National Institute of Science Education and Research

School of Mathematical Sciences

M498: Project-I

Arithmetic Geometry - I

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

Supervisor
Prof. Brundaban Sahu
Reader-F
brundaban.sahu@niser.ac.in

November 17, 2017

Plagiarism statement

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

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

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

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

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

Signed: _____ Date: _____

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

Abstract

This report introduces the reader to the notion of integral closure, rings of dimension one and algebraic curves.

Acknowledgements

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

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

Contents

Introduction

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

Commutative algebra is essentially the study of commutative rings with the central notion being that of a prime ideal. The prime ideals provide a common generalization of the primes of arithmetic and the points of geometry. Prominent examples of commutative rings include polynomial rings, rings of algebraic integers, including the ordinary integers $\mathbb{Z}$, and p-adic integers.

In the first chapter we will see topics from commutative algebra, with basic theme being the concept of integral closure of a ring. As discussed in my 2016 summer internship project report [Kor16a, Ch. 1], in algebraic number theory we study the integral closure $\mathcal{O}_L$ of the ring of integers $\mathbb{Z}$ in a finite extension $L/\mathbb{Q}$, where L is obtained by adjoining to the field $\mathbb{Q}$ a root α of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. In this chapter, we will take a step backwards and try to understand the basic properties we can associate to the integral closure of a ring in general.

In algebraic geometry one associates to a non-singular plane curve given by an equation $f(x, y) = 0$, $f \in k[x, y]$ for any field k, its ring of functions $B = f[x, y]/(f)$ and its function field L (the field of fractions of the integral domain B). The field L is obtained by adjoining to the field $k(x)$ a root of the polynomial $f \in k(x)[y]$. If, in addition, $f(x, y)$ is monic in y, then the ring B is the integral closure of the ring $k[x]$ in L. From a commutative algebra prospective, both quadruples $(\mathbb{Z}, \mathbb{Q}, \mathcal{O}_L, L)$ and $(k[x], k(x), B, L)$ are instances of same phenomenon.

In the second chapter we will see topics from algebraic geometry, with basic theme being the theory of elliptic curves. As discussed in my 2015 summer internship project report [Kor15, §1.8], the study of the group of points of an elliptic curve over the field of rational numbers is one of the fundamental objects of study in arithmetic geometry. In this chapter, we will take a step backwards and try to understand the basic properties of algebraic curves in general using elliptic curves as our source of motivation.

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

Chapter 1

Integral Closure

1.1 Introduction

Definition 1.1 (Minimal polynomial)**.** Let K be any field and L/K be a finite extension. Given an element α on L, we have following ring homomorphism[1]

$$\begin{aligned}\phi :& K[x] \to L \\ & h(x) \mapsto h(\alpha)\end{aligned}$$

Since L is an integral domain, the kernel of this homomorphism is a prime ideal I of $K[x]$. Since $K[x]$ is a principal ideal domain, the prime ideal I is generated by an irreducible polynomial. The *minimal polynomial of* α over K is the unique monic irreducible polynomial $g(x)$ in $K[x]$ that generates the ideal I.

Example 1.1. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{2}]$, then $f(x) = x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$.

Lemma 1.1. *Let L/K be a Galois extension with Galois group $\mathrm{Gal}(L/K)$ and $R \subseteq L$ be a subring such that $\tau(R) = R$ for all $\tau \in \mathrm{Gal}(L/K)$. Then the minimal polynomial over K of any element of R has coefficient in $R \cap K$.*

Proof. See Lemma I.2.1 of [Lor96]. □

Definition 1.2 (Integral element)**.** Let R be a subring of a ring S. An element α of S is said to be *integral over* R if it is the root of a monic polynomial $f(x)$ in $R[x]$.

Example 1.2. Let $S = \mathbb{Z}[\sqrt{2}]$ and $R = \mathbb{Z}$, then $\sqrt{2}$ is integral over $\mathbb{Z}$.

Definition 1.3 (Integral extension)**.** Let R be a subring of a ring S. The ring S is said to be integral over R, or to be an *integral extension* of R, if every element of S is integral over R.

Example 1.3. Let $S = \mathbb{Z}[\sqrt{2}]$ and $R = \mathbb{Z}$, then $\mathbb{Z}[\sqrt{2}]$ is integral extension of $\mathbb{Z}$ since $\alpha = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is root of $f(x) = x^2 - 2mx + m^2 - 2n^2$.

Proposition 1.1. *Let L/K be a Galois extension with Galois group $\mathrm{Gal}(L/K)$ and $R \subseteq L$ be a subring such that $\tau(R) = R$ for all $\tau \in \mathrm{Gal}(L/K)$. Then every element of R is integral over $R \cap K$, or equivalently, R is an integral extension of $R \cap K$.*

Proof. Follows from previous lemma. □

Theorem 1.1. *Let R be a ring of a field K and $\alpha \in K$. The following statements are equivalent:*

[1] Since the dimension of L as a K-vector space is finite but $K[y]$ is not a finite dimensional K-vector space, it follows that the homomorphism ϕ cannot be injective.

(i) *The element α is integral over R.*

(ii) *The subring $R[\alpha]$ of K, generated by R and α, is finitely generated R-module.*

(iii) *There exists a finitely generated R-submodule M of K such that $\alpha M \subseteq M$.*

Proof. See Proposition I.2.10 of [Lor96]. □

Corollary 1.1. *Let R be a subring of a field K. The set S consisting of all elements of L that are integral over R is a ring.*

Proof. Follows from part (iii) of previous theorem. □

Definition 1.4 (Integral closure)**.** Let R be a subring of a field K. The *integral closure* S of R in K is the ring of elements of K integral over R.

Example 1.4. Let $K = \mathbb{Q}[\sqrt{5}]$ and $R = \mathbb{Z}$, then $S = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Definition 1.5 (Integrally closed)**.** An integral domain R is said to be *integrally closed* if it is equal to its integral closure in its field of fractions.

Example 1.5. Let $R = \mathbb{Z}$, its field of fractions is $\mathbb{Q}$. Since the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$ itself (roots of linear polynomials), $\mathbb{Z}$ is integrally closed.

Proposition 1.2. *A unique factorization domain R is integrally closed.*

Proof. See Lemma I.2.16 of [Lor96]. □

Proposition 1.3. *Let R be an integral domain, integrally closed in its field of fractions K. Let α be an algebraic element over K, with minimal polynomial $g(x) \in K[x]$. The element α is integral over A if and only if its minimal polynomial has coefficients in R.*

Proof. See Lemma I.2.17 of [Lor96]. □

Corollary 1.2. *Let K be the field of fractions of a unique factorization domain R and L/K be a finite extension. Then $\alpha \in L$ is integral over R if and only if its minimal polynomial has coefficients in R.*

Proof. It's enough to prove that every unique factorization domain is integrally closed in its field of fractions.

