Undergraduate Algebraic Geometry

Ali Sinan Sertöz

Contents

CHAPTER 1

Affine Varieties

1. First Definitions

Affine Space: We fix an algebraically closed field k. The affine n space over k, denoted by $\mathbb{A}^n_k$, is the set of n-tuples of elements of k, where n is any positive integer. We generally denote $\mathbb{A}^n_k$ by $\mathbb{A}^n$ when there is no confusion about which k is used. $\mathbb{A}^n$ is simply k^n without the k-vector space structure.

We will consider $\mathbb{A}^n$ only with polynomial functions of the form

$$f : \mathbb{A}^n \longrightarrow \mathbb{A}^1$$

where $f \in k[x_1, \dots, x_n]$.

Zero Set: For any ideal J of the polynomial ring $k[x_1, \dots, x_n]$ we define

$$Z(J) = \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in J \}.$$

Every ideal in $k[x_1, \dots, x_n]$ is finitely generated. If $J = (f_1, \dots, f_r)$, then we denote $Z(J)$ also by $Z(f_1, \dots, f_r)$. Clearly, for any two ideals $J_1 \subseteq J_2$, we have $Z(J_1) \supseteq Z(J_2)$.

Definition 1. *A subset X of $\mathbb{A}^n$ is called an algebraic set if it is of the form $X = Z(J)$ for some ideal $J \subset k[x_1, \dots, x_n]$.*

Some immediate examples of algebraic sets are $Z(1) = \emptyset$, $Z(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ and $Z(0) = \mathbb{A}^n$. If $k = \mathbb{C}$, then a nonempty proper subset of $\mathbb{A}^n$ which is open with respect to the usual metric topology is not an algebraic set.

By the Fundamental Theorem of Algebra a nonconstant polynomial $f \in k[x_1]$ always has a root in k. Since $k[x_1]$ is a principal ideal domain, every proper ideal J in $k[x_1]$ is generated by a single nonconstant polynomial and consequently $Z(J) \neq \emptyset$.

However a proper ideal J in $k[x_1, \ldots, x_n]$ is not necessarily generated by a single element and attempts to check if $Z(J)$ is empty or not using the Fundamental Theorem of Algebra above raises complicated technical difficulties. We have nonetheless the highly nontrivial result:

THEOREM 2 (Hilbert's Nullstellensatz). *If k is algebraically closed then $Z(J) \neq \emptyset$ for every proper ideal J in $k[x_1, \ldots, x_n]$.*

PROOF. Let $\mathfrak{m}$ be a maximal ideal containing J. Since $Z(\mathfrak{m}) \subseteq Z(J)$, it suffices to show that $Z(\mathfrak{m})$ is not empty. Let

$$k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]/\mathfrak{m} = k[\bar{x}_1, \ldots, \bar{x}_n] = K$$

be the usual surjection, where $\bar{x}_i$ is x_i mod $\mathfrak{m}$. Here K is a field and $(\bar{x}_1, \ldots, \bar{x}_n)$ is a point of $Z(\mathfrak{m})$ in $\mathbb{A}^n_K$. We want to show that this point actually lies in $\mathbb{A}^n_k$. We will achieve this by showing that K is in fact k. If K is algebraic over k, then since k is algebraically closed it will follow that $K = k$.

We then proceed to show that each $\bar{x}_1, \ldots, \bar{x}_n$ is algebraic over k. Here we follow [**14**, p165].

If $n = 1$, then $k[\bar{x}_1]$ being a field, $\bar{x}_1$ has an inverse, say $f(\bar{x}_1)$. Then $\bar{x}_1 f(\bar{x}_1) - 1 = 0$ is an algebraic equation for $\bar{x}_1$ over k.

