. So is M/x_1M. Thus by induction $Q_{\ker(x_1)}(T)$ and $Q_{M/x_1M}(T)$ are both of the form

$$\frac{\text{Polynomial}}{\prod_{i=2}^{n}(1 - T_i^{d_i})}.$$

Thus formula (2) implies that $Q_M(T)$ has the form

$$\frac{\text{Polynomial}}{\prod_{i=1}^{n}(1 - T_i^{d_i})}.$$

This completes the proof of the above theorem.

Theorem 4.3.7. *If we assume $d_1 = \ldots = d_n = 1$ then there is a polynomial $P_M(T)$ with rational coefficients such that*

$$\dim M_m = P(m)$$

for m sufficientely large.

Proof. By Theorem 2, $Q_A(T) = R_A(T)/(1 - T)^n$. Write

$$\frac{1}{(1-T)^n} = \sum_{m=0}^{\infty} \binom{m+n-1}{m} T^m, \qquad P_A(T) = \sum_{i=0}^{\ell} a_i T^i.$$

Assume $a_n = 0$ for $n < 0$ then

$$\dim A_m = \sum_{i=0}^{\ell} a_{m-i} \binom{n+i-1}{i}.$$

This is of course a polynomial of n when $m \geq \ell$. □

Definition 4.3.8. The polynomial $P_M(T)$ is called *the Hilbert polynomial* of M.

4.4 Dimensions

Let S be a Noetherian graded ring with $S_0 = k$ a field. $S = \bigoplus_{n\geq 0} S_n$, $S_+ = \bigoplus_{n>0} S_n$. Assume S is Noetherian then $\dim S_n < \infty$. $Q_S(T) = \sum_{n\geq 0} \dim S_n \cdot T^N$. If S is generated over K by homogeneous elements $x_0, \ldots, x_n$ with degrees $d_0, \ldots, d_n$ then

$$Q_S(T) = \frac{R_S(T)}{\prod_{i=0}^{n}(1 - T^{d_i})}.$$

We thus have the formula to compute $\dim S_n$. Let $P_S(n) = \dim S_n$. If $d_0 = d_1 = \ldots = d_n = 1$ then $P_S(n)$ is a polynomial for $n \gg 0$.

Theorem 4.4.1. $\deg P_S(T) = \dim \operatorname{Proj} S$

Notice that $\dim \operatorname{Proj} S$ is the maximal length of chains of non-maximal homogeneous prime ideals. The proof uses two kinds of techniques. One is using inductions. Thus it is more convenient to work with language of modules. So we want to generalize the theorem to modules. Let M be a finitely generated and graded S-module. Let $\operatorname{Ann}(M)$ denote the annihilater of M, i. e.

$$\operatorname{Ann}(M) = \{x \in S \colon x \cdot M = 0\}.$$

M can be thought of as an $S/\operatorname{Ann}(M)$-module. We have a diagramm

$$\begin{array}{ccc} M & & M \\ \downarrow & & \downarrow \\ \operatorname{Proj}\big(S/\operatorname{Ann}(M)\big) & \hookrightarrow & \operatorname{Proj}(S) \\ || & & \\ \operatorname{Supp}(M) & & \end{array}$$

where $\operatorname{Supp}(M)$ is the support of M.

Definition 4.4.2. $\dim(M) = \dim \operatorname{Supp}(M) = \dim\big(S/\operatorname{Ann}(M)\big)$.

Exercise 4.4.3.

$$\operatorname{Supp}(M) = \left\{\wp \in \operatorname{Proj} S : \quad M_\wp = (S - \wp)^{-1} M \neq 0.\right\}.$$

Theorem 4.4.4. $\dim(M) = \deg P_M(T)$.

(Recall $M = \bigoplus M_n$, $\dim M_n = P_M(n)$.)

Lemma 4.4.5. *If M fits in an exact sequence*

$$0 \to M_1 \to M \to M_2 \to 0$$

and the Theorem is true for both M_1 and M_2 then the Theorem is true for M.

This follows from the following idenities:

$$\dim M = \max\Big(\dim M_1, \dim M_2\Big) \tag{4.4.1}$$

$$\deg P_M = \max\Big(\deg P_{M_1}, \deg P_{M_2}\Big). \tag{4.4.2}$$

These idenities follows from the following facts:

$$\dim M = \dim M_1 + \dim M_2 \qquad P_M = P_{M_1} + P_{M_2}$$

$$\mathrm{Ann}(M) = \mathrm{Ann}(M_1) \cap \mathrm{Ann}(M_2).$$

The second technique is to decompose modules back to rings as dimension of a module is really defined through some ring.

Proposition 4.4.6. *Let R be a Northerian ring and let M be a R-module of fnite type. Then N has a filtration: $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M$ such that $M_i/M_{i-1} \cong (R/\mathfrak{p})$ where $\mathfrak{p}$ is a prime ideal of S.*

Proof. We starts with the following:

Lemma 4.4.7. *If M is not zero, then there is an element $m \in M$, $m \neq 0$, such that $\mathrm{Ann}(m) = \{x \in R : \qquad x \cdot m = 0\}$ is a prime ideal.*

Proof. Consider the set of ideals $T = \{\mathrm{Ann}(m), m \neq 0, m \in M\}$. Let $\mathrm{Ann}(m)$ be a maximal element in in T. Then we claim $\mathrm{Ann}(m)$ is prime. Assume $ab \in \mathrm{Ann}(m)$ and $a \notin \mathrm{Ann}(m)$. Then $abm = 0$ but $am \neq 0$. It follows that

$$\mathrm{Ann}(am) \in T, \quad \mathrm{Ann}(m) \subseteq \mathrm{Ann}(am).$$

Since $\mathrm{Ann}(m)$ is maximal, $\mathrm{Ann}(m) = \mathrm{Ann}(am)$. Thus $b \in \mathrm{Ann}(m)$ so we are done. □

Now we go back to proof of the Proposition. If $M = 0$ we are done. Otherwise by the above lemma, M contans a submodule $M_1 := Rx$ isomorphic to $R/\wp_1$. Again we are done if $M = M_1$. Otherwise we applying the above lemma to M/M_1 to obtain a submodule M_2 such that M_2/M_1 (as a submodule of M/M_1) is isomorphic $R/\wp_2$. Continueing this procedure, we have that either the proposition is true, or there is an infinite sequence of distinct submodules $0 \subset M_1 \subset \cdots \subset M_i \subset$. But this is impossible as R is Noetherian. □

Lemma 4.4.8. *Assume that S is generated by S_1. Then*

$$\dim \mathrm{Proj}S = \dim \mathrm{Spec}S - 1.$$

Proof. First we need to reduce to the integral domain. In fact since S is Noetherian, it has finitely many minimal prime ideals $\wp_i$. It is easy to show that these are homogenous since the subset $\wp_i'$ of homogenous elements in each $\wp_i$ is also a prime ideal. Thus we have $\mathrm{Proj}S = \cup_i \mathrm{Proj}(S/\wp_i)$ and $\mathrm{Spec}S = \cup_i \mathrm{Spec}S/\wp_i$.

Assume now that S is integral. To see this last identity, we notice that $\dim \mathrm{Spec}S$ is the transcendental degree of S over k. Denote this number by r. But $\mathrm{Proj}S$ is the covering of $\mathrm{Spec}A_i$ $(i = 0, 1, \cdots, n)$, where $A_i = k[x_i/x_j, i = 0, \cdots, n]$. Thus $\dim \mathrm{Proj}S$ is the maximal dimension of A_i's or equivalently, the transcendental degree of A_i's. We claim that the transcendental degree of each A_i over k is equal to $r - 1$. We may assume that $i = 0$. As $x_0 \notin k$, x_0 is transcendental over k. Thus S has a base consisting of elements of x_i's including x_0. We may assume this base is $\{x_0, \cdots, x_r\}$. Then it is easy to show that $\{x_1/x_0, \cdots, x_r/x_0\}$ forms a transcendental base for A_0 over k. □

We also want to define a third invariant $\delta(S)$.

Definition 4.4.9. $\delta(S)$ is the minimal number of elements $y_1, \ldots, y_l \in S_1$ such that $S/\sum y_i S$ is a finite dimensional k-vector space.

Theorem 4.4.10. $\dim S = \deg P + 1 = \delta(S)$.

A generalization: Let M/S be a module of finite type with M graded, we define S_M to be $S/Ann(M)$ where $\mathrm{Ann}(M) = \{x \in S \colon xM = 0\}$, and $\delta(M)$ to be the minimal number of $x_1, \ldots, x_m \in S$ such that $M/\sum x_i M$ is of finite length.

Theorem 4.4.11. $\dim S_M = \deg P_M + 1 = \delta(M)$.

Proof. We'll do the proof in three steps:
Step 1: $\deg P_M + 1 \geq \dim S_M$.
Step 2: $\delta(M) \geq \deg P_M + 1$.
Step 3: $\dim S_M \geq \delta(M)$.

Step 1 : $\deg P_M + 1 \geq \dim S_M$

First let us consider the case $M = S$. We use induction on $\dim S$. If $\dim S = 0$ we are done. Assume $\dim S > 0$. Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \ldots \subsetneq \mathfrak{p}_r$ be a chain of prime ideals in S_1, $r - 1 = \dim S > 0$. Let $x \in \mathfrak{p}_2 - \mathfrak{p}_1$,

$$0 \longrightarrow S/\mathfrak{p}_1 \xrightarrow{x} S/\mathfrak{p}_1 \longrightarrow S/(xS + \mathfrak{p}_1) \longrightarrow 0.$$

Because $r - 1 = \dim S$,

$$\dim S/(\mathfrak{p}_1 + xS) = \dim S - 1 = \dim S/\mathfrak{p}_1 - 1.$$

From the exact sequence,

$$\dim\big(S/\mathfrak{p}_1\big)_n = \dim\big(S/\mathfrak{p}_1\big)_{n-\deg x} + \dim\big(S/(xS + \mathfrak{p}_1)\big)_n.$$

Thus

$$P_{S/\mathfrak{p}_1}(T) = P_{S/\mathfrak{p}_1}(T - \deg x) + P_{S/(xS+\mathfrak{p}_1}(T).$$

So

$$\deg P_{S/(\mathfrak{p}_1+xS)} \leq \deg P_{S/\mathfrak{p}_1} - 1 \leq \deg P_S - 1.$$

Now by induction $\deg S/(\mathfrak{p}_1 + xS) \geq \dim S/(\mathfrak{p}_1 + xS)$. So now

$$\dim S = 1 + \dim S/(\mathfrak{p}_1 + xS) \leq 2 + P_{S/(\mathfrak{p}_1+xS)} \leq 1 + \deg P_S.$$

So step 1 works for the case $M = S$. For general M we use the exact sequence

$$0 \to M_1 \to M \to M_2 \to 0.$$

If Step 1 works for M_1, M_2, then it works for M as well. $\dim S_M = \max(\dim S_{M_1}, \dim S_{M_2})$ and $\deg P_M = \max(\deg P_{M_1}, \deg P_{M_2})$. (Recall that $S_M = S/\operatorname{Ann}(M)$). This will reduce to the case $M = S/\mathfrak{p}$.

Step 2: $\delta(M) \geq \deg P_M + 1$.

We use induction on $\delta(M)$. If $\delta(M) = 0$, M is of finite length so $M_n = 0$ for n large enough, so $P_M = 0$ and $\deg P_M = -1$. We are done. Now assume $\delta(M) > 0$. There are elements $x_1, \ldots, x_{\delta(M)} \in S_+$ such that $M/\sum x_i M$ has finite length. Consider the exact sequence:

$$M \xrightarrow{x_1} M \longrightarrow \big(M/xM\big) \longrightarrow 0$$

We have $\delta(M/x_1M) = \delta(M) - 1$ and

$$\dim\big(M/x_1M\big)_n \geq \dim M_n - \dim M_{n-\deg x}.$$

It follows that $\deg P_{M/xM} \geq \deg P_M - 1$. From induction $\delta(M/x_1) \geq \deg P_{M/x_1} + 1$, we have

$$\delta(M) = \delta(M/x_1M) + 1 \geq \deg P_{M/x_1} + 2 \geq \deg P_M + 1.$$

Step 3: $\dim S_M \geq \delta(M)$

Again we use induction on $\dim S_M$. If $\dim S_M = 0$ then $S_{M,+}$ is the only maximal ideal. So it is own nill radical. Thus some power of $S_{M,+}$ is zero, as $S_{M,+}$ is finitely generated. Thus $S_{M,n} = 0$ for n sufficiently large. So S_M, therefore M, has finite length. It follows that $\delta(M) = 0$.