Let $\alpha \in K$ be a root of some monic polynomial $f(x) \in R[x]$. We can express α as $\frac{a}{b}$ with $a, b \in R$, and using unique factorization we may assume that no irreducible of R divides both a and b. If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in R[x]$, then plugging in α and multiplying through by b^n we obtain

$$a^n + c_{n-1}ba^{n-1} + \cdots + c_0 b^n = 0$$

Now, $c_{n-1}ba^{n-1} + \cdots + c_0 b^n$ is divisible by b, hence a^n is divisible by b. Since no irreducible of R divides both a and b, it follows that b must be a unit by unique factorization. Hence $\alpha \in R$. □

Proposition 1.4. *Let A, B and C be three integral domains such that $A \subseteq B \subseteq C$. Then C is integral over A if and only if C is integral over B and B is integral over A.*

Proof. See Proposition I.2.18 of [Lor96]. □

Theorem 1.2. *Let R be an integral domain and K be its field of fractions. Let L/K be a finite extension. Let S be the integral closure of R in L.*

(i) *Let $\alpha \in L$, then there exist $s \in S$ and $r \in R$ such that $\alpha = s/r$. In particular, L is the field of fractions of S.*

(ii) *S is integrally closed.*

(iii) *If R is integrally closed,, then $S \cap K = R$.*

(iv) *If L/K is Galois with Galois group $\mathrm{Gal}(L/K)$, then $\tau(S) = S$, for all $\tau \in \mathrm{Gal}(L/K)$. Moreover, if R is integrally closed, then $R = \{s \in S : \tau(b) = b, \forall \tau \in \mathrm{Gal}(L/K)\}$.*

Proof. See Proposition I.2.19 of [Lor96]. □

Corollary 1.3. *Let R be an integral domain and K be its field of fractions. If L/K is an extension of degree n and S is the integral closure of R in L, then S contains a basis $\{e_1, \ldots, e_n\}$ of the K-vector space L.*

Proof. Follows from part (i) of previous theorem. □

Definition 1.6 (Chain complex)**.** A set of R-modules $\{M_i\}_{i\in\mathbb{Z}}$ and a set of homomorphisms of R-modules $\delta_i : M_i \to M_{i+1}$

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\delta_{i-1}} M_i \xrightarrow{\delta_i} M_{i+1} \longrightarrow \cdots$$

are called a *chain complex*, if image of δ_{i-1} is a subset of the kernel of δ_i, i.e. $\mathrm{Im}(\delta_{i-1}) \subseteq \mathrm{Ker}(\delta_i)$, for all $i \in \mathbb{Z}$.

Definition 1.7 (Exact sequence)**.** A chain complex of R-modules and R-module homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\delta_{i-1}} M_i \xrightarrow{\delta_i} M_{i+1} \longrightarrow \cdots$$

is *exact* at M_i if $\mathrm{Ker}(\delta_i) = \mathrm{Im}(\delta_{i-1})$. The chain complex is an *exact sequence* if it is exact at each M_i.

Definition 1.8 (Short exact sequence)**.** A *short exact sequence* is a five-term exact sequence of the form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Remark 1.1. Equivalently, a five-term chain complex is a short exact sequence if

(i) f is injective

(ii) g is surjective

(iii) $\mathrm{Ker}(g) = \mathrm{Im}(f)$

Lemma 1.2. *Consider the following short exact sequence of R-modules*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Then M is finitely generated R-module if both M' and M'' are finitely generated R-modules. Moreover, if M is a finitely generated R-module, then M'' is a finitely generated R-module.

Proof. See Lemma I.4.19 of [Lor96]. □

Definition 1.9 (Noetherian module)**.** An R-module M is called noetherian if every submodule of M is finitely generated as an R-module.

Theorem 1.3. *Let R be any commutative ring and M be any R-module. The following statements are equivalent:*

(i) M is noetherian R-module.

(ii) Every increasing sequence $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n \subseteq \ldots$ of submodules of M is stationary (i.e., there exists n such that $M_n = M_{n+1} = \ldots$).

(iii) Every nonempty subset of the set of submodules of M has a maximal element.

Proof. See Proposition I.4.13 of [Lor96]. □

Proposition 1.5. *Consider the following short exact sequence of R-modules*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Then M is noetherian if and only if M' and M'' are noetherian.

Proof. See Proposition I.4.20 of [Lor96]. □

Corollary 1.4. *Let $\{M_i\}_{i=1}^n$ be a set of noetherian R-modules. Then the module $M = \oplus_{i=1}^n M_i$ is noetherian.*

Proof. See Corollary I.4.21 of [Lor96]. □

Definition 1.10 (Noetherian ring)**.** A ring in which every ideal is finitely generated is called *noetherian*.

Example 1.6. Since principal ideal domains are noetheiran, we conclude that the polynomial ring $R = k[x]$ is noetherian.

Remark 1.2. If R is noetherian and $I \subseteq R$ is any ideal, then R/I is noetherian. Hence, $k[x]/(x^2)$ is also noetherian. Also, a ring R is noetherian if and only if it is a noetherian R-module.

Theorem 1.4. *Let R be a noetherian ring. Then every submodule of a finitely generated R-module is finitely generated.*

Proof. Let M be a finitely generated R-module and $m_1, \ldots, m_s$ be a system of generators of M. Let $\oplus_{i=1}^s Re_i$ denote the free R-module of rank s with basis $\{e_1, \ldots, e_s\}$. Consider the short exact sequence

$$0 \longrightarrow \mathrm{Ker}(g) \longrightarrow \bigoplus_{i=1}^{s} Re_i \xrightarrow{g} M \longrightarrow 0$$

with $g(\sum_{i+1}^s a_i e_i) = \sum_{i=1}^s a_i m_i$ and the map $\mathrm{Ker}(g) \to \oplus_{i=1}^s Re_i$ being the inclusion map. Since R is noetherian, it follows from Corollary 1.4 that $\oplus_{i=1}^s Re_i$ is also noetherian. Hence, Proposition 1.5 shows that M is noetherian. □

Corollary 1.5. *Let $R \subseteq S$ be two rings. If R is noetherian and S is finitely generated R-module, then S is noetherian.*

Proof. See Corollary I.4.5 of [Lor96]. □

Theorem 1.5 (Hilbert's Basis Theorem)**.** *Let R be a noetherian ring. Let S be a finitely generated R-algebra. Then S is a noetherian ring.*

Proof. See Theorem II.10.1 of [Lor96]. This is the generalization of Corollary 1.5. □

Proposition 1.6. *Let R be an integral domain, integrally closed in its field of fractions K. Let L/K be a separable extension of degree n. Let $\{e_1, \ldots, e_n\} \subset S$ be a basis of L over K. Then there exists a non-zero element $d \in R$ such that the R-module S is contained in the free R-module generated by $e_1/d, \ldots, e_n/d$, that is:*

$$Re_1 \oplus \ldots \oplus Re_n \subseteq S \subseteq R\frac{e_1}{d} \oplus \ldots \oplus R\frac{e_n}{d} \subseteq L$$

Proof. See Proposition I.4.8 of [Lor96]. □

Theorem 1.6. *Let R be a noetherian domain, integrally closed in its field of fractions K. Let L/K be a finite extension. Then the integral closure S of R in L is a finitely generated R-module. In particular, S is a noetherian ring.*

Proof. Theorem 1.4 shows that to prove S is a finitely generated R-module, it is sufficient to show that S is R-submodule of a finitely generated R-module. Proposition 1.6 implies that S is an R-submodule of a free finitely generated R-module. □

Proposition 1.7 (Structure theorem for finitely generated modules over principal ideal domains)**.** *Let R be a principal ideal domain and let M be a finitely generated R-module.*

(i) Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus \ldots \oplus R/(a_m)$$

for some integer $r \geq 0$ and non-zero elements $a_1, \ldots, a_m$ of R which are not units in R and which satisfy the divisibility relations $a_1 \mid a_2 \mid \ldots \mid a_m$.