We now show how to pass from $n = 1$ case to $n = 2$ case. The field $k[\bar{x}_1, \bar{x}_2]$ contains the field $k(\bar{x}_1)[\bar{x}_2]$. By what we showed above, $\bar{x}_2$ is algebraic over $k(\bar{x}_1)$. If we can now show that $\bar{x}_1$ is algebraic over k, we will be done. Assume that $\bar{x}_1$ is transcendental over k. Recall then that $k[\bar{x}_1]$ is integrally closed in $k(\bar{x}_1)$.

Take an algebraic equation of $\bar{x}_2$ over $k(\bar{x}_1)$, clear denominators and obtain

$$h(\bar{x}_1)\bar{x}_2^m + h_{m-1}(\bar{x}_1)\bar{x}_2^{m-1} + \cdots + h_0(\bar{x}_1) = 0$$

for some $m > 0$ and $h(\bar{x}_1), h_{m-1}(\bar{x}_1), \ldots, h_0(\bar{x}_1) \in k[\bar{x}_1]$. Then $(h^m(\bar{x}_1)\bar{x}_2)$ is integral over $k[\bar{x}_1]$. It follows that for every $f(\bar{x}_1, \bar{x}_2) \in k[\bar{x}_1, \bar{x}_2]$ there exists an integer r such that $h^r(\bar{x}_1)f(\bar{x}_1, \bar{x}_2)$ is integral over $k[\bar{x}_1]$. Since the field $k(\bar{x}_1)$ is in $k[\bar{x}_1, \bar{x}_2]$, this also applies to fractions of the form $f(\bar{x}_1)/g(\bar{x}_1)$ where f and g are polynomials and are relatively prime. In particular choose g to be nonconstant and also relatively prime to h. From $h^r(\bar{x}_1)f(\bar{x}_1)/g(\bar{x}_1)$ being integral over $k[\bar{x}_1]$ for some integer $r \geq 0$ and $k[\bar{x}_1]$ being integrally closed in $k(\bar{x}_1)$, it follows that

$h^r(\bar{x}_1)f(\bar{x}_1)/g(\bar{x}_1)$ is in $k[\bar{x}_1]$ and hence $g(\bar{x}_1)$ divides $h^r(\bar{x}_1)$ which is a contradiction. So $\bar{x}_1$ is algebraic over k and consequently so is $\bar{x}_2$.

For the general case apply the induction hypothesis to $k(\bar{x}_1)[\bar{x}_2, \ldots, \bar{x}_n]$. Each $\bar{x}_2, \ldots, \bar{x}_n$ is algebraic over $k(\bar{x}_1)$. We can find a polynomial $h(\bar{x}_1) \in k[\bar{x}_1]$ and an integer m such that each $(h^m(\bar{x}_1)\bar{x}_i)$ is integral over $k[\bar{x}_1]$, $i = 2, \ldots, \bar{x}_n$. This leads to a contradiction since $k[\bar{x}_1]$ is integrally closed in $k(\bar{x}_1)$. □

Observe how k being algebraically closed is used in the proof. In fact $Z(x_1^2 + x_2^2 + 1) = \emptyset$ in $\mathbb{A}^2_{\mathbb{R}}$.

Zariski Topology: We put a new topology on $\mathbb{A}^n$ by declaring that the collection of closed sets will consist only of algebraic sets. The topology thus defined is called the *Zariski topology.*

A closed set in a topological space is called *irreducible* if it is not the union of two proper nonempty closed subsets. The empty set is then not irreducible.

The only proper irreducible subsets of $\mathbb{A}^1$ are singletons. Since k is algebraically closed, $\mathbb{A}^1$ is infinite. This shows that $\mathbb{A}^1$ is irreducible.

Affine Variety: An affine algebraic set is called an *affine variety* if it is irreducible in the Zariski topology.

We know so far that $\mathbb{A}^1$ and singletons in $\mathbb{A}^1$ are algebraic varieties. We cannot yet show that $\mathbb{A}^n$ is irreducible for any $n \geq 1$. Try it!

Dimension: The *dimension* of a set V in a topological space is defined to be the supremum of the integers m for which there is a chain of inclusions

$$V \supseteq V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_m$$

where each V_i is a closed irreducible subset.