So now assume $\dim S_M > 0$. Let $\mathfrak{p}_i$ $(i = 1, \cdots, n)$ all minimal ideals of S_M.

Exercise 4.4.12.

1. Show that there is an $x \in S_{M,+} - \bigcup_{i=1}^n \mathfrak{p}_i$.
2. For such x, $\dim S_M \geq \dim S_{M/xM} + 1$ and $\delta(M/xM) \geq \delta(M) - 1$.

Now the inequality follows from the exercise and the induction $\dim S_{M/xM} \geq \delta(M/xM)$. □

Definition 4.4.13. The degree of X is a number such that the leading coefficient of $P(T)$ has the form $\dfrac{\deg(X)}{d!}T^d$.

Exercise 4.4.14. Compare the degree and leading coefficient of the Hilbert polynomial for $k[x_0, \ldots, x_n]/(F) = S$, where F is a homogeneous polynomial of degree d, $\dim S_n = P(n)$.

Chapter 5

Regularity

5.1 Derivatives, tangent spaces, cotangent spaces

We know a curve C in $\mathbb{R}^2$ is smooth at a point p if we can define the tangent line at this point. Similarly, a surface S in $\mathbb{R}^3$ is smooth at a point p if we can define tangent plane. Thus a geometric object X of dimension d is smooth at a point p if one can define tangent space T_p at this point and dimension of T_p is exactly n. How to define tangent space for an affine spectrum? Tangent space should consist of tangent vectors. What is a tangent vector? Since we can't draw the tangent vector for spectrum. Maybe the we need to know what kind of property we need for tangent vector.

The essential property of tangent vector is to allow us to find directional derivative of functions. More precisely, if v is a nonzero tangent vector of a surface X in $\mathbb{R}^3$ at p, then we can find a sequence of points q_i of points on X such that

1. $\lim_{i\to\infty} q_i = p$, but $q_i \neq p$;
2. $\lim_{i\to\infty} \frac{\overrightarrow{pq_i}}{\|\overrightarrow{pq_i}\|} = \frac{v}{\|v\|}$.

then we can define the derivative D_v in direction v of a function f on X by

$$D_v(f)(x) = \|v\| \lim_{i\to\infty} \frac{f(q_i) - f(p)}{\|pq_i\|}.$$

This derivative has usual properties of derivatives:

$$\begin{cases} D_v(f+g) = D_v(f) + D_v(g), \\ D_v(f\cdot g) = D_v(f)\cdot g + f D_v(g). \end{cases}$$

Definition 5.1.1. A (directional) derivative at a point p in a geometric object X is a map $D\colon$ (functions) $\longrightarrow$ (valuation at p) satisfying

$$\begin{cases} D(f+g) = Df + Dg, \\ D(f\cdot g) = Df\, g(p) + f(p)\, Dg. \\ D(a) = 0, \quad \text{if } a \text{ is a constant function} \end{cases}$$

One can show that $v \to D_v$ defines a bijection between the space of tangent vectors on X and the space of derivatives.

Let A denote the space functions on X which is *differentiable* for every derivative D at p. Let $D_p(A)$ denote the space of all derivatives of A at p. Let m be the space of real functions which vanishes at p. Then the evaluation of A at p defines an isomorphism $A/m \simeq \mathbb{R}$. Let D be a derivative of X at p then $D(m^2) = 0$. Thus D is factored through A/m^2. The restriction of D on m induces a linear map ϕ_D from m/m^2 to $\mathbb{R}$. Let $\mathrm{Hom}_{\mathbb{R}}(m/m^2, \mathbb{R})$ denote the space of all $\mathbb{R}$-linear maps from m/m^2 to $\mathbb{R}$.

Proposition 5.1.2. *The correspondence $D \to \phi_D$ defines an isomorphism*

$$\phi : \quad D_p(A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{R}}(m/m^2, \mathbb{R}).$$

Proof. Any function can be written as a sum of a constant function and a function vanishes at p. Thus

$$A = \mathbb{R} \oplus m.$$

If $\phi_D = 0$, then D vanishes on m. As D always vanishes at $\mathbb{R}$, the space of constant functions, D vanishes on whole A. This shows that ϕ is injective.

Now let ℓ be any linear map from m/m^2 to $\mathbb{R}$, then we define a map $D^\ell : A \to \mathbb{R}$ by composition ℓ with the map $A \to m$ defined by the above decomposition, and the map $m \to m/m^2$. It is easy to show that D^ℓ is a derivative. Thus ϕ is surjective. □

In Summary, we have shown that an usual geometric object in $\mathbb{R}^n$:

1. Smoothness means the dimension of the tangent space equals dimension of X itself.
2. Tangent space can be identified with the space of derivatives $D_p(A)$ at p.
3. The space $D_p(A)$ can be identified with $\mathrm{Hom}(m/m^2, \mathbb{R})$.

Definition 5.1.3. Let A be a ring, and m a maximal ideal of A ($m \in \mathrm{Spec}A$ is a closed point). The cotangent space of A is defined as m/m^2, and the tangent space of A at m is defined to be the space of

$$T_m = \mathrm{Hom}_{A/m}\big(m/m^2, A/m\big).$$

Theorem 5.1.4.

$$\dim_{A/m} T_m \geq \dim \mathrm{Spec}A_{(m)},$$

where $A_{(m)} = (A \backslash m)^{-1} A$.

Definition 5.1.5. We say m is a regular point if

$$\dim_{k(m)} T_m = \dim_{k(m)} m/m^2 = \dim A_{(m)}$$

where $k(m) = A/m$.

Example 5.1.6. Consider the curve $y^2 = x^2(1-x)$ at the point $(0,0)$. It corresponding to the ring

$$A = \frac{k[x,y]}{y^2 - x^2 + x^3}.$$

and the maximal ideal m generated by x and y. Then m^2 is generated by x^2, xy, y^2. It follows that

$$m/m^2 = \frac{xk[x,y] + yk[x,y]}{\{x^2, y^2, xy, y^2 - x^2 + x^3\}} \cong k\overline{x} + k\overline{y}.$$

$\dim m/m^2 = 2$, $\dim A = 1$. So this curve is not regular at $(0,0)$.

Example 5.1.7. Consider the ring

$$A = \mathbb{Z}[2\sqrt{5}] = \frac{\mathbb{Z}[x]}{x^2 - 20}.$$

It has an maximal ideal $m = (x, 2)$ with quotient $A/m = \mathbb{Z}/2\mathbb{Z}$. The cotangent space is given by

$$m/m^2 = \frac{(x,2)}{(x^2, 2x, 4)} = \frac{(x,2)}{(2x,4)}$$

It is clear that this quotient has dimension 2 generated by 2 and x. So A so its not regular at m, since $\dim A = 1$. (Prove $\dim A = 1$ as an exercise.)

Now we going to prove Theorem 5.1.4. Since $\dim T_m = \dim m/m^2$ and $A_{(m)}$ is local, Theorem 5.1.4 is equivalent to the following:

Theorem 5.1.8. *Let A be a Noetherian local ring with maximal ideal m, then $\dim_k m/m^2 \geq \dim(A)$, where $k = A/m$.*

If A is graded with $A_0 = k$ and the maximal ideal A_+ is generated by A_1, then this has been done in the last lecture. Actually the theorem of the last lecture can be generalized to arbitrary local Noetherian rings. Indeed, we define $\dim A$ as usual, and $\delta(A)$ as minimal number of elements x_i's in m such that $A/(x_1, \cdots, x_\ell)$ has finite length, and P_A to be a polynomial such that $P_A(n)$ equal to the length of A/m^n for n sufficiently large. Then the exact same proof gives the following:

Theorem 5.1.9.

$$\dim A = \deg P_A = \delta(A).$$

Now Theorem 5.1.8 follows from Theorem 5.1.9 by the facts that if $x_1, \cdots, x_\ell$ be elements of m generating m/m^2, then $x_1, \cdots, x_\ell$ generate m. This a typical application of Nakayama's lemma. Indeed, let N denote the quotient $m/(x_1, \cdots, x_\ell)$ then $mN = 0$. But this implies that $N = 0$.

Theorem 5.1.10 (Nakayama's lemma)**.** *Let A be a local ring with maximal ideal m. Let M be a finitely generated A-module such that $mM = 0$. Then $M = 0$.*

Proof. Let x_i $(i = 1, \cdots, n)$ be some generators of M over A. Since $mM = M$, each x_i can be written as a linear combination of x_j's with coefficients in m: thus there are $a_{i,j} \in m$ such that $x_i = \sum_j a_{ij} x_j$. Let A denote the matrix of (a_{ij}). Then

$$(I - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Multiplying both sides by the adjoint matrix of $(I - A)$, we obtain

$$\det(I - A)x_i = 0, \qquad i = 1, \cdots, n.$$

Now $\det(I - A)$ is of form $1 - a$ with $a \in m$. As m is maximal, $1 - m$ is invertible, then $x_i = 0$ for every i. It means that $M = 0$. □

Example 5.1.11 (Regular ring of dimension 0). An Noetherian ring of dimension 0 is also called an *Artinian ring*. For an Artinian ring A, every prime ideal is maximal and $\operatorname{Spec}(A)$ is finite. Moreover, $A/\operatorname{Nil}(A) \cong \bigoplus k_i$, k_i are fields.

When is an Artin local ring regular? The condition of A to be regular at $m \subseteq A$ is $\dim m/m^2 = \dim \operatorname{Spec}(A) = 0$, so $m/m^2 = 0$, so $m = m^2$ which implies $m = 0$. This uses Nakayama's lemma. Thus a local Artinian ring is regular if and only if it is a field.

5.2 Regular ring of dimension 1

Now let A be a local Noetherian ring of dimension 1. When is A regular?

Proposition 5.2.1. *Let A be a local ring of dimension 1. Then A is regular if and only if the maximal ideal m is principle.*

Proof. The condition A is regular is equivalent to $\dim m/m^2 = 1$, $k = A/m$. By Nakayama lemma, this is equivalent to that m is generated by one element. □

Theorem 5.2.2. *Let R be a local regular ring of dimension 1. Let m be its maximal ideal. Then*

1) *m is principle, is generated by π (is called the uniformizer).*
2) *Every element $x \in A \setminus \{0\}$ can be written uniquely in the form $x = u \cdot \pi^n$ where u is an invertible element, $n = 0, 1, 2, \ldots$*
3) *$x^n \neq 0$ for all n.*

We need first prove the following:

Lemma 5.2.3. $\bigcap_{n=0}^{\infty} m^n = 0$ *if A is a Noetherian local ring.*

Proof. Set $N = \bigcap_{n=0}^{\infty} m^n$. Then N is an ideal of A and thus finitely generated. The equality $mN = N$ implies $N = 0$ by Nakayama lemma. □

Remark 5.2.4. Notice that $\bigcap_{n=0}^{\infty} m^n =$ functions that vanish with infinite order at a closed point. If A is Noetherian, $\bigcap_{n=0}^{\infty} m^n = 0$. Thus the functions which vanish in infinite order are only zero function.

Proof of Theorem 5.2.2. The first part is implies by previous proposition. For other part, we notice that m^n for a strict decreasing sequence with intersection 0. Otherwise there is some n, $m^n = 0$ which contract to the fact that A has dimension 1. Let $x \neq 0$, $x \in A$, then there is a unique n such that $x \in m^n$, $x \neq m^{n+1}$. Since $m^n = (\pi)^n$, $x = u \cdot \pi^n \implies u \notin m$ so u is invertible and we are done. Thus every element $x \in A$ can be written down in the form of $u \cdot \pi^n$ where b is invertible. Any equation $ux^n = vx^\ell$ (for invertible $u, v \notin m$, $n, \ell \in \mathbb{N}$) implies that $m^n = m^\ell$. Thus $\ell = n$, and $(u - v)x^n = 0$. If $u - v \neq 0$, then $u - v = w\pi^t$ for w invertible and $t \in \mathbb{N}$. This implies that $m^{t+n} = 0$: a contraction. Thus every non-zero $x \in A$ can be written uniquely as $x = u\pi^n$. □

The defines a map $v \colon A \setminus \{0\} \to \mathbb{N}_+$ (non negative integers) defined by $x = u\pi^n \mapsto n$. This map has the following properties

1) $v(xy) = v(x) + v(y)$;

2) $v(x + y) \geq \min(v(x), v(y))$;

3) v is surjective.