(ii) M is torsion free if and only if M is free.

(iii) In the decomposition in (i),

$$Tor(M) \cong R/(a_1) \oplus \ldots \oplus R/(a_m)$$

In particular, M is a torsion module if and only if $r = 0$ and in this case the annihilator of M is the ideal (a_m).

Proof. For proof see Theorem 12.5 of [DF11]. □

Proposition 1.8. *Let R be a principal ideal domain and L be a finite separable extension of the field of fractions of R. Then the integral closure S of R in L is a free finitely generated R-module.*

Proof. Follows from Theorem 1.6 and Proposition 1.7. See Corollary I.4.9 of [Lor96]. □

Lemma 1.3. *Let K be the field of fractions of a domain R, L/K be a finite extension of degree n and S be the integral closure of R in L. If S is a free finitely generated R-module, then the rank of S over R is equal to n.*

Proof. Follows from part (i) of Theorem 1.2. See Lemma I.4.10 of [Lor96]. □

Definition 1.11 (Integral basis)**.** Let R be a subring of a field L and S be the integral closure of R in L. When S is a free finitely generated R-module, we call a basis $\{b_1, \ldots, b_n\}$ of S over R an *integral basis* of S.

Example 1.7. The sets $\{1, \sqrt{d}\}$ and $\{1, (1+\sqrt{d})/2\}$ are integral bases over $\mathbb{Z}$ for the ring of integers $\mathbb{Q}[\sqrt{d}]$, when $d \equiv 2, 3 \pmod 4$ and $d \equiv 1 \pmod 4$ respectively. For details, see Section 2.3 of [Kor16a].

1.2 Quadratic Extension of Function Field

Much of the formalism in the theory of number fields carries over to a class of fields of prime characteristic, known as function fields. The function fields we consider in this section are the finite extensions of the fields of rational functions $k(x)$ in a single indeterminate x, for some field k of prime characteristic.

In this section, let $R = k[x]$ and $K = k(x)$. Let $f(x) \in R$ be a square-free polynomial[2] and $\sqrt{f}$ denote a root[3] in $\overline{K}$ of the monic polynomial $y^2 - f(x) \in R[y]$. Set $L = K(\sqrt{f})$. Since the element $\sqrt{f}$ is clearly integral over R, we can easily check that every element of $R[\sqrt{f}]$ is integral over R.

Our motive is to describe the R-module structure of the integral closure S of R in L. We will divide our discussion into two subsections, when k is not of characteristic 2 and when it is of characteristic 2.

1.2.1 k is not of characteristic 2

Claim 1. $S = R[\sqrt{f}]$

Since R is a unique factorization domain, we can use Corollary 1.2 to prove this claim. Let $\alpha = m + n\sqrt{f} \in L$ with $m, n \in K$. If $n = 0$ then the minimal polynomial of α over K is the linear polynomial $y - \alpha \in K(y)$. Hence by Corollary 1.2, α is integral over R if and only if $y - \alpha \in R[y]$, that is, if and only if $\alpha = m \in R = k[x]$. Let us assume that $n \neq 0$. Then the minimal polynomial of α over K is (removing square root from $y = m + n\sqrt{f}$)

$$(y - m)^2 - (n\sqrt{f})^2 = y^2 - 2my + m^2 - n^2 f$$

Again, by Corollary 1.2, α is integral over $R = k[x]$ if and only if $2m \in R$ and $m^2 - n^2 f \in R$. Since the characteristic of k is different from 2, the element 2 is invertible in k. Hence, $2m \in R$ if and only if $m \in R$. It follows that $n^2 f \in R$. Since R is a unique factorization domain and f is square-free we conclude the $n \in R$. Hence if $\alpha \in L$ is integral over R, then $\alpha \in S = \{m + n\sqrt{f} : m, n \in R\}$.

Claim 2. *S is a free R-module of rank 2*

Since R is a euclidean domain, hence a principal ideal domain, and L/K is a degree 2 separable extension, we can use Proposition 1.8 and Lemma 1.3 to conclude that S is a free R-module of rank 2.

Claim 3. *Integral basis of S is* $\{1, \sqrt{f}\}$

Follows trivially from the above two claims.

1.2.2 k is of characteristic 2

Claim 1. *If f' is square free then* $S = R[\sqrt{f}]$

Since R is a unique factorization domain, we can use Corollary 1.2 to prove this claim. Let $\alpha = m + n\sqrt{f} \in L$ with $m, n \in K$. If $n = 0$ then the minimal polynomial of α over K is the linear polynomial $y - \alpha \in K(y)$. Hence by Corollary 1.2, α is integral over R if and only if $\alpha = m \in R = k[x]$. Let us assume that $n \neq 0$ i.e. $\alpha \notin K$. Then the minimal polynomial of α over K is

$$y^2 - 2my + m^2 - n^2 f = y^2 + (m^2 + n^2 f)$$

[2]Recall that a non-constant polynomial in $k[x]$ is square-free of it factors in $\overline{k}[x]$ as a product of distinct irreducible polynomials, where $\overline{k}$ is the algebraic closure of k.

[3]Note that the root need not be unique, we are considering one of the roots of the polynomial.

Again, by Corollary 1.2, α is integral over $R = k[x]$ if and only if $m^2 + n^2 f \in R$. Without loss of generality, we may assume that $m = a/c$ and $n = b/c$, with $a, b, c \in R$ and $\gcd(a, b, c,) = 1$. It follows that α is integral over R if and only if c^2 divides $a^2 + b^2 f$. Let $h \in R$ be such that $c^2 h = a^2 + b^2 f$. By taking the derivative both sides, we find that $c^2 h' = b^2 f'$ when $\alpha \in S$, then c^2 divides $b^2 f'$ in R. Since R is a unique factorization domain and f' is not divisible by a square, we conclude that $c|b$. Therefore, $n = b/c \in R$. Since $m^2 + n^2 f \in R$ we conclude that $m \in R$. Hence if $\alpha \in L$ is integral over R, then $\alpha \in S = \{m + n\sqrt{f} : m, n \in R\}$.

Claim 2. *If k is algebraically closed perfect field*[4] *then S is a free R-module of rank 2*

The extension L is not separable over K since the minimal polynomial $y^2 - f$ of $\sqrt{f}$ has double root in characteristic 2. Hence Proposition 1.8 is not applicable. So we will use the extra assumption of k being perfect to prove our claim in two steps:

Step 1. S is a finitely generated R-module.