Dimension of V is denoted by $\dim V$ or by $\dim_k V$ when the reference to k is relevant.

For any nonconstant $f \in k[x_1, \ldots, x_n]$, the algebraic set $Z(f)$ is called a *hypersurface*, and if f is linear it is called a *hyperplane.*

We would like to show that the dimension of $\mathbb{A}^n$ is n and to know if it is irreducible. Moreover we expect in general that the dimension of a hypersurface $Z(f)$ in $\mathbb{A}^n$ is $n-1$ and that it is irreducible if f is an irreducible polynomial.

To answer such questions we must have a tool of recovering information about the ideal from its zero set.

Ideal of a Set: When X is a subset of $\mathbb{A}^n$ define

$$I(X) = \{ f \in k[x_1, \ldots, x_n] \mid f(p) = 0 \text{ for all } p \in X \}.$$

This is a radical ideal in $k[x_1, \ldots, x_n]$. Clearly, for any subsets $X \subseteq Y$, we have $I(X) \supseteq I(Y)$.

We have the immediate relations:
(i) $X \subset Z(I(X))$ for any $X \subset \mathbb{A}^n$ and
(ii) $J \subset I(Z(J))$ for any ideal $J \subset k[x_1, \ldots, x_n]$.

To understand when equality holds in these inclusions we need the following corollary to Theorem 2.

Corollary 3. *If J is any ideal in $k[x_1, \ldots, x_n]$, then $I(Z(J)) = \sqrt{J}$, where $\sqrt{J}$ is the radical of J.*

Proof. First take any $f \in \sqrt{J}$. Then $f^r \in J$ for some integer $r > 0$ and f vanishes at every point of $Z(J)$. Hence $f \in I(Z(J))$.

For the converse inclusion let f be in $I(Z(J))$. Choose a set of generators for J, say $J = (f_1, \ldots, f_m)$. Then f vanishes at every point where $f_1, \ldots, f_m$ simultaneously vanish. Consider the ideal

$$J_0 = (f_1, \ldots, f_m, 1 - tf) \subset k[x_1, \ldots, x_n, t].$$

Clearly $Z(J_0) = \emptyset$ in $\mathbb{A}^{n+1}$ and by Theorem 2, J_0 cannot be proper. So $1 \in J_0$ and there are polynomials $g, g_1, \ldots, g_m \in k[x_1, \ldots, x_n, t]$ such that

$$1 = g_1 f_1 + \cdots + g_m f_m + g \cdot (1 - tf).$$

In this identity substitute $t = 1/f$ and clear denominators to obtain

$$f^r = h_1 f_1 + \cdots + h_m f_m$$

where

$$h_i = g_i(x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}) \cdot f^r(x_1, \ldots, x_n)$$

and r is chosen to be the largest of the degrees of the g_i's in t. This then gives $f \in \sqrt{J}$ and establishes the equality. □

We now have an inclusion reversing correspondences between radical ideals in $k[x_1, \ldots, x_n]$ and algebraic sets in $\mathbb{A}^n$.

$$\left\{ \begin{array}{c} \text{Radical ideals} \\ \text{in } k[x_1, \ldots, x_n] \end{array} \right\} \begin{array}{c} \xrightarrow{Z} \\ \xleftarrow[I]{} \end{array} \left\{ \begin{array}{c} \text{Algebraic sets} \\ \text{in } \mathbb{A}^n_k \end{array} \right\}$$

Moreover these correspondences are inverses of each other. $I \circ Z$ is identity on radical ideals and $Z \circ I$ is identity on algebraic sets.