The first property implies that A is an integral domain. Let K be the field of fractions of A. We can extend v to $K \setminus \{0\}$ multiplicatively:

$$v(a/b) = v(a) - v(b), \qquad a, b \in A \setminus \{0\}.$$

Then v on K satisfies the same properties as above.

Definition 5.2.5. Let K be a field. A map from $K^* = K - \{0\}$ to $\mathbb{Z}$ is called a discrete valuation if the above three properties are satisfied.

Lemma 5.2.6. *If $v \colon K \to \mathbb{Z}$ is a discrete valuation then*
1) $R = \{x \in K \colon \ v(x) \geq 0\}$ is a local ring;
2) $m = \{x \in K \colon \ v(x) > 0\}$ is a maximal ideal.
We call R the discrete valuation ring.

Example 5.2.7. $Z_{(p)} = \left\{ \frac{a}{b} \colon \ p \nmid b \right\}$.

Example 5.2.8. $k[x]_{(x)} = \left\{ \dfrac{f(x)}{g(x)} : \ g(0) \neq 0 \right\}$.

Thus we just proved that a local ring of dimension 1 is regular if and only if it is a discrete valuation ring. In the following we will give another equivalent condition which is very useful when we compare different regular rings.

Definition 5.2.9. Let A be an integral ring, R a subring. We say X is integrally dependent on R if every $x \in X$ satisfies a monic polynomial equation $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0$, $a_i \in R$.

Lemma 5.2.10. *The set of elements in A which is integral over R is a subring of A.*

Lemma 5.2.11. *The element x is integral over R if and only if $R[x]$ is a R-module of finite type.*

The proof is left to the reader as an exercise.

Definition 5.2.12. The subring of A of elements integral over R is called the integral closure of R in A.

Definition 5.2.13. Let R be an integral ring. We say R is integrally closed (normal) if R coincides with its integral closure in its field of fractions.

Theorem 5.2.14. *Suppose R is integral with dimension 1. The following three are equivalent:*

1. *R is regular;*
2. *R is a discrete valuation ring;*
3. *R is integrally closed.*

Recall that R is integrally closed if for $x \in K$ satisfying $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with $a_i \in R$, then $x \in R$.

Proof. We already have shown (1) is equivalent to (2).

We now show (2) $\Longrightarrow$ (3). Let $x \in K$, where K is the fraction field of R, which satisfies an equation $x^d + a_1 x^{d-1} + \ldots + a_d = 0$ with $a_i \in R$. We want to show that $x \in R$, or equivalently, if we write $x = u\pi^n$, $n \in \mathbb{Z}$, $u \in R^x$, we need to show that $n \geq 0$.

Assume that $n < 0$.

$$x = \frac{u}{\pi^{|n|}}, \quad \text{so} \quad \left(\frac{u}{\pi^{|n|}}\right)^d + a_1 \left(\frac{u}{\pi^{|n|}}\right)^{n-1} + \ldots + a_d = 0.$$

Multiply both sides by $\pi^{|n|d}$ so $u^d + \pi^{|n|} \cdot A = 0$ where $A \in R$. Now u is a unit, therefore $\pi^{|n|} \cdot A$ is a unit which is impossible.

Now show (3) $\Longrightarrow$ (1). We need only show that $\mathfrak{m}$ is principal. Let $a \in R \setminus \{0\}$, $a \in \mathfrak{m}$, then we know that

Lemma 5.2.15. *$R/(a)$ is dimension 0.*

Proof. This is clear as $m/(a)$ is the only prime ideal. □

Lemma 5.2.16. *$\mathfrak{m}/(a)$ as an ideal in $R/(a)$ is nilpotent.*

Proof. This is clear as the nilpotent radical of $A/(a)$ is $\mathfrak{m}/(a)$. □

So we know $\big(\mathfrak{m}/(a)\big)^n = 0$ for some n or $\mathfrak{m}^n \subset (a)$. Take n minimal with this property, $\mathfrak{m}^n \subset (a) \not\supseteq \mathfrak{m}^{n-1}$. Let $b \in \mathfrak{m}^{n-1} \setminus (a)$. Let $x = a/b$. We want to show x generates $\mathfrak{m}$, that is $(x) = \mathfrak{m}$, or $x^{-1}\mathfrak{m} = R$ as an identity of subsets in K. Notice that

$$x^{-1}\mathfrak{m} = \frac{b}{a}\mathfrak{m} \subset \mathfrak{m}^{n-1}\mathfrak{m}/a = \mathfrak{m}^n/a \subset R.$$

Thus we have two choices:

1) $x^{-1}\mathfrak{m} = R$ which implies $\Longrightarrow \mathfrak{m} = xR$ and we are done.

2) $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$.

We want to show that 2) implies that x^{-1} is integral over R thus $x^{-1} \in R$ which is a contradiction since $b/a \in R$ implies $b \in Ra$ which contradicts our choice of a, b.

Now we need the following

Lemma 5.2.17. *Let Q be an endomorphism of a module over a ring R which is finitely generated. Then Q satisfies an equation of the form*

$$Q^n + a_1 Q^{n-1} + \ldots + a_n = 0, \qquad a_i \in R.$$

The proof is left to the reader as an exercise.

Lemma 3 completes our proof. □

Exercise 5.2.18. 1. Find all discrete valuations on $\mathbb{Q}$.

2. Find all discrete valuations on $k(T)$ where k is a field.

5.3 Dedekind domain

Definition 5.3.1. A ring R is called a Dedekind ring if R is integral of dimension 1 and satisfies one of the following equivalent conditions:

1) Spec$R$ is regular.

2) $R_{\mathfrak{p}}$ is a discrete valuation ring for maximal ideal $\mathfrak{p}$.

3) R is integrally closed.

First two conditions are local while the third is global. We need to check the third.

Theorem 5.3.2. *Let R be an integral Noetherian ring. Then R is integrally closed if and only if $R_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$.*

Proof. Suppose R is integrally closed. Let $\mathfrak{p}$ be a prime ideal, $x \in K$ is the fraction field of R which is integrally closed over $R_{\mathfrak{p}}$.

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \quad a_i \in R_{\mathfrak{p}} = \left\{ \frac{\alpha}{\beta} \in K,\ \beta \notin \mathfrak{p} \right\}.$$

$$a_i = \frac{\alpha_i}{\beta_i} = \frac{\alpha_i \prod_{j \neq i} \beta_j}{\prod_j \beta_j}.$$

So assume $\beta_i = \beta_j = \beta$ without a loss of generality. So multiply through by β^n,

$$\beta^n x^n + \beta^{n-1} \alpha_1 x^{n-1} + \ldots + \alpha_n = 0.$$

Equivalently

$$(\beta x)^n + \alpha_1 (\beta x)^{n-1} + \ldots + \alpha_n = 0,$$

so βx is integral over R. By assumption $\beta x \in R$ since R is integrally closed, $x = (1/\beta)R \in R_{\mathfrak{p}}$.

Now in the other direction: Let $x \in K$, integral over R. Thus x is integral over $R_{\mathfrak{p}}$ for every $\mathfrak{p}$ so $x \in R_{\mathfrak{p}}$ for every $\mathfrak{p}$. Equivalently for any $\mathfrak{p}$ there is an $y \notin \mathfrak{p}$ such that $xy \in R$. Let $I = \{y \in R \colon yx \in R\}$. Then $I \not\subset \mathfrak{p}$ for every $\mathfrak{p}$. This last condition implies that $I = R$, and thus $x \in R$. □

Theorem 5.3.3 (Unique Factorization Theorem for Dedekind Domains)**.** *Every ideal I in a Dedekind domain can be decomposed in a unique way into a product of prime ideals.*

Proposition 5.3.4. *Let R be a Noetherian ring.*

1. *Let M be an R-module of finite type, then $M = 0$ if and only if $M\mathfrak{p} = 0$ for every prime ideal $\mathfrak{p}$.*
2. *Let $\phi \colon M_1 \to M_2$ be a homomorphism between R-modules of finite type, then ϕ is bijective (respectively injective or surjective) if and only if $\phi_{\mathfrak{p}} \colon (M_1)_{\mathfrak{p}} \to (M_2)_{\mathfrak{p}}$ is bijective (respectively injective or surjective) for every $\mathfrak{p}$.*
3. *Let N_1, N_2 be submodules of M of finite type, then $N_1 = N_2 \iff (N_1)_{\mathfrak{p}} = (N_2)_{\mathfrak{p}}$ for every $\mathfrak{p}$.*

Proof. For the first part, $M_{\mathfrak{p}} = 0$ for all prime $\mathfrak{p}$, then $\operatorname{Ann}(M) \not\subset \mathfrak{p}$ for every $\mathfrak{p}$, so $1 \in \operatorname{Ann}(M)$. It follows that $M = 0$.

For the second part we apply the first part to $\ker \phi$ and $\operatorname{coker}(\phi)$ and use the fact

$$\ker(\phi)_{\mathfrak{p}} = \ker(\phi_{\mathfrak{p}}), \qquad \operatorname{coker}(\phi)_{\mathfrak{p}} = \operatorname{coker}(\phi_{\mathfrak{p}}).$$

For the last part, we apply the second part to the inclusion

$$\phi_1 : N_1 \cap N_2 \subset N_1, \qquad \phi_2 : N_1 \cap N_2 \subset N_2$$

and use the fact

$$(N_1 \cap N_2)_{\mathfrak{p}} = N_{1\mathfrak{p}} \cap N_{2\mathfrak{p}}.$$

□

Now for a proof of the unique factorization theorem for Dedekind domains. For every prime ideal $\mathfrak{p}$, $I_\mathfrak{p}$ is a non-zero ideal of $R_\mathfrak{p}$. Thus there is $n_\mathfrak{p} \in \mathbb{N}$ such that $I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{n_\mathfrak{p}}$. If $n_\mathfrak{p} > 0$ then $I_\mathfrak{p} \subset \mathfrak{p}_\mathfrak{p}$ which implies $I \subset \mathfrak{p}$ since $\mathfrak{p} = A \cap \mathfrak{p}_{(\mathfrak{p})}$. Since $\dim(A/I) = 0$, A/I is Artinian. Thus A/I has only finitely many prime ideals containing I. In summary we have proven:

1) for every $\mathfrak{p}$: $I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{n_\mathfrak{p}}$, $n_\mathfrak{p} \geq 0$.

2) $n_\mathfrak{p} \neq 0$ for only finitely many $\mathfrak{p}$.

Let $J = \prod \mathfrak{p}^{n_\mathfrak{p}}$. We want to prove $I = J$. By the proposition, we need only prove that $I_\mathfrak{p} = J_\mathfrak{p}$ for all prime $\mathfrak{p}$ which is given by the following lemma:

Lemma 5.3.5. *Let R be a Dedekind domain.*

1. *Let I_1, I_2 two ideals of R then*

$$(I_1 I_2)_\mathfrak{p} = (I_1)_\mathfrak{p} \cdot (I_2)_\mathfrak{p}.$$

2. *If $\mathfrak{p}_1$, $\mathfrak{p}_2$ are two nontrivial prime ideals and $\mathfrak{p}_1 \neq \mathfrak{p}_2$ ($\mathfrak{p}_1 \not\subset \mathfrak{p}_2$, $\mathfrak{p}_2 \not\subset \mathfrak{p}_1$). Then $\mathfrak{p}_{1\mathfrak{p}_2} = \mathfrak{p}_{2\mathfrak{p}_1} = K$, where K is the fractional field of R.*

We have proved the exitance part of the theorem. The uniqueness is left as an exercise.