Let $f(x) = \sum_{i=0}^{s} a_i x^i$, then since k is of characteristic 2, we have

$$f'(x) = \sum_{\substack{i \text{ even} \\ 0 \le i \le s-1}} a_{i+1} x^i \qquad \text{and} \qquad f''(x) = 0$$

Since k is perfect, k contains the square root of any of its elements, and $f'(x)$ is a perfect square given by

$$f'(x) = \left(\sum_{2j+1 \le s} \sqrt{a_{2j+1}} x^j \right)^2$$

Since k is algebraically closed, we can re-write $f'(x)$ as

$$f'(x) = \left(\prod_{i=1}^{t} (x - b_i)^{r_i} \right)^2$$

Note that, in particular, if $f'(x) = (x - b)^2$ then $f'(x) = x^2 + b^2$. Hence $f(x) = x^3 + b^2 x + a$ for some $a \in k$. Thus $f(b) = a$, leading to the conclusion that

$$\alpha = \frac{f(b) - f(x)}{(x - b)^2} = \frac{x^3 + b^2 x}{x^2 + b^2} = x \in k[x] = R$$

Therefore, $\sqrt{\alpha}$ is integral over R, with $y^2 - \alpha$ being the desired monic polynomial in $R[y]$. Thus, in general the elements

$$\alpha_i = \frac{\sqrt{f(b_i)} - \sqrt{f(x)}}{(x - b_i)^{r_i}}, \quad i = 1, 2, \ldots, t$$

are integral over R. Now following the arguments of the previous claim, one can show that the set $\{1, \alpha_1, \alpha_2, \ldots, \alpha_t\}$ generates the integral closure S over R.

Step 2. S is a free finitely generated R-module.

Note that S is a finitely generated R-module and that R is a principal ideal domain. Since S is an integral domain, the R-module S contains no non-trivial torsion elements. Indeed, let $r \in R, r \neq 0$, and $s \in S$. If $rs = 0$, then $s = 0$ because S is an integral domain. Hence S is torsion free. Therefore, it follows from Proposition 1.7 that S is free finitely generated R-module.

[4] A field k is said to be perfect if either k has characteristic 0, or, when k has characteristic $p > 0$, every element of k is a pth power.

Now by Lemma 1.3 we conclude that S can be generated over R by 2 elements.

Claim 3. *Let $\ell \in R$ denote of polynomial of least degree such that $K(\sqrt{\ell}) = K(\sqrt{f})$, then $\{1, \sqrt{\ell}\}$ is a basis for S over R.*

By construction, $\sqrt{\ell}$ is integral over R and hence, belongs to S. Let $\alpha = \frac{a}{c} + \frac{b\sqrt{\ell}}{c}$ be an integral element, with $a, b, c \in R$ and $\gcd(a, b, c) = 1$. Let's assume that $\deg(c) > 0$ (otherwise nothing to prove). By subtracting, if necessary, an element of $R + R\sqrt{\ell}$, we hay assume that $\deg(c) > \deg(b), \deg(a)$. Since α is integral, there exists a polynomial h such that $c^2h = a^2 + b^2\ell$. This equality shows that $K(\sqrt{h}) = K(\sqrt{\ell})$. Therefore, $\deg(h) \geq \deg(\ell)$, since ℓ is of least degree. Since $\deg(c) > \deg(b)$, we find that $\deg(c^2h) = \deg(a^2)$. This is not possible since $\deg(c) > \deg(a)$. Therefore, $\deg(c) = 0$, and $\{1, \sqrt{\ell}\}$ is a basis of S.

Remark 1.3. Describing ℓ in terms of f can be really difficult. For example, assume that k is an algebraically closed perfect field of characteristic 2, then we have:

1. If $\deg(f) = 1$ or 2, then $f'(x) \in k$ and $S = R[\sqrt{f}]$
2. If $\deg(f) = 3$ or 4, then $f'(x) = (x - b)^2$ and
$$\left\{1, \frac{\sqrt{f(b)} - \sqrt{f(x)}}{(x - b)}\right\}$$
is a basis of S over R.

From the two subsections discussed above, one can conclude that the integral closure S of $k[x]$ in $k(x)(\sqrt{f})$, for a square-free f, is always a finitely generated $k[x]$-module. This is in-fact true in general also, as stated in the following theorem.

Theorem 1.7. *Let k be any field. Let $L/k(x)$ be a finite extension. Let S denote the integral closure of $k[x]$ in L. Then S is a finitely generated $k[x]$-module.*

Proof. See Theorem X.1.7 of [Lor96]. □

Remark 1.4. Since function fields play a central role in algebraic geometry, their ties with geometry are much closer, and often help to provide intuition in the number field case. For instance, instead of the class group, one usually considers the related Picard group of divisors of degree 0 modulo principal divsors [Sha17, Introduction]. The completions of function fields are fields of Laurent series over finite fields. In general, we use the term *global field* refer to number fields and function fields in general, while the term *local field* refers to their nonarchimedean completions [Kor16b].

1.3 Rings of Dimension 1

In this section, field will not to be considered to be a principal ideal domain.

Definition 1.12 (Chain of prime ideals)**.** Let R be any ring. A *chain of prime ideals* of length n in R is a set of $n + 1$ distinct prime ideals[5] $P_0, P_1, \ldots, P_n$ of R such that $P_n \subset P_{n-1} \subset \ldots \subset P_1 \subset P_0$.

Example 1.8. Let k be a field. The ideal $P = (x_1, \ldots, x_i)$ is a prime ideal in the polynomial ring $R = k[x_1, \ldots, x_n]$ because $R/P \cong k[x_{i+1}, \ldots, x_n]$, which is an integral domain. We have following chain of primes of length i

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots, x_i)$$

[5]By definition, a prime ideal is a proper ideal, meaning that it is not the entire ring.

Definition 1.13 (Height of a prime ideal)**.** The *height of a prime ideal* P, $\mathrm{ht}(P)$, is the supremum of the lengths of the chains of primes in R with $P_0 = P$. That is,

$$\mathrm{ht}(P) = \sup\{n : P_n \subset P_{n-1} \subset \ldots \subset P_1 \subset P, P_i \text{ are prime ideals of } R\}$$

Example 1.9. Let k be a field. The ideal $P = (x_1, \ldots, x_i)$ is a prime ideal in the polynomial ring $R = k[x_1, \ldots, x_n]$ and has a chain of primes of length i (as in previous example). Hence $\mathrm{ht}(P) \geq i$.

Definition 1.14 (Krull dimension)**.** The *Krull dimension* of a ring R, $\dim(R)$, is defined to be

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

Example 1.10. If k is a field, then $\dim(k) = 0$ since (0) is the only prime ideal.

Remark 1.5. An integral domain R has dimension 1 if and only if R contains a non-zero primes ideal and every non-zero prime ideal of R is maximal.

Lemma 1.4. *Let R be an integral domain. Let $P_1 = (p_1)$ and $P_2 = (p_2)$ be two distinct non-trivial principal prime ideals of R. Then $P_1 \not\subset P_2$. In particular, a principal prime ideal domain has dimension 1.*

Proof. See Lemma I.5.3 of [Lor96]. □

Lemma 1.5. *Let R be a unique factorization domain, and let $P \neq (0)$ be a prime ideal of R. Then $ht(P) = 1$ if and only if P is principal.*

Proof. See Lemma I.5.4 of [Lor96]. □

Theorem 1.8. *R is a noetherian unique factorization domain of dimension 1 if and only if it is a principal ideal domain.*

Proof. See Proposition I.5.5 of [Lor96]. □

Proposition 1.9. *Let R be an integral domain of dimension 1. Let S be an integral domain containing R and such that each element of S is integral over R. Then S has dimension 1.*

Proof. See Proposition I.5.6 of [Lor96]. □

Remark 1.6. This proposition can be generalized to higher dimensions. For example, if R and S are noetherian and S is integral over R, then $\dim(S) = \dim(R)$. See *Going-up Theorem* in [AM07, Chapter 5].