Commutative Algebra: Let R be a finitely generated k-algebra which is an integral domain. For example R can be $k[x_1, \ldots, x_n]/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$. The dimension of R, denoted by $\dim R$, is defined to be the supremum of all integers m for which there is a chain of prime ideals of length m of the form

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m.$$

Every maximal chain of primes have the same length. If we denote the transcendence degree of R over k by $\text{tr.deg}_k R$, then $\dim R = \text{tr.deg}_k R$. In particular $\dim k[x_1, \ldots, x_n] = n$. Moreover for any prime ideal $\mathfrak{p}$ in R, there is a maximal chain of primes as above where $\mathfrak{p} = \mathfrak{p}_i$ for some i. For the proofs we refer to [**4**, Chapter 13].

Exercises

1. An algebraic set $Z(J)$ is irreducible if and only if J is a prime ideal. It follows that $\mathbb{A}^n$ is irreducible, and the hypersurface $Z(f)$ is irreducible if and only if f is an irreducible polynomial.

2. If $X \subsetneq Y$ are algebraic sets, then $\dim X < \dim Y$.

3. The dimension of an algebraic variety $Z(J)$ is the Krull dimension of the ring $k[x_1, \ldots, x_n]/J$. In particular $\dim \mathbb{A}^n = n$.

4. Dimension of a hypersurface in $\mathbb{A}^n$ is $n - 1$.

5. For any ideal J in $k[x_1, \ldots, x_n]$, $Z(J)$ is singleton if and only if J is a maximal ideal.

6. Closure with respect to Zariski topology of a set X in $\mathbb{A}^n$ is $Z(I(X))$.

7. An arbitrary union of algebraic sets need not be algebraic.

8. With respect to the induced Zariski topology on an algebraic variety, any nonempty open subset is dense.

9. For any $f \in k[x_1, \dots, x_n]$ let D_f denote the complement of $Z(f)$ in $\mathbb{A}^n$. It is called a *fundamental open set.* Every open subset of $\mathbb{A}^n$ can be written as a finite union of fundamental open sets.

10. Every fundamental set is isomorphic to an affine variety. However the union of two fundamental sets need not be isomorphic to an algebraic set. Does this contradict with the fact that the union of two algebraic sets is again an algebraic set?

2. Affine Morphisms

In this section $X \in \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are affine varieties and J denotes the prime ideal $I(X)$.

Polynomial Functions: A function $f : X \to k$ is called a *polynomial function* if there is a polynomial $F \in k[x_1, \dots, x_n]$ such that $f(p) = F(p)$ for all $p \in X$. Two polynomials F_1 and F_2 define the same polynomial function on X if and only if $F_1 - F_2 \in J$. The set of polynomial functions on X form a ring which we call the *coordinate ring* of X. This ring is denoted by $k[X]$. Clearly $k[X] \cong k[x_1, \dots, x_n]/J$.

Rational Functions: An expression of the form F/G where $F, G \in k[x_1, \dots, x_n]$ is traditionally called a rational function on $\mathbb{A}^n$. It is not a function in general since it is not defined at the points where G vanishes. However, elsewhere it defines a legitimate function. If we define D_G as $\mathbb{A}^n \backslash Z(G)$, then F/G is a function on D_G. We denote this by

$$\frac{F}{G} : \mathbb{A}^n \dashrightarrow k$$

where broken arrow notation warns that the domain of the function may not be all of what is written there but is an open dense subset of it. Here with this understanding we call F/G a *rational function on* $\mathbb{A}^n$.

A *rational function on* X is a function on an open dense subset of X where it is evaluated as the restriction of a rational function of $\mathbb{A}^n$. A rational function ϕ on X is denoted by

$$\phi : X \dashrightarrow k$$

where the broken arrow reminds that the domain is some open dense subset. If $\phi = F/G$ for some polynomials $F, G \in k[x_1, \dots, x_n]$ on some open dense subset of X, then we agree to use F/G to denote the rational function ϕ.

If F/G and F'/G' are rational functions on $\mathbb{A}^n$ with $G, G' \notin J$, then they define the same rational function on X if and only if $FG' - GF' \in J$.

Two rational functions are added and multiplied on their common domain. If ϕ is a rational function which is not identically zero, then $1/\phi$ is also a rational function on X. The set of all rational functions on X forms a field, called the *field of rational functions* or the *function field* of X, and is denoted by $k(X)$.