Fractional ideals of Dedekind domain

Definition 5.3.6. Let R be a Dedekind domain. Let K denote the fraction field of R. By a fractional ideal we mean a R-submodule I of K which is finitely generated over R. Thus a fractional ideal can be written as

$$I = \sum_i a_i R, \quad a_i \in R, \quad a_i = \frac{\alpha_i}{\beta_i}, \quad \alpha_i, \beta_i \in R.$$

By taking a denominator $I = \frac{1}{\beta} \sum \alpha_i R$ ($\sum \alpha_i R$ is a real ideal) so equivalently a fractional ideal of R is an R-submodule I of K with the form $I = \frac{1}{\beta} J$ where a is a nonzero element of R and J is an ideal of R.

Properties of fractional ideals. We can add two fractional ideals $I_1 + I_2$. Also the operation $I_1 \cdot I_2$ makes the set of non-zero fractional ideals a free group over prime ideals with unit R. We need only show the inverse does exist. In other words: for every ideal I there is a fraction ideal J such that $I \cdot J = R$.

Proof of statement: Let J be a fractional ideal defined by $J = \{x \in K \colon xI \subset R\}$, so $I \cdot J \subset R$. We want to show $I \cdot J = R$.

Now to finish the proof of the statement: We need only show that $I_\mathfrak{p} \cdot J_\mathfrak{p} = R_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$.

$$J_\mathfrak{p} = \left\{ \frac{a}{b},\ a \in J, b \notin \mathfrak{p} \right\} = \{x \in K,\ xI_\mathfrak{p} \subset R_\mathfrak{p}\}$$

Now $R_{\mathfrak{p}}$ is a discrete valuation ring. If π is a uniformizer of $R_{\mathfrak{p}}$ then $I_{\mathfrak{p}} = (\pi^n)$ for some integer n. It follows that $J_{\mathfrak{p}} = \{x \in K, xI_{\mathfrak{p}} \subset R_{\mathfrak{p}}\}$ but $x = u\pi^m$, $m \in \mathbb{Z}$, $u\pi^{m+1} \subset R_{\mathfrak{p}}$, $m + n \geq 0$, take $m = -n$ so $J_{\mathfrak{p}} = (\pi^{-n})$. Thus $I_{\mathfrak{p}} \cdot J_{\mathfrak{p}} = R_{\mathfrak{p}}$ and we are done.

Let $\mathbb{I}(k)$ denote the group of all fractional ideals. When are two fractional ideals isomorphic? For any isomorphism $\phi\colon I_1 \xrightarrow{\sim} I_2$, we can localize with respect to 0-ideal of R.

$$\begin{array}{ccc} (I_1)_{(0)} & \xrightarrow{\phi_{(0)}} & (I_2)_{(0)} \\ \downarrow & & \downarrow \\ K & \longrightarrow & K \end{array}$$

This is K-linear, $K = R_{(0)}$. So $\phi_{(0)}$ is given by multiplication of $a = \phi(1)$. Thus ϕ is also given by multiplication. Notice that $aI_1 = (a)I_1$ for some $a \in K$. So

$$1 \longrightarrow \{\text{principal ideals}\} \longrightarrow \mathbb{I} \longrightarrow \{\text{isomorphic class of ideals}\} \longrightarrow 1.$$

The set of isomorphic classes of ideals of R is denoted by $\mathrm{Cl}(R)$, and is called the ideal class group of R. The group of nonzero principal fractional ideals is denoted by P. So we have the exact sequence:

$$1 \longrightarrow P \longrightarrow \mathbb{I} \longrightarrow \mathrm{Cl}(R) \longrightarrow 1.$$

Historic remarks: Studying ideals was started from trying to solve Fermat's Last Theorem: $x^\ell + y^\ell = z^\ell$, ℓ prime, $\ell \geq 3$, x, y, z relative prime positive integers. Let $e^{2\pi i/\ell} = \xi$ then we have decomposition

$$\prod_{i=0}^{\ell-1}(x + \xi^i y) = z^\ell.$$

If $R := \mathbb{Z}[e^{2\pi i/\ell}]$ is a UFD then one can show that the factors in the left hand side are almost relatively coprime each other. Thus each of them is an ℓ-th power. From this one can easily obtain a contradiction. So Fermat's theorem is true. If R is not a UFD, then one can decompose both sides as product of prime ideals. One can show that $\mathrm{Cl}(R)$ is finite and the above argument still works if $l \nmid |\mathrm{Cl}(R)|$.

Some properties of fractional ideals

1) Moving lemma
2) Projectivity
3) $I \oplus J \cong R \oplus IJ$

1) Moving Lemma.

Lemma 5.3.7. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be a finite set of prime ideals. Then every ideal I is isomorphic an ideal J which is not divided by the $\mathfrak{p}_i$'s.*

Proof. Write $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$. By Chinese remainder theorem, there is an $a \in K^x$, such that $a \in I^{-1}$, $a \notin I^{-1} \cdot \mathfrak{p}_i$. Now it is easy to see that aI satisfies the requirement of the lemma. $\square$

2) Projectivity.

Lemma 5.3.8. *Let $Q : M \to I$ be a surjective map, where M is a finitely generated R-module and I is a R-ideal. Then Q has a section: this means that there is a homomorphism $s\colon I \to M$ such that $Q \circ s$ is the identity map.*

Example 5.3.9. If I is the trivial ideal this lemma is easy. Indeed, let $m \in M$ such that $Q(m) = 1$, then we can define s by $s(x) = xm$.

Notation: Let M, N be two R-modules. $\mathrm{Hom}_R(M, N)$ is the set of R-homeomorphisms from M to N. Then this set has a natural R-module structure: $(Q_1+Q_2)(x) = Q_1(x)+Q_2(x)$, if $a \in R$, $aQ_1(x) = a(Q_1(x))$.

Exercise 5.3.10. If M, N are of finite type then $\mathrm{Hom}(M, N)$ is of finite type.

Now it is easy to see that the Lemma is equivalent the surjectivity of the following homomorphism of R-modules:

$$\mathrm{Hom}_R(I, M) \longrightarrow \mathrm{Hom}_R(I, I)$$

but this is true, as it is true locally. Indeed, locally R is a principal ideal domain.

3) Let I and J be two fractional ideals, then $I \oplus J \simeq R \oplus IJ$.

Proof. Using the moving lemma, we may assume I is an ideal, $I = \prod \mathfrak{p}_i^{n_i}$, $n_i > 0$, J is an ideal, $\mathfrak{p}_i \nmid J$ for every i.

Now $I + J = R$ because of localization. Now we have a surjection $\phi : I \oplus J \twoheadrightarrow R$ given by $(x, y) \mapsto x + y$. Since this map is surjective, there is a section. To finish the proof, we need discuss the wedge product. □

The wedge product. Let V be an R-module of rank 2. ($V_\mathfrak{p} \simeq R_\mathfrak{p}^2$ for every $\mathfrak{p}$, i.e. locally it is a 2-dimensional space.) Define $\det(V) = V \wedge V$, the quotient of the free R-module generated by $V \times V$ modulo the following relations:

$$(ax, y) = (x, ay) = a(x, y)$$
$$(x, y) = -(y, x)$$

In practice: $\det(V)$ is an R-module characterized by the following property:

1) $V \times V \xrightarrow{\phi} V \wedge V = \det(V)$ such that

$$\phi(ax, y) = \phi(x, ay) = \phi(x, y),$$
$$\phi(x, y) = -\phi(y, x).$$

2) $\det(V)$ is universal wih respect to property (1): If $\psi\colon V \times V \to W$ satisfies 1) then there exists unique $f\colon \det(V) \to W$ such that $\psi = f \circ \phi$.

We use this to show $I_1 \oplus I_2 = R \oplus I_1 I_2$. We have already shown $I_1 \oplus I_2 = R \oplus J$ for some J. Left: (i) J is an ideal (easy), (ii) $\det(I_1 \oplus I_2) = I_1 \cdot I_2$, (iii) $\det(I_1 \oplus I_2) = \det(R \oplus J)$.

Prove (i)–(iii) as an exercise.

Corollary 5.3.11. *Every ideal I of R is generated by two elements.*

Proof. $I \oplus I^{-1} \simeq R \oplus II^{-1} = R \oplus R$. Therefore $\exists\ R^2 \twoheadrightarrow I$. □

5.4 Modules over Dedekind domain

Let M be a finitely generated module over a Dedekind domain R. The torsion submodule of M is defined to be:

$$M_{tor} = \{x \in M : \exists\, r \in R, r \neq 0, rx = 0\}\,.$$

Equivalently, the M_{tor} is the kernel of the natural homomorphism from M to the localization $M_{(0)}$ at the 0-ideal of R:

$$0 \longrightarrow M_{tor} \longrightarrow M \xrightarrow{\pi} M_{(0)}.$$

Write $K = R_{(0)}$ and $M_{(0)} = M_K$. Then M_K is a K-vector space of finite dimension, say n.

Let M' be the image of π, then

$$0 \longrightarrow M_{tor} \longrightarrow M \longrightarrow M' \longrightarrow 0, \qquad M' \hookrightarrow K^n,$$

and M' has no torsion. If M is not torsion, then $n \neq 0$, then we have the projection $K^n \twoheadrightarrow K$ onto the first factor. Let N be the image of M' of this projection. Then N is a nonzero fractional ideal of R. We thus have

Lemma 5.4.1. *If $M_{(0)} \neq 0$ (i.e. $M \neq M_{tor}$) then there is a surjective map $M \twoheadrightarrow N$ with N a fractional ideal of R.*

Since N is projective, $M \twoheadrightarrow N$ has a section, whence $M \cong M_1 \oplus N$.

Continuing this argument for M_1, if M_1 is not torsion... Eventually, after n steps ($n = \dim_K M_{(0)}$) we have

$$M \simeq M_{tor} \oplus I_1 \oplus I_2 \oplus \ldots \oplus I_n.$$

Now apply the fact $I_1 \oplus I_2 = R \oplus I_1 I_2$ then we may assume $M \simeq M_{tor} \oplus R^{n-1} \oplus I$ where I is an ideal of R (if M is not torsion). What remains is to study the structure of M_{tor}. Since M_{tor} is finitely generated, there exists $x \in R$, $x \neq 0$ such that $xM_{tor} = 0$. Therefore $(M_{tor})_{\mathfrak{p}} = 0$ if $x \notin \mathfrak{p}$ (equivalently, $\mathfrak{p} \nmid (x)$). It follows that $(M_{tor})_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p}$ ($(x) = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$). Now by localization principal, the natural homomorphism

$$M_{tor} \longrightarrow \bigoplus_{\mathfrak{p}} (M_{tor})_{\mathfrak{p}}$$

is actually an isomorphism. This is because $\mathfrak{p}_1 \neq \mathfrak{p}_2$ implies $\mathfrak{p}_1 + \mathfrak{p}_2 = R$ whence $((M_{tor})_{\mathfrak{p}_1})_{\mathfrak{p}_2} = M_{(0)} = 0$.

It remains to study the structure of $(M_{tor})_{\mathfrak{p}}$. It is an $R_{\mathfrak{p}}$-module, $R_{\mathfrak{p}}$=DVR.

Lemma 5.4.2. *Let R be a discrete valuation ring. Let N be a finitely generated torsion R-module, then*

$$N \simeq \bigoplus_{i=0}^{k} R/\pi^{n_i}, \qquad n_i \geq 0.$$

Proof. Let $k = R/\pi$, (π) = maximal ideal of R, then $N/\pi N$ is a finite dimensional k-vector space. Let $x_1, \ldots, x_t$ be elements of N such that their images in $N/\pi N$ generate $N/\pi N$ over k. By Nakayama's lemma $x_1, \ldots, x_t$ generate N. Thus we have a surjective map $R^t \overset{\phi}{\twoheadrightarrow} N \to 0$, $\ker \phi$ is an R-module without torsion.

By what we have proved for non-torsion modules over Dedekind domain: $\ker \phi \simeq R^{m+1} \oplus I$, I an R-ideal but R is PID, hence $I \simeq R$. Thus we have an exact sequence

$$0 \longrightarrow R^m \xrightarrow{\alpha} R^t \longrightarrow N \longrightarrow 0.$$

Claim 5.4.3. $m = t$.