Corollary 1.6. *Let K be the field of fractions of an integral domain R of dimension 1. Let L/K be a finite extension. Then the integral closure S of R in L has dimension 1.*

Definition 1.15 (Dedekind domain)**.** Ler R be an integral domain. The ring R is called *Dedekind domain* if it has the following three properties:

(i) R is noetherian.

(ii) R has dimension 1.

(iii) R is integrally closed in its field of fractions.

Example 1.11. Analogous to the ring of integers of number fields [Kor16a, Chapter 2], the *rings of integers* of function fields, such as $k[x]$ in the case of $k(x)$, are again Dedekind domains.

Theorem 1.9. *Let R be a Dedekind domain and L/K be a finite separable extension of the field of fractions K of R. Then the integral closure S of R in L is a Dedekind domain.*

Proof. The proof follows by putting together the statements of Theorem 1.6 and Proposition 1.9. □

Chapter 2

Elliptic Curves

2.1 Introduction

Definition 2.1 (Affine plane)**.** *Affine plane* over a field K is the set $\mathbb{A}^2(K) = K^2$.

Definition 2.2 (Affine plane curve)**.** An *affine plane curve*, $Z_f(\overline{K})$, defined over a field K is the set of zeros in $\mathbb{A}^2(\overline{K})$ of a non-zero polynomial $f(x, y) \in K[x, y]$, i.e.

$$Z_f(\overline{K}) = \{(x, y) \in \overline{K}^2 : f(x, y) = 0\}$$

Example 2.1. For $f(x, y) = x^2 + y^2 - 1$ and $K = \mathbb{R}$, then the restriction of $Z_f(\overline{K})$ in K represents a unit circle.

Lemma 2.1. *Let $f \in K[x, y]$ be a polynomial of degree $d > 0$. Then $Z_f(\overline{K})$ is an infinite set. In particular, $Z_f(\overline{K})$ is not empty.*

Proof. See Lemma II.1.3 of [Lor96]. □

Remark 2.1. Algebraically closed fields, like $\overline{K}$, are infinite sets. It follows from their definition that an algebraically closed field must contain root of every polynomial in the corresponding polynomial ring.

Definition 2.3 (Irreducible affine plane curve)**.** An affine plane curve is said to be irreducible if its defining polynomial $f(x, y) \in K[x, y]$ is irreducible in $\overline{K}[x, y]$.

Example 2.2. Let $f(x, y) = x^2+y^2 \in \mathbb{Q}[x, y]$. Then, though f is an irreducible polynomial in its parent ring $\mathbb{Q}[x, y]$, $Z_f(\overline{K})$ is not an irreducible affine plane curve since $f(x, y) = (x+iy)(x-iy)$ in $\mathbb{Q}(i)[x, y] \subset \overline{\mathbb{Q}}[x, y]$.

Definition 2.4 (Taylor series formula)**.** Let $(a_1, a_2, \ldots, a_d) \in \Omega \subseteq \mathbb{R}^d$ and $f : \Omega \to \mathbb{R}$ be a sufficiently smooth function, then we have

$$\begin{aligned} f(x_1, \ldots, x_d) = f(a_1, \ldots, a_d) &+ \sum_{j=1}^{d} \frac{\partial f(a_1, \ldots, a_d)}{\partial x_j}(x_j - a_j) \\ &+ \frac{1}{2!} \sum_{j=1}^{d} \sum_{k=1}^{d} \frac{\partial^2 f(a_1, \ldots, a_d)}{\partial x_j \partial x_k}(x_j - a_j)(x_k - a_k) \\ &+ \frac{1}{3!} \sum_{j=1}^{d} \sum_{k=1}^{d} \sum_{l=1}^{d} \frac{\partial^3 f(a_1, \ldots, a_d)}{\partial x_j \partial x_k \partial x_l}(x_j - a_j)(x_k - a_k)(x_l - a_l) + \cdots \end{aligned}$$

Example 2.3. For a function that depends on two variables, x and y, the Taylor series to second order about the point (a, b) is

$$f(x,y) = f(a,b) + (x-a)f_x(a,b) + (y-b)f_y(a,b) + \\ \frac{1}{2!}\Big((x-a)^2 f_{xx}(a,b) + 2(x-a)(y-b)f_{xy}(a,b) + (y-b)^2 f_{yy}(a,b)\Big)$$

where the subscripts denote the respective *partial derivatives*. See Exercise 9.30 of [Rud76] for more details.

Definition 2.5 (Taylor expansion of an irreducible affine plane curve at origin)**.** The Taylor expansion of an irreducible affine plane curve at a point $P \equiv (0,0) \in Z_f(\overline{K})$ is

$$0 = f(x,y) = f_1(x,y) + f_2(x,y) + \dots$$

where $f_d(x,y)$ is a homogeneous polynomial of degree d, and the expansion is obtained by "formal" Taylor series formula.

Example 2.4. If $f(x,y) = y^2 - x^3 - x^2$ then $f_2(x,y) = y^2 - x^2$ and $f_3(x,y) = -x^3$.

Definition 2.6 (Non-singular affine plane curve at origin)**.** An irreducible affine plane curve is said to be *non-singular* at $P \equiv (0,0)$ if $f_1(x,y) \not\equiv 0$, that is, at least one of the two partial derivatives f_x or f_y are non-zero at P. Also, we say that $f_1(x,y) = 0$ is the *tangent line* at P (i.e. the set of zeros of this degree one homogeneous polynomial).

Example 2.5. $f(x,y) = y^2 - x^3 - x^2$ is singular at origin.

Remark 2.2. If an irreducible affine plane curve is singular at $P = (0,0)$ and d is the least integer such that f_d is non-zero then

$$f_d(x,y) = \prod_{i=1}^{d} (\alpha_i x + \beta_i x)$$

over $\overline{K}$ and $(\alpha_i x + \beta_i y)$ distinct factors are the tangent lines at $P \equiv (0,0)$.

Example 2.6. If $d = 2$ in the previous remark, then:

(1) An irreducible singular affine plane curve is said to have *cusp* at $P \equiv (0,0)$, if the tangent line is of multiplicity 2. For example, if $f(x,y) = y^2 - x^3$.

(2) An irreducible singular affine plane curve is said to have *node* at $P \equiv (0,0)$, if there are two distinct tangent lines at P. For example, if $f(x,y) = y^2 - x^3 - x^2$.

Remark 2.3. If we wish to study the curve at some point other than origin, then we can do the appropriate change of coordinates, as stated in next definition, to bring the point of interest $P' = (a,b)$, say, to $(0,0)$ and then use the above definitions.

Definition 2.7 (Affine changes of coordinates)**.** The non-singular linear transformations followed by translations, that is, maps of the form

$$v \mapsto Mv + w, \qquad M \in \mathrm{GL}_2(K), w \in \mathbb{A}^2(K)$$

are called the *affine changes of coordinates*.