Regular Functions: A rational function F/G on X is called *regular* at $p \in X$ if $G(p) \neq 0$. The set of all regular functions at p is a ring denoted by $\mathcal{O}_{p,X}$, or by $\mathcal{O}_p$ if the reference to X is clear, and is called the ring of regular functions at p.

For any subset U of X, we say that a rational function is regular on U if it is regular at every point of U. The set of all such functions forms a ring which is denoted by $\mathcal{O}(U)$.

It follows from these definitions that

$$\mathcal{O}(U) = \bigcap_{p \in U} \mathcal{O}_p, \quad \mathcal{O}(\{p\}) = \mathcal{O}_p \text{ and } k[X] \subset \mathcal{O}_p \text{ for all } p \in X.$$

A function is regular on X if it is regular at all points of X. The nature of such functions is given by the following theorem.

THEOREM 4.

$$\mathcal{O}(X) = k[X].$$

PROOF. The inclusion $k[X] \subset \mathcal{O}(X)$ is clear. Conversely take $\phi \in \mathcal{O}(X)$.

For any polynomial $H \in k[x_1, \ldots, x_n]$, let h denote the corresponding polynomial function in $k[X]$.

Let J_0 consist of all polynomials H such that $h\phi$ is a polynomial function on X.

Clearly J_0 is an ideal in $k[x_1, \ldots, x_n]$. Moreover if $H \in J$, then $h\phi$ is identically zero on X, so $H \in J_0$. Thus $J \subset J_0$ and $Z(J_0) \subset X$.

For every point $p \in X$, there is a rational function F/G in the equivalence class of ϕ with $G(p) \neq 0$. Clearly $G \in J_0$, so $p \notin Z(J_0)$. This forces $Z(J_0)$ to be empty. By the nullstellensatz, $1 \in J_0$. It follows now from the description of J_0 that ϕ is in $k[X]$. □

Morphisms of Varieties: If $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are two algebraic varieties, then a *morphism*

$$\phi : X \longrightarrow Y$$

is given by $\phi = (f_1, \ldots, f_m)$ where each f_i is a regular function on X, i.e. each f_i is a polynomial function on X.

Two varieties X and Y are *isomorphic* if there are polynomial maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$ such that $f \circ g = Id_Y$ and $g \circ f = Id_X$, where Id_X and Id_Y denote the identity map on X and Y respectively. In this case we call f, an also g, an isomorphism between X and Y. If $X = Y$, we usually call f an automorphism.

The simplest case of an automorphism is the one on $\mathbb{A}^n_k$. Let $F = (F_1, \ldots, F_n) : \mathbb{A}^n_k \longrightarrow \mathbb{A}^n_k$ be a polynomial map which is an automorphism. The Jacobian of this map

$$J^{(n)}_k(F) = \det(\frac{\partial F_i}{\partial x_j}),$$

where x_i's are coordinates on $\mathbb{A}^n_k$, is a polynomial and is nonzero wherever F has a local inverse. Since k is algebraically closed and since F is invertible everywhere, $J^{(n)}_k(F)$ is a nonzero constant. The converse however is a challenge. In particular we have,

CONJECTURE 5 (Jacobian Conjecture). *If $J^{(n)}_{\mathbb{C}}(F)$ is a nonzero constant, then F is an automorphism.*

Biregular Theory: When $f : X \longrightarrow Y$ is a morphism of algebraic varieties and $\phi \in k[Y]$ is a polynomial function on Y, then $\phi \circ f$ is a polynomial function on X and is denoted by $f^*\phi$. This is a k-algebra morphism.