Proof. Localize at (0)-ideal. Since N is torsion, $N_{(0)} = 0$, $R^m_{(0)} = R^t_{(0)}$ and $R_{(0)} = k$ (vector spaces). Thus $m = t$. □

Putting $R^t = \sum_{i=1}^{t} Re_i$, α is given by a $t \times t$ matrix A with entries a_{ij} in R: $\alpha(e_i) = \sum a_{ij} e_j$. Now, for two automorphism u and v of R^t, one has commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^t & \xrightarrow{\alpha} & R^t & \longrightarrow & N & \longrightarrow & 0 \\ & & \wr\downarrow u & & \wr\downarrow v & & \downarrow\wr & & \\ 0 & \longrightarrow & R^t & \xrightarrow{v\alpha u^{-1}} & R^t & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

(change of basis). If u, v are given by invertible $t \times t$ matrices B and C in R, then $u\alpha v$ is given by BAC.

In summary,

1) The structure of N is determined by A (it is the cokernel).

2) The abstract structure of N doesn't change if A is replaced by BAC where B, C are invertible $t \times t$ matrices over R.

Three operations for rows (and columns) are thus allowed to determined the structure of N: (i) Switch row. (ii) Multiply one row by an element in R^*. (iii) Add R-multiple of one row to another row.

Lemma 5.4.4. *There exist matrices B, C such that*

$$BAC = \begin{pmatrix} \pi^{n_1} & 0 & \ldots & 0 \\ 0 & \pi^{n_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \pi^{n_t} \end{pmatrix}, \qquad n_1 \leq n_2 \leq \ldots \leq n_t.$$

Moreover, $\{n_1, \ldots, n_t\}$ are uniquely determined.

Proof.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

(Remark: A may not be invertible in R but it is invertible in K, where A has a non-zero entry.)

Let $n_1 = \min v(a_{ij}) = v(a_{i_0 j_0})$. After switching rows and columns, we may assume that $i_0 = 1$, $j_0 = 1$. Thus every a_{ij} is a multiple of a_{11} (in R!), $a_{11} = u \cdot \pi^{n_1}$, multiply row 1 by u^{-1}, then may assume $a_{11} = \pi^{n_1}$. Performing operation (iii) on rows and columns, we may assume that $a_{1k} = 0 = a_{k1}$ for every k. So A is transformed to

$$\begin{pmatrix} \pi^{n_1} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$a_{ij} \in R$, $\pi^{n_1} \mid a_{ij}$. Continue this argument.

Exercise 5.4.5. Prove the uniqueness of $n_1 \leq n_2 \leq \ldots \leq n_t$.

□

Apply to find the structure of N

$$0 \longrightarrow R^t \xrightarrow{A} R^t \longrightarrow N \longrightarrow 0$$

with $A = \mathrm{diag}(\pi^{n_1}, \ldots, \pi^{n_t})$, i.e. $Ae_i = \pi^{n_i} e_i$.

We obtain

$$N = \frac{R}{\pi^{n_1} R} \oplus \ldots \oplus \frac{R}{\pi^{n_t} R}$$

and we are done. □

Chapter 6

Curves

6.1 Number fields

Definition 6.1.1. A field K is called a number field, if it is a finite extension of $\mathbb{Q}$.

Definition 6.1.2. The integral closure of $\mathbb{Z}$ in K is called *the ring of integers* of K and is denoted by $\mathcal{O}_K$.

$$\mathcal{O}_K = \{x \in K \colon \exists \text{ a monic } p(T) \in \mathbb{Z}[T] \text{ such that } p(x) = 0\}.$$

Theorem 6.1.3. *Let K be a number field ($K \supseteq \mathbb{Q}$, $[K \colon \mathbb{Q}] < \infty$). Let $\mathcal{O}_K$ be the ring of integers in K. Then:*

1. *$\mathcal{O}_K$ is Noetherian ($\mathcal{O}_K$ is a free $\mathbb{Z}$ module of rank $n = [K \colon \mathbb{Q}]$).*
2. *$\mathcal{O}_K$ is a Dedekind domain (dimension 1 and integrally closed).*
3. *The set $|\mathrm{Spec}\mathcal{O}_K|$ of closed points are in 1 – 1 correspondence to discrete valuations of K.*
4. *$\mathcal{O}_K$ is the unique subring of K that satisfies 1), 2) and 3).*

Recall $x \in K$ is integral over $\mathbb{Z}$ if and only if $\mathbb{Z}[x]$ is a $\mathbb{Z}$-module of finite type.

Part 1

The idea of the proof. (a) The theorem is true for $K = \mathbb{Q}$. (b) We want to include $\mathcal{O}_K$ in a finite $\mathbb{Z}$-submodule of K. This will imply $\mathcal{O}_K$ is Noetherian. It is easy to find a submodule M of $\mathcal{O}_K$ such that M over $\mathbb{Z}$ is free of rank $[K \colon \mathbb{Q}]$. Say $[K \colon \mathbb{Q}] = n$. $K = \sum_{i=1}^{n} \mathbb{Q}x_i$, $x_i \in K$, x_i may not be integral over $\mathbb{Z}$ but $n_i x_i$ will be integral over $\mathbb{Z}$ for some $n_i \in \mathbb{N}$. So we may take $M = \sum_i \mathbb{Z}x_i$.

We need to define some pairing then we can find the dual $M^\vee$ of M such that $M \subseteq \mathcal{O}_K \subseteq M^\vee$, where $M^\vee$ is also free over $\mathbb{Z}$ of rank n.

We have $\mathbb{Q} \hookrightarrow K = \sum_{i=1}^{n} \mathbb{Q}x_i$. For $x \in K$, $xx_i = \sum a_{ij}(x)x_j$, $a_{ij} \in \mathbb{Q}$. $x \mapsto A(x) = (a_{ij})$ is an $n \times n$ matrix.

$$\begin{aligned} P_x(T) &= \det(T - A(x)) \in \mathbb{Q}[T], \qquad P_x(x) = 0 \\ \operatorname{tr}(x) &= \operatorname{tr}(A(x)) \in \mathbb{Q}, \\ \nu(x) &= \det(A(x)) \in \mathbb{Q}. \end{aligned}$$

We can define a pairing $K \times K \to \mathbb{Q}$ via $(x, y) \mapsto \operatorname{tr}(xy)$. Now

1) $(\alpha x, y) = (x, \alpha y) = \alpha(x, y)$ if $\alpha \in \mathbb{Q}$,

2) the pairing is non-degenerate, that is if $(x, y) = 0$ for every y then $x = 0$. (Proof: if $x \neq 0$ let $y = 1/x$, then $\operatorname{tr}(xy) = \operatorname{tr}(1) = n \neq 0$.)

3) $(x + y, z) = (x, z) + (y, z)$.

□

Definition 6.1.4. If $M \hookrightarrow K$ is a submodule then we define the dual of M by $M^\vee = \{x \in K : (x, y) \in \mathbb{Z} \ \forall\, y \in M\}$.

Lemma 6.1.5. *1) $\mathcal{O}_K^\vee \supset \mathcal{O}_K$ or, equivalently, $\operatorname{tr}(x, y) \in \mathbb{Z}$ for all $x, y \in \mathcal{O}_k$.*

2) If $M \supset N$ then $M^\vee \subset N^\vee$.

3) If $M/\mathbb{Z}$ is free of rank $[K : \mathbb{Q}]$ then $M^\vee/\mathbb{Z}$ is also free of rank $[K : \mathbb{Q}]$.

(Note that $x \in K$ is integral over $\mathbb{Z}$ if and only if $P_x(T)$ is monic. Show this as an exercise.)

Write $M = \sum_{i=0}^{n} \mathbb{Z}x_i$, $\implies$ $K = \sum_{i=0}^{n} \mathbb{Q}x_i$. The pairing is non-degenerate. This means $(x, y) = 0$ for every y implies $x = 0$. We have $K \to \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$ via $x \longmapsto (y \mapsto (y, x))$. This non-degeneracy implies a perfect pairing, i.e. $K \simeq \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$. If $K = \sum_{i=0}^{n} \mathbb{Q}x_i$, $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{Q}) = \sum_i \mathbb{Q}\, l_i$, where

$$l_i : K \to \mathbb{Q}, \qquad l_i(x_j) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

There are $x_i^* \in K$ such that $x_i^* \mapsto l_i$, or in other words $(x_i^*, x_j) = \delta_{ij}$.

Claim 6.1.6. $M^\vee = \displaystyle\sum_{i=0}^{n} \mathbb{Z}x_i^*$.

Proof. If $\alpha \in M^\vee$ then $\alpha = \sum a_i x_i^*$, $a_i \in \mathbb{Q}$, $\operatorname{tr}(a_i) \in \mathbb{Z}$ if and only if $\operatorname{tr}(\alpha x_i) \in \mathbb{Z}$ if and only if $\sum a_i \operatorname{tr}(x_j^*, x_i) \in \mathbb{Z}$, if and only if $a_i \in \mathbb{Z}$ for all i. □

Now we will go back to the proof of the first part of Theorem 6.1.3. We have proved that $\mathcal{O}_K$ contains an M, free over $\mathbb{Z}$ of rank $[M : \mathbb{Z}]$. Take the dual $\mathcal{O}_K^\vee \hookrightarrow M^\vee$ also $\mathcal{O}_K \hookrightarrow \mathcal{O}_K^\vee \hookrightarrow M^\vee$ so $\mathcal{O}_K \hookrightarrow M^\vee$, thus $\mathcal{O}_K$ is a submodule of a module over $\mathbb{Z}$ which is finitely generated as a $\mathbb{Z}$-module. As $\mathbb{Z}$ is Noetherian, $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$ so $\mathcal{O}_K$ is Noetherian by the Hilbert basis theorem. Actually we showed that $\mathcal{O}_K$ as a finite $\mathbb{Z}$-module.

Part 2

Lemma 6.1.7. *The ring $\mathcal{O}_K$ is integrally closed.*

Proof. Let $x \in K$, x is integral over $\mathcal{O}_K$. Show x is integral over $\mathbb{Z}$. x is integral over $\mathcal{O}_K$ if and only if $\mathcal{O}_K[x]$ is finite over $\mathcal{O}_K$ which implies $\mathcal{O}_K[x]$ is finite over $\mathbb{Z}$ as $\mathcal{O}_K/\mathbb{Z}$ is finite so $\mathbb{Z}[x]$ is finite over $\mathbb{Z}$ because $\mathbb{Z}[x] \subset \mathcal{O}_K$. □

Lemma 6.1.8. *$\mathcal{O}_K$ is a Dedekind domain.*

Proof. We need only show that $\mathcal{O}_K$ is of dimension 1. $\mathbb{Z} \hookrightarrow \mathcal{O}_K$, $\mathcal{O}_K/\mathbb{Z}$ is finitely generated. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. We want to show $\mathfrak{p}$ is maximal.

Lemma 6.1.9. *$\mathfrak{p} \cap \mathbb{Z} \neq \emptyset$.*

Proof. $x \in \mathfrak{p}$, thus $x/\mathbb{Z}$ is integral so $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ where $a_n \in \mathbb{Z}$, $a_n \in \mathfrak{p}$ because everything else is in $\mathfrak{p}$. □

Now we have $\mathbb{Z} \longrightarrow \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}$, $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \hookrightarrow \mathcal{O}_K/\mathfrak{p}$ — integral ring (we want this to be a field). Thus $\mathfrak{p} \cap \mathbb{Z}$ is a non-zero prime ideal (p). Write $F = \mathcal{O}_K/\mathfrak{p}$, and $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) = \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. We have the embedding of integral rings $\mathbb{F}_p \hookrightarrow F$, $F/\mathbb{F}_p$ is finite $\implies$ F is a field (since $\mathbb{F}_p$ is a field if and only if F is a field when $F/\mathbb{F}_p$ is finite). Thus $\mathfrak{p}$ is maximal. □

Exercise 6.1.10. Show that $\mathbb{Z}[e^{2\pi i/n}]$ is regular.

Hint: Use the local integral condition, and consider the case $n = p$, p is a prime.