Definition 2.8 (Intersection multiplicity of an affine plane curve)**.** If a line $L = \{(x_0 + at, y_0 + bt) : t \in \overline{K}\}$ $(a, b \in K$ are fixed) in the affine plane intersects an irreducible affine plane curve $Z_f(\overline{K})$ at $P \equiv (x_0, y_0)$ then the *intersection multiplicity*, $I_P(L \cap Z_f(\overline{K}))$, at point P is the order of vanishing of the polynomial $g(t) := f(x_0 + at, y_0 + bt)$.

Example 2.7. If $f(x,y) = y^3 - x^3 - x^2$ and $L = \{(t,0) : t \in \overline{K}\}$ then $g(t) = t^2(t+1)$. Thus the points of intersection are $(0,0)$ and $(-1,0)$, with $I_{(0,0)}(L \cap Z_f(\overline{K})) = 2$ and $I_{(-1,0)}(L \cap Z_f(\overline{K})) = 1$.

Definition 2.9 (Point of inflection of an affine plane curve)**.** If the intersection multiplicity of a tangent line of an irreducible non-singular affine plane curve at a point P is greater than 2, then the point P is said to be a *point of inflection.*

Example 2.8. If $f(x,y) = y - x^3$ and $L = \{(t,0) : t \in \overline{K}\}$ then $P \equiv (0,0)$ is the only point of intersection and $I_P(L \cap Z_f(\overline{K})) = 3$. Note that the curve should be non-singular, hence we can't use the curve used in the previous example though its tangent at origin also has intersection multiplicity 3.

Definition 2.10 (Component of an affine plane curve)**.** If $L \subset Z_f(\overline{K})$, i.e. the result of using the equation of the line to eliminate a variable in $f(x,y)$ is that the equation of the curve becomes zero, then the line L is said to be a component of the reducible affine plane curve $Z_f(\overline{K})$.

Example 2.9. $L = \{(x,y) \in \overline{K}^2 : x = 0\}$ is a component of $Z_f(\overline{K}) = \{(x,y) \in \overline{K}^2 : x^2 + xy = 0\}$.

Definition 2.11 (Projective n-space)**.** Projective n-space, $\mathbb{P}^n(K)$, is defined to be the set of equivalence classes $[x_1 : x_2 : \ldots : x_{n+1}]$ of non-zero $(n+1)$-tuples $x = (x_1, \ldots, x_{n+1}) \in K^{n+1}$ under the scalar multiplication relation

$$x \sim \lambda x, \qquad \lambda \in K, \lambda \neq 0$$

That is,

$$\mathbb{P}^n(K) = \{[x_1 : x_2 : \ldots : x_{n+1}] \,|(x_1, \ldots, x_{n+1}) \sim (\lambda x_1, \ldots, \lambda x_{n+1}),\ \lambda \in K, \lambda \neq 0, x_i \in K\}$$

Remark 2.4. We can think $\mathbb{A}^n(K)$ to be embedded in $\mathbb{P}^n(K)$, since the map $\phi : \mathbb{A}^n(K) \longrightarrow \mathbb{P}^n(K)$ such that

$$(x_1, \ldots, x_n) \longmapsto [x_1 : x_2 : \ldots : x_n : 1]$$

is an injective map. Moreover, the complement of the image of ϕ, consisting of all equivalence classes of the points with $x_{n+1} = 0$ is isomorphic to $\mathbb{P}^{n-1}$ and is sometimes called the *hyperplane at infinity.*

Example 2.10. $\mathbb{P}^2(K) \cong \mathbb{A}^2(K) \cup \mathbb{P}^1(K)$.

Definition 2.12 (Projective algebraic variety)**.** Projective algebraic variety, $Z(S)$, is the set of zeros in $\mathbb{P}^n(\overline{K})$ of some finite family, S, of homogeneous polynomials in $n+1$ variables with coefficients in $\overline{K}$, i.e

$$Z(S) = \{x \in \mathbb{P}^n(\overline{K}) : f(x) = 0 \,\text{such that}\, f \in S\}$$

where S is a finite set of homogeneous polynomials in $n+1$ variables.

Example 2.11. Let $K = \mathbb{R}$ and $S = \{xy, yz, zx\}$ then $Z(S)$ is the union of the three coordinate axis in $\mathbb{R}^3$.

Definition 2.13 (Defining ideal of a projective variety)**.** Given a projective variety $Z(S)$, the ideal $I \subset \overline{K}[x_1, \ldots, x_{n+1}]$ generated by the finite collection S of homogeneous polynomials is called the defining ideal of the variety.

Remark 2.5. We can now represent a projective algebraic variety as

$$Z(S) = \{[x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n(\overline{K}) \,|f(x_1, \ldots, x_{n+1}) = 0 \forall f \in I = \langle S \rangle \subset \overline{K}[x_1, \ldots, x_{n+1}]\}$$

Example 2.12. $I = \langle x^2 + y^2 + z^2, xy + yz + zx, z^5 \rangle \subset \mathbb{C}[x, y, z]$

Definition 2.14 (Irreducible projective variety)**.** If the defining ideal $I = \langle S \rangle$ of a projective variety $Z(S)$ is a prime ideal then the projective variety is called irreducible.

Example 2.13. For $S = \{x^2 + xy + y^2 - z^2\}$ we get $I \subset \mathbb{C}[x, y, z]$ as a prime ideal since the homogeneous polynomial $f(x, y, z) = x^2 + xy + y^2 - z^2$ can't be factored as a product to linear homogeneous polynomials. Hence the projective variety $Z(S) \subset \mathbb{P}^2(\mathbb{C})$ is irreducible.

Definition 2.15 (Dimension of projective variety)**.** The dimension of projective algebraic variety $Z(S) \subset \mathbb{P}^n(\overline{K})$ is defined to be one less than the Krull dimension of the quotient ring $\overline{K}[x_1, \ldots, x_{n+1}]/\langle S \rangle$.

Example 2.14. Since by Noether normalization lemma, $\dim(K[x_1, \ldots, x_{n+1}]) = n + 1$, the space $\mathbb{P}^n(K)$ is n-dimensional.

Definition 2.16 (Projective curve)**.** A projective curve, C, is an irreducible 1-dimensional projective variety.

Example 2.15. Let $K = \mathbb{C}$ and $S = \{x_1x_3 - x_2^2, x_2x_4 - x_3^2, x_1x_4 - x_2x_3\}$, then $I = \langle S \rangle \subset \mathbb{C}[x_1, x_2, x_3, x_4]$ is prime ideal since there exist following surjective homomorphism

$$\begin{aligned} \phi : \mathbb{C}[x_1, x_2, x_3, x_4] &\longrightarrow \mathbb{C}[s, t] \\ x_1 &\longmapsto \quad s^3 \\ x_2 &\longmapsto \quad s^2t \\ x_3 &\longmapsto \quad st^2 \\ x_4 &\longmapsto \quad t^3 \end{aligned}$$

with $\ker(\phi) = I$, hence by first isomorphism theorem of rings, we have $\mathbb{C}[x_1, x_2, x_3, x_4]/I \cong \mathbb{C}[s, t]$. Since $\mathbb{C}[s, t]$ is an integral domain I is prime ideal. Also, since by Noether normalization lemma, $\dim(\mathbb{C}[s, t]) = 2$ we conclude that the dimension of the projective variety $Z(S)$ is 1. This curve $C = Z(S)$, is known as *twisted cubic*.