Conversely any k-algebra morphism $\alpha : k[Y] \longrightarrow X$ on the coordinate rings induces a map on the varieties themselves. To show this define a map

$$\begin{array}{rcl} f : X & \longrightarrow & \mathbb{A}^m \\ p & \mapsto & (\alpha(y_1)(p), \ldots, \alpha(y_m)(p)). \end{array}$$

We claim that $f(p)$ is actually in Y. To show this take any $G \in I(Y)$. Then $G(f(p)) = G(\alpha(y_1)(p), \ldots, \alpha(y_m)(p)) = \alpha(G(y_1, \ldots, y_m))(p) = 0$ since $G \equiv 0$ in $K[Y]$. This shows that $f(X) \subset Y$. It is also clear that $\alpha = f^*$.

For two algebraic varieties X and Y, we denote the set of all morphisms $f : X \longrightarrow Y$ by $\mathrm{Hom}_k(X, Y)$, and the set of all k-algebra morphisms between their coordinate rings by $\mathrm{Hom}_k(k[Y], k[X])$.

Theorem 6. *There is a one-to-one bijection between the sets* $\mathrm{Hom}_k(X, Y)$ *and* $\mathrm{Hom}_k(k[Y], k[X])$.

□

This theorem is the first crucial link between algebra and geometry. In particular two varieties are isomorphic if and only if their coordinate rings are isomorphic.

Rational Morphisms: If $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ are affine varieties, a *rational morphism*

$$\phi : X \dashrightarrow Y$$

is given by $\phi = (f_1, \ldots, f_m)$ where each f_i is a rational function on X. Two algebraic varieties X and Y are said to be *birationally equivalent*, or simply *birational*, if there exist rational maps $f : X \dashrightarrow Y$ and $g : Y \dashrightarrow X$ such that $f \circ g = Id_V$ and $g \circ f = Id_U$ on some open sets $U \subset X$ and $V \subset Y$.

Birational Theory: Any rational map $f : X \dashrightarrow Y$ between algebraic varieties induces through composition a field morphism $f^* k(Y) \longrightarrow k(X)$. Similar to the biregular theory, any field morphism from $k(Y)$ to $k(X)$ induces and is in turn induced by a rational map from X to Y. Two varieties are birational if and only if their function fields are isomorphic.

Exercises

1. For a morphism $f : X \longrightarrow Y$ of varieties, f^* is injective if and only if $f(X)$ is dense in Y. And if f^* is surjective, then f is an isomorphism of X with $f(X)$.

2. The function field of an algebraic variety is the field of fractions of its coordinate ring. The transcendence degree of the function field over the coordinate ring is equal to the dimension of the variety.

3. If $\mathfrak{p}_1 \subset k[x_1, \dots, x_n]$ and $\mathfrak{p}_2 \subset k[y_1, \dots, y_m]$ are two prime ideals, denote by $\mathfrak{p} \subset k[x_1, \dots, x_n, x_1, \dots, x_m]$ the ideal generated by $\mathfrak{p}_1\mathfrak{p}_2$. Let $X = Z(\mathfrak{p}_1) \subset \mathbb{A}^n$, $Y = Z(\mathfrak{p}_2) \subset \mathbb{A}^m$ and $W = Z(\mathfrak{p}) \subset \mathbb{A}^{n+m}$. Show that the coordinate ring of W is isomorphic to $k[X] \otimes_k k[Y]$ and that W is the product of X and Y in the category of affine varieties with affine morphisms. We denote W by $X \times_k Y$.

4. For an algebraic variety X and any point $p \in X$, the ring $\mathcal{O}_p$ is a local ring whose maximal ideal $\mathfrak{m}_p$ is the set of all regular functions in $\mathcal{O}_p$ vanishing at p. If $Z_X(p)$ denotes the set of all polynomial functions on X vanishing at p, then it is a maximal ideal and $\mathcal{O}_p$ is isomorphic to the localization of $k[X]$ at $Z_X(p)$.

5. If $f \in k[x, y]$ is a non-degenerate quadratic polynomial and $\operatorname{char} k \neq 2$, then the coordinate ring of $Z(f) \subset \mathbb{A}^2$ is isomorphic either to the polynomial ring $k[x]$ or $k[x, \frac{1}{x}]$. What happens if $\operatorname{char} k = 2$?