Part 3

Proof (continuation). Let $v \colon K^\times \to \mathbb{Z}$ be one discrete valuation. Let R be the correspondent discrete valuation ring. We want to show that $R = \mathcal{O}_{K,\mathfrak{p}}$ (localization of $\mathcal{O}_K$ at a prime ideal $\mathfrak{p}$). Let $\mathfrak{m}$ be the maximal ideal of R.

Recall that R is integraly closed, thus it include $\mathcal{O}_K$ which is integrally closed over $\mathbb{Z}$. We have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & R \\ \downarrow & & \downarrow \\ \mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{m}) & \longrightarrow & R/\mathfrak{m} \end{array}$$

Thus $\mathfrak{m} \cap \mathcal{O}_K$ is a prime ideal. Claim: $\mathfrak{m} \cap \mathcal{O}_K \neq (0)$. If $\mathfrak{m} \cap \mathcal{O}_K = (0)$ then if $x \in \mathcal{O}_K$, $x \neq 0$, $x \notin \mathfrak{m}$ then $(1/x) \in R$, thus $K \hookrightarrow R \hookrightarrow K$. This is impossible since the valuation is assumed to be non-trivial. So $\mathfrak{p} := \mathfrak{m} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. Since every element in $\mathcal{O}_K \setminus \mathfrak{p}$ is invertible in R, R includes the localoization $\mathcal{O}_{K,\mathfrak{p}}$ of $\mathcal{O}_K$. Notice that $\mathcal{O}_{K,\mathfrak{p}}$ its self is integrally local ring, thus is a discrete valuation ring. We then must have $R = \mathcal{O}_{K,\mathfrak{p}}$ by the following lemma. □

Lemma 6.1.11. *Let R_1, R_2 be two discrete valuation rings with the same fraction field K. Assume $R_1 \subseteq R_2$, then $R_1 = R_2$.*

The proof is left to the reader as an exercise.

Exercise 6.1.12. Prove part 4).

Quadratic fields

Let K be a quadratic extension of $\mathbb{Q}$, namely an extension of $\mathbb{Q}$ with degree $[K\colon \mathbb{Q}] = 2$. We can to describe $\mathcal{O}_K$ explicitly.

Let $\alpha \in K - \mathbb{Q}$, then $\mathbb{Q}(\alpha) \neq \mathbb{Q}$ and $\mathbb{Q}(\alpha) \hookrightarrow K$. It follows that $K = \mathbb{Q}(\alpha)$ and α will satisfy the equation

$$x^2 + ax + b = 0, \qquad a, b \in \mathbb{Q}.$$

Replacing α by $\alpha - (a/2)$ ($\alpha - (a/2) \notin \mathbb{Q}$), we may assume $a = 0$. In other words K has the form $\mathbb{Q}(\sqrt{\alpha})$. If $d = \dfrac{a}{b} = \dfrac{ab}{b^2}$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{ab})$. It follows that K can be written as $\mathbb{Q}(\sqrt{d})$ with a unique square free $d \in \mathbb{Z}$. Every $\alpha \in K$ can be written uniquely as $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Q}$.

If $\alpha \notin \mathbb{Q}$ then the minimal equation of α over $\mathbb{Q}$ is

$$T^2 + 2xT + (x^2 + Dy^2) = 0.$$

Thus α is integral over $\mathbb{Z}$ if and only if $2x \in \mathbb{Z}$ and $x^2 + Dy^2 \in \mathbb{Z}$. Modulo $\mathbb{Z}$, $x = 0$ or $x = 1/2$. Thus $Dy^2 \in \mathbb{Z}$ or $(1/4) - Dy^2 \in \mathbb{Z}$. If $Dy^2 \in \mathbb{Z}$ then $y \in \mathbb{Z}$. If $(1/4) - Dy^2 \in \mathbb{Z}$, then let $y = a/b$ with $b > 1, (a, b) = 1$,

$$\frac{1}{4} - \frac{a^2 D}{b^2} \in \mathbb{Z}, \quad \text{thus} \quad \frac{4a^2 D}{b^2} \in \mathbb{Z}.$$

Thus one must has $b = 2$, and then

$$\frac{1 - a^2 D}{4} \in \mathbb{Z}.$$

Now $2 \nmid a$, If $a = 2N + 1$, $a^2 \equiv 1 \pmod 4$. So $D \equiv 1 \pmod 4$.

We have shown

Theorem 6.1.13.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{D}, & D \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1 - \sqrt{D}}{2}\right), & D \equiv 1 \pmod 4 \end{cases}$$

6.2 Function fields

Let k be a field. Let K be an extension of k. Assume that K/k is finitely generated and $\operatorname{tr}\deg K/k = 1$, and that k is algebraically closed in K. If $p := \operatorname{char} k > 0$, we assume that k is perfect: $k^p = k$.

Theorem 6.2.1. *There is a curve X such that*

1. *Function field of X is K.*
2. *X is regular.*
3. *$|X|$= set of closed points is in 1 – 1 correspondence with the discrete valuations of K.*
4. *X is maximal with properties 1, 2 and is unique with respect to 1 – 3.*

Preliminary Field Theory

Let L/K be a finite extension of fields, $[L\colon K] < \infty$. We can define $\operatorname{tr}\colon L \to K$, and a pairing $(\,,\,)\colon L \times L \to K$ where $(x, y) \mapsto \operatorname{tr}(xy)$.

Definition 6.2.2. We say L/K is separable if the pairing $(\,,\,)$ is non-degenerate. That is $(x, y) = 0$ for all y implies $x = 0$.

Theorem 6.2.3. *Let K/k be as before. Then there is a $T \in K$ transcendental over k such that $K/k(T)$ is separable.*

Exercise 6.2.4. If L/K is inseparable then

1. $\operatorname{char}(K) = p > 0$ (p prime, $p = 0$ in K).
2. $p \mid [L\colon K]$.

Example 6.2.5. Here is a typical xxample of inseparable extension:

$$\mathbb{F}_p(T) \hookrightarrow \mathbb{F}_p\left(T^{1/p}\right).$$

Main construction

Before we considered

$$\begin{array}{ccc} K & \longleftarrow & \mathcal{O}_K \\ \uparrow & & \uparrow \\ \mathbb{Q} & \longleftarrow & \mathbb{Z} \end{array}$$

where $\mathcal{O}_K$ is a ring of integers and is the integral closure of $\mathbb{Z}$ in K.

In the function field case, we take K is a separable extension of a subfield $k(T)$. Theorem 6.2.1 is true for $k(T)$ with $X = \mathbb{P}^1 = \operatorname{Proj} k[x_0, x_1]$ and $x_1/x_0 = T$.

Now consider the diagram

$$\begin{array}{ccc} K[x_0,x_1] & \longleftarrow & S \\ \uparrow & & \uparrow \\ k(T)[x_0,x_1] & \longleftarrow & k[x_0,x_1] \end{array}$$

where S is the integral closure of $k[x_0,x_1]$ in $K[x_0,x_1]$.

Some properties of S

1. S is Noetherian, because $K/k(T)$ is separable, by the same proof for $\mathcal{O}_K$ in the number field case.
2. Define a grading on $K[x_0,x_1]$ where $\deg a = 0$ if $a \in K$, $\deg x_0 = \deg x_1 = 1$. Then S is a graded ring.

Now $X := \mathrm{Proj}S$ will satisfy the requirements of the theorem. More precisely, we may reduced the arguments to affine case as follows: let $f: \quad \mathrm{Proj}S = X \longrightarrow \mathrm{Proj}k[x_0,x_1] = \mathbb{P}^1$ be the natural projection and cover $\mathbb{P}^1$ by open affines $U = \mathrm{Spec}k[1/T]$ and $\mathrm{Spec}k[T] = V$, then X is covered by $f^{-1}(U) = Y$, $f^{-1}(V) = Z$.

$$\begin{array}{ccccc} Y & \subseteq & X & \supseteq & Z \\ \downarrow & & \downarrow f & & \downarrow \\ U & \subseteq & \mathbb{P}^1 & \supseteq & V \end{array}$$

From the construction, one can show that

$$Y = \mathrm{Spec}(\text{integral closure of } k[T] \text{ in } K) = \mathrm{Spec}S[1/x_0]^{\deg 0}$$

$$Z = \mathrm{Spec}(\text{integral closure of } k[1/T] \text{ in } K) = \mathrm{Spec}S[1/x_1]^{\deg 0}.$$

Proof of Theorem 6.2.3

The theorem is trivial if the characteristic of K is 0. Now we assume $\mathrm{char}(K) = p > 0$. We want to prove the theorem. First a few preparations:

1) We can extend the definition of separability. Let K be a field. Let A be a finite K-algebra, we can define trace $A \times A \longrightarrow K$ via $(x,y) \mapsto \mathrm{tr}(xy)$. We say A/K is separable if and only if the pairing $(\,,\,)$ is non-degenerate.

Example 6.2.6. $K = \mathbb{F}_p(T^p)$, $L = \mathbb{F}_p(T)$ — this is not separable. This is because L has a basis $1, T, T^2, \ldots, T^{p-1}$ and T^i satisfies the minimal equation $x^p - (T^p)^i = 0$.

Let $\{x_1, \ldots, x_n\}$ be a base of A over K. Then A/K is separable if and only if $\det(\mathrm{tr}(x_i \cdot x_j)) \neq 0$. This follows from the formula:

$$\left(\sum_i c_i x_i, \sum_j d_j x_j\right) = \sum_{i,j} c_i d_j \mathrm{tr}(x_i x_j).$$

2) Separability is unchanged after base change. Let M, N be A-modules, we can define another A-module $M \otimes_A N$. If B is an A-algebra and M is an A-module then $M \otimes_A B$ is a B-module. Let A be a K-algebra and let L be a field containing K. Then $A \otimes_K L$ will be an L-algebra. $A = \sum Kx_i$. Since its an algebra $x_i x_j = \sum a_{ijk} x_k$. $A \otimes_K L = \sum Lx_i$.

Lemma 6.2.7. *A/K is separable if and only if $(A \otimes L)/L$ is separable.*

Proof. Both are equivalent to the fact that $\det(\mathrm{tr}(x_i x_j)) \neq 0$. □

3) Criterion of separability when K is algebraically closed:

Lemma 6.2.8. *If A is a finite K-algebra then $A = \oplus A_i$, where A_i are local K-algebras and $A_i = K \oplus M_i$ and M_i is a nilpotent A_i-ideal.*

Lemma 6.2.9. *Let A, B, be two K-algebras. Then $(A \oplus B)/K$ is separable if and only if A/K, B/K are separable.*

Lemma 6.2.10. *Let A be a local finite K-algebra with $K = \overline{K}$. Then A/K is separable if and only if $A = K$.*

Proof. Write $A = K + \mathfrak{m}$. Let $x \in \mathfrak{m}$, then for any $a \in A$, $ax \in \mathfrak{m}$ thus ax is nilpotent. Thus $(ax)^n = 0$ so $\mathrm{tr}(ax) = 0 \Longrightarrow (a, x) = 0$ for all a. So A/K is separable implies $A = K$. (Note that if matrix is nilpotent its trace is 0.) □

Exercise 6.2.11. Let A be a $n \times n$ matrix over a field K. Then if $A^m = 0$ for some m then $\mathrm{tr}(A) = 0$.

Combine all above, we have the following:

Theorem 6.2.12. *Let A be a finite K-algebra. Then A/K is separable if and only if $A \otimes \overline{K}$ is reduced, i.e., it has no nonzero nilpotent element.*

We have the following corollaries:

Corollary 6.2.13. *Let $L \supset F \supset K$ be a finite field extensions. Then L/K is separable iff L/F is separable and F/K is separable.*

Corollary 6.2.14. *Let L/K be a finite field extension which is generated by two subfield extensions F_1, F_2 ($K \subset F_i \subset L$, L is generated by F_1, F_2). Then L/K is separable if and only if F_1/K, F_2/K are both separable.*

Corollary 6.2.15. *Let L be a finite field extension of K which is generated by a single $x \in L$ ($L = K(x)$). Then L/K is separable if and only if the minimal equation of x over K is not of the form $F(T^p)$, $p = \mathrm{char}(K)$.*

Proof. Write $L = K[T]/G(T)$ where G is the minimal polynomial of x. Take a decomposition,

$$G(T) = \prod_{i=0}^{l} (x - \alpha_i)^{n_i}, \quad \alpha_i \in \overline{K}.$$

Then

$$L \otimes \overline{K} = \overline{K}[T]/G(T) = \frac{\overline{K}[T]}{\left(\prod_{i=0}^{l}(x-\alpha_i)^{n_i}\right)} = \oplus \frac{\overline{K}[T]}{(x-\alpha_i)^{n_i}}.$$

Here in the last step, we have used the Chinese Remainder Theorem: Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be two ideals in a ring R, such that $\mathfrak{p}_1 + \mathfrak{p}_2 = R$ and $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = 0$. Then $A = (R/\mathfrak{p}_1) \oplus (R/\mathfrak{p}_2)$.