Definition 2.17 (Non-singular projective curve at origin)**.** An irreducible projective curve in $\mathbb{P}^n(\overline{K})$ is said to be *non-singular* at $P \equiv [0 : \ldots : 0 : 1]$ if $f_1(x_1, \ldots, x_{n+1}) \not\equiv 0$, that is, at least one of the $(n + 1)$ partial derivatives $f_{x_1}, \ldots, f_{x_{n+1}}$ are non-zero at P. Also, we say that $f_1(x_1, \ldots, x_{n+1}) = 0$ is the *tangent line* at P (i.e. the set of zeros of this degree one homogeneous polynomial).

Definition 2.18 (Projective change of coordinates)**.** The non-singular linear transformations, that is, maps of the form

$$x \mapsto Mx \qquad M \in \mathrm{GL}_{n+1}(K), x \in \mathbb{P}^n(K)$$

are called the *projective changes of coordinates*.

Remark 2.6. Using above definition we can check whether a projective curve is non-singular at a given point. Hence a projective curve is said to be smooth/irreducible if it's irreducible at all the points.

Definition 2.19 (Homogenization)**.** Given a polynomial $f(x_1, \ldots, x_n)$ of degree d, by homogenization be obtain a homogeneous polynomial $f^*(x_1, \ldots, x_{n+1})$ of degree d, such that

$$f^*(x_1, \ldots, x_{n+1}) = x_{n+1}^d f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right)$$

Example 2.16. Thus any affine curve $Z_f(\overline{K})$ determines a projective curve C with the projective dual being defined by $S = \{f^*(x, y, z)\}$. This projective curve C consists of the points in $\mathbb{A}^2(K)$ with $f(x, y) = f^*(x, y, 1) = 0$ as well as the points at infinity, i.e., on the line $z = 0$, which are found by solving $f^*(x, y, 0) = 0$. See §1.8 of [Kor15] for more examples.

Remark 2.7. The intersection between a line $L = \{[x : y : z] \in \mathbb{P}^2(\overline{K}) : ax + by + cz = 0\}$ for some $a, b, c \in \overline{K}$ and a curve $C = \{[x : y : z] \in \mathbb{P}^2(\overline{K} : f(x, y, z) = 0\}$ for some homogeneous polynomial f, can be found by eliminating one of the variables, that occurs with a non-zero coefficient in the equation of line and factoring the resulting form in two variables.

Lemma 2.2 (Weierstrass form)**.** *An affine plane curve $Z_f(\overline{K})$ is of the Weierstrass form, i.e., $f(x, y) = 0$ is*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in K$$

if and only if the point $O \equiv [0 : 1 : 0]$ is a smooth point, inflection point and has the line $z = 0$ at infinity as the tangent line to the corresponding projective curve C defined by $f^*(x, y, z) = 0$.

Proof. See Example 1.15 of [Buh01]. □

2.2 Weierstrass Form of Elliptic Curves

Definition 2.20 (Rational map)**.** If $V \subset \mathbb{P}^n(K)$ is an irreducible projective variety defined over K then a rational mapping, g, from V to $\mathbb{P}^m(K)$ is an equivalence class of $m + 1$ homogeneous polynomials g_i, $0 \leq i \leq m$, with coefficients in $\overline{K}$, in $n + 1$ variables of same degree, such that at least one of them does not vanish identically on V, that is,

$$\begin{aligned} g : V &\to \mathbb{P}^m(K) \\ x &\mapsto g_0(x) : g_1(x) : \ldots : g_m(x) \end{aligned}$$

where $x = [x_1 : \ldots : x_{n+1}]$ and $g_i(x) = g_i(x_1, \ldots, x_{n+1})$ such that at least one of $g_i(x) \not\equiv 0$.

Remark 2.8. Two rational maps g and G, from V to $\mathbb{P}^m(K)$ are said to be equivalent if

$$g_i(x)G_j(x) = g_j(x)G_i(x)$$

for all i, j and $x \in V$.

Example 2.17. The rational map $g([x_1 : x_2 : x_3]) = [x_1x_2 : x_1x_3 : x_2x_3]$ from $\mathbb{P}^2(K)$ to $\mathbb{P}^2(K)$ is defined everywhere except at the three points $[1 : 0 : 0]$, $[0 : 1 : 0]$ and $[0 : 0 : 1]$.

Definition 2.21 (Birational map)**.** A rational mapping is birational if there is a rational mapping that is inverse to it, where both are defined, i.e. there exist a rational map G such that $G(g(x)) = x$ if x is in the domain of g and $g(x)$ is in domain of G.

Example 2.18. Let V be the quadratic surface in $\mathbb{P}^3(K)$ defined by $x_1x_4 - x_2x_3 = 0$. Then the map $g([x_1 : x_2 : x_3 : x_4]) = [x_1 : x_2 : x_3]$ from V to $\mathbb{P}^2(K)$ is birational since we have an inverse rational map $G([x_1 : x_2 : x_3]) = [x_1^2 : x_1x_2 : x_1x_3 : x_2x_3]$ from $\mathbb{P}^2(K)$ to V. See [Wil06] for more details.

Definition 2.22 (Rational function)**.** A rational function on a projective variety V defined over K is a rational map from V to $\mathbb{P}^1(K)$.

Remark 2.9. Usually, a rational function $g = g_0 : g_1$ is written as $g(x) = g_0(x)/g_1(x)$ and g has a *zero* at x if $g_0(x) = 0, g_1(x) \neq 0$ and has a *pole* if $g_0(x) = 1, g_1(x) = 0$.

Definition 2.23 (Function field of a projective variety)**.** The set of all rational functions on irreducible projective variety V, along with the zero map form a field and is called the function field of V, denoted by $K(V)$.

Definition 2.24 (Order of vanishing)**.** Given a rational function g on a projective curve V and a smooth/non-singular point P on V, then g can be written as

$$g = u_P^n G$$

where u_P is a rational function (called uniformizer at P) such that $u_P(P) = [0 : 1]$, and G is a rational function whose value at P is neither zero nor infinity (i.e., neither $[0 : 1]$ nor $[1 : 0]$). The integer n is the order of vanishing of g at P, $\mathrm{ord}_P(g) \in \mathbb{Z} \cup \{\infty\}$, where we set $\mathrm{ord}_P(0) = \infty$.

Remark 2.10. If $\mathrm{ord}_P(g) < 0$ then g has a *pole* of order $-\mathrm{ord}_P(g)$ at P and if $\mathrm{ord}_P(g) > 0$ then g has a *zero* of order $\mathrm{ord}_P(g)$ at P.