6. The polynomial map $f : \mathbb{A}^1 \longrightarrow Z(y^2 - x^3) \subset \mathbb{A}^2$, given by $f(t) = (t^2, t^3)$ is one-to-one and onto but the varieties $\mathbb{A}^1$ and $Z(y^2 - x^3)$ are not isomorphic.

3. Complete Intersections

Definition 7. *For an ideal J in $k[x_1, \dots, x_n]$ we define $\mu(J)$ to be the number of elements in a minimal generating set for J. If X is an algebraic set we define $\mu(X)$ as the minimum integer r such that there exist r polynomials $f_1, \dots, f_r$ with $X = Z(f_1, \dots, f_r)$ We define* $\operatorname{codim}(X)$*, the codimension of X, as $n - \dim(X)$, where the dimension of X is its dimension in the Zariski topology of $\mathbb{A}^n$*

We immediately have the inequalities $0 \leq \operatorname{codim}(X) \leq \mu(X) \leq \mu(J(X))$.

In $\mathbb{A}^2$, when C is a curve, we always have $1 = \operatorname{codim} C = \mu(C) = \mu(I(C))$.

Every codimension one variety X in $\mathbb{A}^n$ is a hypersurface and necessarily $n - 1 = \mu(X) = \mu(I(X))$, see [**12**].

For every variety X in $\mathbb{A}^n$, it is known that $\mu(X) \leq n$, see [**5**]. However for any given integer m, there exists a variety X in $\mathbb{A}^n$ with $\mu(I(X)) \geq m$. One such variety will be discussed in the next section.

Complete Intersections: For any variety X, if $\mu(X) = \operatorname{codim} X$, then X is called a *set theoretical complete intersection*, STCI for short. If further $\mu(I(X)) = \operatorname{codim} X$, then X is an *ideal theoretical complete intersection*, or ITCI. We have examples of STCI varieties which are not ICTI.

Conjecture: It is conjectured that all curves in $\mathbb{A}^3$ are STCI.

4. Affine Monomial Curves

It is known that all monomial curves in $\mathbb{A}^3$ are STCI. However the situation is more complicated in $\mathbb{A}^4$. Let $C \in \mathbb{A}^4$ be a monomial curve associated to the integers $m_1, \ldots, m_4$ where $gcd(m_1, \ldots, m_4) = 1$. Let g be the Frobenius number of the semigroup $S = \langle m_1, \ldots, m_4 \rangle$. S is called symmetric if $g - c \in S$ if and only if $c \in \mathbb{N} - S$. It is known that C is a STCI if and only if the semigroup $\langle m_1, \ldots, m_4 \rangle$ is symmetric.

It is an open question to describe all STCI monomial curves in $\mathbb{A}^n$ for $n > 4$.

CHAPTER 2

Projective Varieties

1. First Definitions

The projective n-space over k, denoted by $\mathbb{P}^n_k$, is the space of all lines through the origin in $\mathbb{A}^{n+1}_k$. We also denote it by $\mathbb{P}^n$ if the reference to k is understood. To define a line ℓ through the origin in $\mathbb{A}^{n+1}$ it suffices to know only one point on ℓ other than the origin. If $(x_0, \dots, x_n)$ is such a point, then each $(\lambda x_0, \dots, \lambda x_n)$ is also on ℓ and is different than the origin for every nonzero λ in k. Thus any of these points can be used to uniquely define ℓ. We denote by $[x_0 : \dots : x_n]$ the line passing through $(x_0, \dots, x_n)$ and the the origin in $\mathbb{A}^{n+1}$ when $(x_0, \dots, x_n) \neq (0, \dots, 0)$.