Thus $(L \otimes \overline{K})/\overline{K}$is reduced if and only if $n_i = 1$. So L/K is separable if and only if $G(T)$ has no multiple zeros. This is equivalent to $G(T)$ and $G'(T)$ have no common zeros $\iff$ $G(T) \nmid G'(T) \iff G'(T) \neq 0$. Now suppose $G(T) = \sum a_i T^i$, $G'(T) = \sum i a_i T^{i-1}$, $ia_i = 0$ (in K) $\iff i = 0$ if $a_i \neq 0 \iff p \mid i$ if $a_i \neq 0 \iff G(T) = F(T^p)$ for some F. □

As a consequence, for a finite extension L/K there is a maximal subfield L' of L such that L'/K is separable. We call L' the *separable closure* of K in L.

If $x \in L$, $x \notin L'$ then x is not separable, so the minimal equation of x on K has the form $P(t^{p^c})$ where $c \geq 1$ and $P(X)$ is *not* of the form $Q(t^p)$ (i. e. c maximal). Thus t^{p^c} is separable over K, so $t^{p^c} \in L'$.

Definition 6.2.16. $[L : L']$ is called the degree of inseparability of $[L : K]$ (some power of p).

Proof of Theorem 6.2.3. Choose $t \in K$ such that the degree of inseparability of $K/k(t)$ is minimal. Want to show $K/k(t)$ is already separable. Let L be the separable closure of $k(t)$ in K.

Assume $K/k(t)$ is not separable. Then we have an $u \in K \setminus L$ such that $u^p \in L$. Then we have that u/k is transcendental, and that the minimal equation of u over $k(t)$ has the form $F(x^p) = 0$ with $F(x) = \sum_i a_i(t)x^i \in k(t)[x]$. Clean the denominators and take a non-trivial factor to obtain an irreducible $F(x) = G(x, t) \in k[t, x]$. Thus we have $G(t, u^p) = 0$.

Claim 6.2.17. *This equation is not an equation of t^p.*

Indeed, otherwise, every monomial is of power of p, so $G(t, u^p) = [G^*(t, u)]^p$ (char p). Therefore $G^*(t, u) = 0$, so $G(t, u)$ is not minimal. This proves the claim. Hence t is separable over $k(u)$.

If L' is the separable closure of $k(u)$ then $t \in L'$ which implies $L \subset L'$. We now have: Inseparability degree of $K/k(u)$ is $[K : L'] < [K : L]$, which contradicts with minimality of inseparability degree of $K/k(t)$. Thus $K/k(t)$ is separable. □

Exercise 6.2.18. Let $F(X, Y) \in k[X, Y]$ be an irreducible polynomial. Then $F(X, Y)$ is irreducible in $k(X)[Y]$.

6.3 Algebraic curves

Definition 6.3.1. Let $k = \overline{k}$ be an algebraic closed field.

1. By a projective curve over k we mean $X = \mathrm{Proj}S$, where S is an integral, graded, finitely generated k-algebra with $\dim X = 1$.

2. By the function field of X we mean

$$K(X) = \left\{ \frac{f}{g} \mid f, g \text{ homogenoeus of same degree} \right\}$$

   $K(X)/k$ is finitely generated, $\operatorname{tr\,deg} K(X)/k = 1$.

3. Assume S is generated by $x_1, \ldots, x_n$ homogeneous. Then X is covered by $\mathrm{Spec}S^0_{(x_i)}$, where

$$S^0_{(x_i)} = \left\{ \frac{f(X)}{x_i^n} \mid f \text{ homogeneous}, \deg f = n \deg x_i \right\} \subseteq K(X).$$

4. For every $x \in X$ we may define the local ring $\mathcal{O}_x \subset K(X)$ as follows: Let $x \in \mathrm{Spec}S^0_{(x_i)}$. Then x corresponds to a prime ideal $\mathfrak{p}$ of $S^0_{(x_i)}$. Then put

$$\mathcal{O}_x = \left(S^0_{(x_i)}\right)_{(\mathfrak{p})}.$$

   Alternatively, x corresponds to a homogeneous prime ideal $\mathfrak{q}$ in S, $\mathcal{O}_x = S^0_{(\mathfrak{q})}$.

5. We may say that X is regular if $\mathcal{O}_x$ is regular for every $x \in X$. Equivalently, $\mathcal{O}_x$ is a discrete valuation ring in K (if $x \neq (0)$).

Theorem 6.3.2. *There is a 1 – 1 correspondence between the set of closed points $|X|$ and the set of discrete valuations of $K(X)$.*

The correspondence $X \longrightarrow K(X)$ gives a bijection between the "set" of regular projective curves over k and the set of extensions of k which are finitely generated of transcendental degree 1.

Example 6.3.3. $k(t) \longleftrightarrow \mathbb{P}^1$.

$$k\left(t, \sqrt{t(t-1)(t-2)(t-3)}\right) \longleftrightarrow s^3y^2 = t(t-s)(t-2s)(t-3s)$$

in $\mathbb{P}^2$, s — homogenizer. Exercise: show that this curve is regular.

Moreover, if $K(X_1) \hookrightarrow K(X_2)$ we can define $\phi\colon X_2 \to X_1$. Moreover each point $x \in X_2$ gives a discrete valuation ring $R_x \subset K(X_2)$. The intersection $R_x \cap K(X_1)$ is a discrete valuation ring in $K(X_1)$, so it is equal to R_y for some $y \in X_1$. Define $y = \phi(x)$. For $y \in X_1$

$$\phi^{-1}(y) = \Big|\mathrm{Spec}\big(\text{int. closure of } R_y \text{ in } K(X_2)\big)\Big|.$$

Zeros and poles of functions on curves

Let X be a regular projective curve. Let $f \in K(X)$. Let $x \in X$ with local ring $\mathcal{O}_x$ (i. e. $\mathcal{O}_x$ is a discrete valuation ring in $K(X)$). Let π be a uniformizer of $\mathcal{O}_x$ (we call π a uniformizer for x as well). We can write $f = u\pi^n$, $u \in \mathcal{O}_x^*$ ($K(X) = \mathrm{Frac}(\mathcal{O}_x)$). Then we put $\mathrm{ord}_x(f) = n$ (the order of f at x).

If $\mathrm{ord}_x(f) = n > 0$, we say x is a *zero* of f of *order* n.
If $\mathrm{ord}_x(f) = -n > 0$, we say x is a *pole* of f of *order* n.
If $\mathrm{ord}_x(f) = n \geq 0$, we say f is *regular at* x.
If $\mathrm{ord}_x(f) = 0$, we say f is *invertible at* x (regular and nonzero).

Example 6.3.4. $X = \mathbb{P}^1$, $K(X) = k(t)$. Let $a \in \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$. Then

$$\mathcal{O}_a = \begin{cases} k[t]_{(t-a)}, & \text{if } a \neq \infty, \\ k\left[\frac{1}{t}\right]_{(0)}, & \text{if } a = \infty. \end{cases}$$

Let $f \in k(t)$, then

$$f(t) = \frac{G(t)}{F(t)} = \prod_{i=0}^{n} (t - a_i)^{\alpha_i}, \qquad \alpha_i \in \mathbb{Z}.$$

$$\mathrm{ord}_a(f) = \begin{cases} \alpha_i, & \text{if } a = a_i, \\ -\sum \alpha_i, & \text{if } a = \infty, \\ 0 & \text{otherwise.} \end{cases}$$

Two facts for $\mathbb{P}^1$.

1. If $f \in K(\mathbb{P}^1) = k(t)$ is invertible everywhere, then f is a constant.
2. $$\sum_{x \in \mathbb{P}^1} \mathrm{ord}_x(f) = 0.$$

We will prove these facts hold for any projective curve.

Theorem 6.3.5. *Let X be a projective regular curve over an algebraically closed field k. Let $f \in K(x)$ be a non-zero rational function. Then*

1. $\mathrm{ord}_x(f) = 0$ *for almost all* $x \in |X|$.
2. $\sum_x \mathrm{ord}_x(f) = 0$.
3. *If* $\mathrm{ord}_x(f) = 0$ *for all* x *then* f *is constant, i. e.* $f \in k$.

Proof. 1) We can cover X by finitely many affine schemes $U_i = \mathrm{Spec} A_i$ with A_i a Dedekind domain. Then $K(X)$ is also the function field of A_i. Write $(f) = \prod_{i=1}^{n} \mathfrak{p}_i^{n_i}$, $n_i \in \mathbb{Z}$, $\mathfrak{p}_i$ prime ideals in A_i. If $\mathfrak{p}_i$ corresponds to a point x_i in X, then $n_i = \mathrm{ord}_{x_i}(f)$. Thus on each U_i, f has only finitely many zeroes or poles.

2) and 3) If $f \notin k$ then f is transcendental over k. Let $L = k(f) \hookrightarrow K(X)$. This induces a map $X \xrightarrow{Q} \mathbb{P}^1$ such that $f = Q^*(T) := T \circ Q$. Thus Q is surjective. Moreover for each point y in $\mathbb{P}^1$, $Q^{-1}(y)$ is the set of x such that the valuations corresponding to x in $K = K(X)$ induce the valuation corresponding to y in L. The theorem follows from the following claim:

$$[K : L]\mathrm{ord}_y(T) = \sum_{x \to y} \mathrm{ord}_x(f).$$

It is clear that both all terms are zero (resp. positive, resp. negative) when $y \neq 0, \infty$ (resp. $y = 0$, resp. $y = \infty$). Thus we need only work on when $y = 0$ and $y = \infty$. Change coordinates $T \longrightarrow 1/T$, we may switch 0 and ∞. Thus need only work on $y = 0$.

Let R be the valuation ring in L corresponding to $y = 0$. Then $T = f$ is a uniformizer, and $\mathrm{ord}_y(T) = 1$. Let A be the integral closure of R in K. Then A is a free k-module of rank $[K : L]$ and $Q^{-1}(y)$ equals the set of all primes in A. Then A is a free R-module of rank $n := [L : K]$. Thus we have $A \simeq R^n$ and $A/fA \simeq (R/fR)^n$. Write

$$fA = \prod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(f)},$$

Then by Chinese remainder theorem,

$$A \Big/ \prod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(f)} A \simeq \bigoplus_{\mathfrak{p}} A \Big/ \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(f)}$$

Thus we have shown that

$$n = \dim(R/fR)^n = \dim A \Big/ \prod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(f)} A = \sum_{\mathfrak{p}} \dim A \Big/ \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(f)} = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f).$$

□

Recall that if R is a Dedekind domain we have

$$0 \to \{\text{principal ideals}\} \to \{\text{fractional ideals}\} \to \{\text{ideal class group}\} \to 0.$$

$$0 \longrightarrow R^X \longrightarrow K^X \longrightarrow \{\text{principal ideals}\} \longrightarrow 0, \qquad f \longmapsto (f).$$

Analogue for curve X

The group of *divisors* on X is a free Abelian group generated by points in X,

$$\mathrm{Div}(X) = \left\{ D = \sum_i n_i x_i, \quad n_i \in \mathbb{Z}, x_i \in |X| \right\}.$$

For a divisor $D = \sum n_i x_i$ we denote $n_i = \mathrm{ord}_{x_i}(D)$.