Definition 2.25 (Genus of a projective curve)**.** If C is a plane projective curve of degree d and there are n nodes and no other singular points, then the genus of C is

$$\gamma = \frac{(d-1)(d-2)}{2} - n$$

Remark 2.11. The above algebraic definition is based on the fact that the genus of a curve can be defined by projecting it into the plane, and analysing the singularities in the plane carefully. It can be shown that it is possible to find a birational map from a curve to a plane curve whose only singularities (if any) are nodes, i.e., singular points with two distinct tangent lines, see [Abh90, Lecture 5]. For the geometric definition of the genus, defined via Euler characteristic see [USM03, Lecture 1].

Example 2.19. Consider the projective curve $y^2z = x^3 + x^2z$. To determine the number of nodes, we will examine $y^2 = x^3 + x^2$, $z = x^3 + z$ and $y^2z = 1 + z$ separately in their respective copies of $\mathbb{A}^2(\mathbb{C})$. We have already seen that the affine curve $y^2 = x^3 + x^2$ has 1 node. Clearly $x = 0$ has no nodes. We can transform $y^2z = 1 + z$ to $y^2z - y^2 = z$ so that it passes though origin, and also doesn't have any singular point. Therefore the genus $\gamma = \frac{(3-1)(3-2)}{2} - 1 = 0$.

Definition 2.26 (Divisor)**.** A *divisor* D is a finite formal integral linear combination of points on a non-singular projective curve C over an algebraically closed field K, that is

$$D = \sum_{P \in C} a_P P, \qquad a_P \in \mathbb{Z}$$

Definition 2.27 (Space of good functions)**.** Let K be an algebraically closed field and C be a non-singular projective curve over K. Then the space of good functions $L(D)$ is the vector space of rational functions g such that $\mathrm{ord}_P(g) \geq -a_P$ where $D = \sum_{P \in C} a_P P$, that is

$$L(D) = \{g \in K(C) : \mathrm{ord}_P(g) \geq -a_P\}$$

We take $g \equiv 0$ to be in $L(D)$ by convention.

Example 2.20. If $D = 0$ then $L(D)$ consists of rational functions that have no poles, and only such functions are constant functions, i.e. $L(0) = \{1\}$.

Definition 2.28 (Degree of a divisor)**.** The *degree of a divisor* D, $\deg(D)$, is the sum of all the a_P's, where $D = \sum_{P \in C} a_P P$ for some non-singular projective curve C over an algebraically closed field K. That is

$$\deg(D) = \sum_{P \in C} a_P$$

Theorem 2.1 (Riemann-Roch Theorem)**.** *Let K be an algebraically closed field and C be a non-singular projective curve on K. Then there is an integer γ, called the genus of the curve C, such that if $\deg(D) > 2\gamma - 2$ then*

$$\dim(L(D)) = \deg(D) + 1 - \gamma$$

where $\dim(L(D))$ is the vector-space dimension of $L(D)$ over K.

Example 2.21. Let $P = [0 : 1] \in \mathbb{P}^1(K)$, and consider $D = nP$, so that $L(nP)$ consists of rational functions g on the projective line whose only pole is at $P = [0 : 1]$ and the order of the pole at most n. Any rational function in $L(nP)$ can be written as

$$g([x : y]) = \frac{G([x : y])}{x^n}$$

where G is an arbitrary homogeneous polynomial of degree n. Since homogeneous polynomials in two variables of degree n have $n+1$ coefficients, so the dimension of the vector space of such homogeneous polynomials is $n+1$, and hence $\dim(L(nP)) = n+1$. Also, since $\deg(D) = n$, by Riemann-Roch Theorem we get $\gamma = 0$ i.e. the projective line has genus zero.

Definition 2.29 (Elliptic curve)**.** An elliptic curve over a field K is a smooth projective curve E over K of genus 1, together with a specified K-rational point[1] O.

Remark 2.12. Two elliptic curves are isomorphic if there is a non-constant birational map from one curve to the other that maps the specified point on one curve to the specified point on the other curve.

Theorem 2.2. *Every elliptic curve over a field K is isomorphic to the projective curve corresponding to a non-singular affine cubic $Z_f(\overline{K})$ in Weierstrass form, i.e. $f(x, y) = 0$ being*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in K$$

Proof. See §1.6 of [Buh01]. □

Example 2.22. The Fermat cubic $x^3 + y^3 = z^3$ is a smooth projective curve of degree 3, and by Definition 2.25 we find it's genus to be 1. Hence it's an elliptic curve. If we substitute $x = Y + 36$, $y = -Y + 36$ and $z = 6X$, we arrive at the equation $Y^2 = X^3 - 432$, which is in Weierstrass form. See more examples given in [Buh01].

Remark 2.13. If the characteristic of K in not 2 or 3, then by completing the squares and cubes, we end up with an equation of the form $Y^2 = X^3 + aX + b$ equivalent to the general Weierstrass form.

[1] That is $O \in \mathbb{P}^n(K)$ for $O \in E \subset \mathbb{P}^n(\overline{K})$.

Conclusion

In first chapter we saw that as compared to finding the integral basis of ring of integers of a quadratic extension of $\mathbb{Q}$ (as seen in Chapter 2 of [Kor16a]) it's more difficult to find an integral basis of ring of integers of a quadratic extension of $k(x)$, if k is a field of characteristic 2.

In second chapter we came across various fundamental notions in algebraic geometry, leading to a more geometric definition of elliptic curves (as compared to the one discussed in §1.8 of [Kor15]).

Also, I used two important theorems, namely Noether normalization lemma (that lead to the conclusion that $\dim(K[x_1, \ldots, x_n]) = n$) and Riemann–Roch theorem (while defining genus of algebraic curve) without knowledge of their proofs. I will fill this gap in my knowledge by the end of next semester.

Bibliography

[Abh90] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35 of *Mathematical surveys and monographs*. American Mathematical Society, Providence, Rhode Island, 1990.

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

[Buh01] Joe P. Buhler. Elliptic curves, modular forms, and applications. In Brian Conrad and Karl Rubin, editors, *Arithmetic Algebraic Geometry*, volume 9 of *IAS/Park City Mathematics Series*, pages 9–81. American Mathematical Society, Providence, Rhode Island, 2001.

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

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

[Kor16a] Gaurish Korpal. Number fields. Summer internship project report, Indian Statistical Institute, Bangalore, June 2016. https://gaurish4math.files.wordpress.com/2015/12/number-fields_gaurish_rev5.pdf.

[Kor16b] Gaurish Korpal. Reciprocity laws. Winter internship project report, Harish-Chandra Research Institute, Allahabad, December 2016. https://gaurish4math.files.wordpress.com/2015/12/reciprocity_laws-gaurish.pdf.

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

[Rud76] Walter Rudin. *Principles of Mathematical Analysis*. International series in pure and applied mathematics. McGraw Hill Education, Singapore, 3 rd edition, 1976.

[Sha17] Romyar Sharifi. Algebraic number theory. Lecture Notes, 2017. http://math.ucla.edu/~sharifi/algnum.pdf.

[USM03] Kenji Ueno, Koji Shiga, and Shigeyuki Morita. *A Mathematical Gift, I*, volume 19 of *Mathematical World*. American Mathematical Society, Providence, Rhode Island, 2003.

[Wil06] Andrew Wilson. Birational maps and blowing things up. Lecture Notes, 2006. http://ajwilson.co.uk/files/maths/Birmapsandblowingthingsup.pdf.