A divisor D is called *principal* if $D = \sum_x \mathrm{ord}_x(f)x$ for some function f in $K(X)$. We denote by $\mathrm{Pr}(X)$ the subgroup of principal divisors in $\mathrm{Div}(X)$. The factor group

$$\mathrm{Div}(X)\Big/\mathrm{Pr}(X)$$

is known as the Picard group of X.

$$0 \longrightarrow \mathrm{Pr}(X) \longrightarrow \mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow 0.$$

The degree of a divisor $D = \sum n_i x_i$ is defined by $\deg D = \sum_i n_i$. We denote by $\mathrm{Div}^0(X)$ the subgroup of the divisors of zero degree. We have the following exact sequences:

$$0 \longrightarrow \mathrm{Div}^0(X) \longrightarrow \mathrm{Div}(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0,$$

$$0 \longrightarrow \mathrm{Pr}(X) \longrightarrow \mathrm{Div}^0(X) \longrightarrow \mathrm{Pic}^0(X) \longrightarrow 0.$$

$\mathrm{Pic}^0(X)$ is known as the Jacobian variety of X.

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow k^* \longrightarrow K^* \longrightarrow \mathrm{Pr}(X) \longrightarrow 0, \qquad f \longmapsto \sum \mathrm{ord}_x(f)[x].$$

Theorem 6.3.6. $\mathrm{Pic}^0(X)$ *has a natural variety structure which is connected of dimension* $2g$*, where* g *is the genus of* X*.*

The Jacobian variety $Pic^0(X) = \mathbb{C}^g/\Lambda$, where Λ is a $\mathbb{Z}$-lattice of rank $2g$ in $\mathbb{C}^g$.

Example 6.3.7. $X = \mathbb{P}^1$,

$$\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)\Big/\mathrm{Pr}(X) = 0.$$

Proof. Let $D = \sum n_i \alpha_i$ be a zero degree divisor. Define $f = \prod(x - \alpha_i)$ taking product over all $\alpha_i \neq \infty$. Thus D is the principal divisor corresponding to f. □

6.4 Differentials

Let $A \hookrightarrow B$ be rings. The set of differentials $\Omega_{B/A}$ is a free B-module generated by "dB" modulo Leibniz relations:

$$dab = a\,db + b\,da, \quad d(a+b) = da + db, \quad da = 0 \ \text{ if } \ a \in A.$$

There is a map $d\colon B \to \Omega_{B/A}$, satisfies Leibniz rule.

Universal Property of the map $B \xrightarrow{d} \Omega_{B/A}$: Let M be a B-module, let $\delta\colon B \to M$ be a homomorphism of A-modules, such that $\delta(ab) = a\delta(b) + b\delta(a)$. Then there is a unique B-module homomorphism $Q\colon \Omega_{B/A} \to M$ such that $\delta = Q \circ d$.

Proposition 6.4.1. *Let K be a function field of an algebraic curve over an algebraically closed field k, then $\Omega_{K/k}$ is a free K-module of rank 1.*

Proof. There is a $T \in k$ such that T is transcendental over k and $K/k(T)$ is algebraic and separable.

Claim 6.4.2. $K \cdot dT = \Omega_{K/k}$.

Construct a differential map $K \to K\,dT$. Let $x \in K$, let $p(T,S) \in k(T,S)$ be the irreducible minimal polynomial for x in $k(T)$. Since $p(T,x) = 0$, $dp(T,x) = 0$, so

$$\frac{\partial p}{\partial T}\,dT + \frac{\partial p}{\partial x}\,dx = 0$$

in $\Omega_{K/k}$. Since $K/k(T)$ is separable then $\partial p/\partial x \neq 0$. So

$$dx = \frac{\frac{\partial p}{\partial T}}{\frac{\partial p}{\partial x}}\,dT.$$

Define $d\colon K \to K\,dT$ by the formula above. Then d really satisfies Leibniz rule and the universal property of $\Omega_{K/k}$. Therefore $K \cdot dT = \Omega_{K/k}$. □

We have:

$$\begin{aligned} 0 &\longrightarrow \mathrm{Div}^0(X) \longrightarrow \mathrm{Div}(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0, \\ 0 &\longrightarrow \mathrm{Pr}(X) \longrightarrow \mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow 0, \\ 0 &\longrightarrow \mathrm{Pr}(X) \longrightarrow \mathrm{Div}^0(X) \longrightarrow \mathrm{Pic}^0(X) \longrightarrow 0. \end{aligned}$$

Let $dT \in \Omega_{K/k}$ be a generator. Let $x \in X$ be a point with a local parameter π. $T = \sum a_n \pi^n$, $a_n \in K$ the Taylor expansion,

$$dT = \left(\sum_n n a_n \pi^{n-1}\right) d\pi, \qquad \frac{dT}{d\pi} \in K^X,$$

so $d\pi \neq 0$.

Let $\alpha \in \Omega_{K/k}$ be a nonzero differential, then we define formally

$$\mathrm{Div}(\alpha) = \sum_x \mathrm{ord}_x\left(\frac{\alpha}{d\pi_x}\right) \cdot x,$$

where π_x is a local parameter at x. We will show that the right hand side has only finitely many nonzero terms and this defines a divisor. The divisor of this class does not depend on the choice of α:

$$\mathrm{div}(f\alpha) = \mathrm{div}(f) + \mathrm{div}(\alpha).$$

divisor class is called the *canonical divisor class*, and is denoted by K_X.

For example when $X = \mathbb{P}^1$ with affine coordinate T, dT is a differential with no-zero or pole in the finite point, at the infinite point, it has local parameter $\pi = 1/T$. Thus

$$dT = d(\pi^{-1}) = -\pi^{-2}d\pi.$$

Thus $\operatorname{div}(dT) = -2\infty$.

Let $Q : X \to Y$ be a morphism of curves, we define formally

$$\operatorname{Div}(\Omega_{X/Y}) = \sum_x \operatorname{ord}_x(\Omega_{\mathcal{O}_x/\mathcal{O}_{Q(x)}})[x]$$

We want to show that this is a finite sum and this defines a divisor. Cover $X = \bigcup_i \operatorname{Spec} B_i$,

$$\Omega_{B_i/A_i} = \bigoplus_{x \in \operatorname{Spec} B_i} \mathcal{O}_x \Big/ \pi_x^{n_x}$$

is a torsion B_i-module. Here $n_{x^i} = \operatorname{ord}_x \Omega_{B^i/A}$, $n_x = 0$ for almost all x. Thus $\Omega_{X/Y}$ is a divisor. The divisor $\operatorname{div}(\Omega_{X/Y})$ is called the ramification divisor for the map $Q\colon X \to Y$ and is denoted by $R_{X/Y}$.

Let $Q : X \to Y$ be a morphism of curves and let $y \in Y$, we define $Q^* : \operatorname{Div}(Y) \to \operatorname{Div}(X)$ such that

$$Q^*(y) = \sum_{x \to y} \operatorname{ord}_x(\pi_y)[x]$$

For each $y \in Y$, write $Q^{-1}(y) = x_1, \ldots, x_r$. π = uniformizer of $\mathcal{O}_y$, π_i = uniformizer of x_i, $\pi = \prod \pi_i^{e_i}$ (units), $e_i - 1$ is called the ramification index. One has $\sum e_i = n$.

We say $Q\colon X \to Y$ is *tamely ramified* if for any $x \in X$ $p \nmid e(x)$.

Formula: if Q is tamely ramified then

$$R_{X/Y} = \sum_x (e(x) - 1)x.$$

Proof. Let y be an image of x, $\mathcal{O}_y \hookrightarrow \mathcal{O}_x$ with the local coordinates π_y and π_x respectively. The Taylor expansion $\pi_y = \pi_x^e \alpha = \pi_x^e + a_1 \pi_x^{e+1} + \ldots$ leads to

$$d\pi_y = \big(e\pi_x^{e+1} + \ldots\big)d\pi_x = \pi_x^{e-1}\big(e + \pi_x + \ldots\big)d\pi_x.$$

Therefore $\operatorname{ord}_x(d\pi_y) = e - 1$ but $\operatorname{ord}_y(d\pi_y) = 0$, so $\operatorname{ord}_x R_{X/Y} = \operatorname{ord}_x(d\pi_y)$. □

Theorem 6.4.3. *Let $Q\colon X \to Y$ be a separable morphism, let α be a non-zero differential on Y, then*

$$\operatorname{div}(Q^*\alpha) = Q^*\Big(\operatorname{div}(\alpha)\Big) + \operatorname{div}\left(\Omega_{X/Y}\right).$$

and every item in the equality is finite.

Proof. The first part can be proved locally. For the finiteness of $\operatorname{div}(\alpha)$ for any $\alpha \in \Omega_X$ follows from the equation in the theorem as we may apply it to $X \to \mathbb{P}^1$. □

Definition 6.4.4. The *genus* $g(X)$ of X is an integer defined by

$$2g(X) - 2 = \deg(\operatorname{div}(\alpha)) = \deg K_X.$$

Corollary 6.4.5 (Hurwitz formula)**.**

$$2g(X) - 2 = \deg Q \cdot \big(2g(Y) - 2\big) + \deg R_{X/Y}.$$

Example 6.4.6. $\mathbb{P}^1 = k \cup \{\infty\}$. If $x \in k$ then $d(T - x) = dT$, so $\operatorname{ord}_x(dT) = 0$ if $x \in k$. If $x = \infty$ we have a local coordinate $\pi_\infty = 1/T$, so $T = 1/\pi_\infty$ and

$$dT = d\left(\frac{1}{\pi_\infty}\right) = -\frac{1}{\pi_\infty^2}\, d\pi_\infty.$$

Thus $\operatorname{ord}_\infty(dT) = -2$, $\operatorname{div}(dT) = -2(\infty)$ and $2g - 2 = -2$. Therefore the genus $g = 0$.

Example 6.4.7. $y^2 = x(x-1)(x-2)(x-3)$. Show $Q\colon X \to \mathbb{P}^1$ is smooth everywhere except $x = 0, 1, 2, 3$ where $e = 2$. Note $\deg Q = 2$. Assume Q is tamely ramified. Then for the genus we have

$$2g(X) - 2 = \deg Q\big(2g(\mathbb{P}^1) - 2\big) + \sum_x (e_x - 1) = 2(-2) + 4 = 0,$$

so $g(X) = 1$.

Final exam problems

1. Show that $R = \mathbb{Z}[e^{2\pi i/p}]$ is regular for p prime by the following steps:

   Step 1 Let $K = \mathbb{Q}(e^{2\pi i/p})$, we want to show $R = \mathcal{O}_K$. We have a pairing $K \times K \to \mathbb{Q}$. For $M \subset K$ a $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, define the discriminant $\operatorname{dis}(M) \in \mathbb{Q}^\times$. Show that $\operatorname{dis}(M) \in \mathbb{Z}$ if M is a subalgebra.

   Step 2 If $M_1 \subset M_2$ then $\operatorname{dis}(M_2) \mid \operatorname{dis}(M_1)$, and $p \nmid \operatorname{dis}(M_1)/\operatorname{dis}(M_2)$ then $M_{1,p} = M_{2,p}$. This implies that if $p \nmid \operatorname{dis}(R)$ then $R_p = \mathcal{O}_{K,p}$.

   Step 3 Show that R_p is a discrete valuation ring if $p \mid \operatorname{dis}(R)$ then we are done.

2. Let $f(x, y, z)$ be a homogeneous polynomial of degree d. Compute the Hilbert polynomial of $S = \mathbb{C}[x, y, z]/(f)$.

3. Let A be a ring, $m, n \in \mathbb{N}$ and let $Q\colon A^m \to A^n$ be an injective homomorphism of A-modules. Prove $m \leq n$ in the following steps:

   Step 1 Express Q by a matrix $A = (a_{ij})$:

   $$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$$

   There exists $\mathfrak{p}$ prime, $\exists\, a_{ij}$ such that $a_{ij} \notin \mathfrak{p}$. By localization principle, we may replace A by $A_\mathfrak{p}$ and then assume that A is local and that a_{ij} is invertible.

Step 2 Assume that A is local and a_{ij} is invertible. By doing row-column operations so we get the following $m \times n$ matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2m} \\ \vdots & & \ddots & \vdots \\ 0 & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

This step reduces claim for an injective morphism $A^m \to A^n$ to an injective morphism $A^{m-1} \to A^{n-1}$.