This defines $\mathbb{P}^n$ as the set of equivalence classes of points in $\mathbb{A}^{n+1}\backslash(0, \dots, 0)$, where two points p and q in $\mathbb{A}^{n+1}\backslash(0, \dots, 0)$ are called equivalent if $p = \lambda q$ for some nonzero λ in k. If we denote this equivalence relation by $\sim$, then there is a projection

$$\pi : \mathbb{A}^{n+1}\backslash(0, \dots, 0) \longrightarrow \mathbb{P}^n = \big(\mathbb{A}^{n+1}\backslash(0, \dots, 0)\big)/\sim$$

sending each point p to its equivalence class, the line through p and the origin.

We put on $\mathbb{A}^{n+1}\backslash(0, \dots, 0)$ the induced Zariski topology, i.e. $X \subset \mathbb{A}^{n+1}\backslash(0, \dots, 0)$ is closed if $X = Y \cap \{\mathbb{A}^{n+1}\backslash(0, \dots, 0)\}$ for some closed set $Y \subset \mathbb{A}^{n+1}$. Using this we put on $\mathbb{P}^n$ the quotient topology via the above projection π, i.e. $X \subset \mathbb{P}^n$ is closed if $\pi^{-1}(X) \subset \mathbb{A}^{n+1}\backslash(0, \dots, 0)$ is closed.

If $X \subset \mathbb{P}^n$ is a closed set and $f \in I(\pi^{-1}(X))$, then f vanishes on every line $\ell \subset \pi^{-1}(X)$. If $f = f_0 + \dots + f_d$ where each f_i is homogeneous of degree i, then it follows that each $f_i \in I(\pi^{-1}(X))$. Moreover of $[x_0 : \dots : x_n] \in X$, then $f_i(x_0, \dots, x_n) = 0$ for each $i = 0, \dots, d$.In particular $f_0 \equiv 0$ if X is not empty.

These observations necessitates the following definitions but first recall that a polynomial ideal is called homogeneous if it is generated by homogeneous polynomials.

Zero Set: For any homogeneous ideal J in $k[x_0, \ldots, x_n]$ we define

$$Z(J) = \{[p_0 : \cdots : p_n] \in \mathbb{P}^n \bigm| f(p_0, \ldots, p_n) = 0 \text{ for all } f \in J\ \}.$$

Generally if $p = [p_0 : \cdots : p_n]$, we denote $f(p_0, \ldots, p_n)$ by $f(p)$. If J is generated by the homogeneous polynomials $f_1, \ldots, f_r$, then we denote $Z(J)$ also by $Z(f_1, \ldots, f_r)$. For any two homogeneous ideals $J_1 \subseteq J_2$, we have $Z(J_1) \supseteq Z(J_2)$.

Definition 8. *A subset X of $\mathbb{P}^n$ is called an algebraic set if it is of the form $X = Z(J)$ for some homogeneous ideal $J \subseteq k[x_0, \ldots, x_n]$.*

The topology defined on $\mathbb{P}^n$ by taking algebraic sets as the closed sets is the same as the quotient topology defined above. We also call this topology the Zariski topology.

Clearly $Z(1) = \emptyset$ and $Z(0) = \mathbb{P}^n$ are closed sets. For any point $a = [a_0 : \cdots : a_n] \in \mathbb{P}^n$, let J be the ideal in $k[x_0, \ldots, x_n]$ generated by the set $\{a_i x_j - a_j x_i \bigm| 0 \leq i, j \leq n.\ \}$. Then $Z(J) = \{a\}$.

If J is a homogeneous ideal in $k[x_0, \ldots, x_n]$ then we temporarily denote by $Z_a(J)$ its zero set in $\mathbb{A}^{n+1}$ and by $Z_p(J)$ its zero set in $\mathbb{P}^n$. Using the above projection we have the obvious relation $\pi(Z_a(J) \backslash (0, \ldots, 0)) = Z_p(J)$. We usually drop these subscripts when no confusion arises.

In the affine case we had $Z(J) \neq \emptyset$ for every proper ideal. However in the projective case a slight exception occurs. The ideal in $k[x_0, \ldots, x_n]$ generated by $x_0, \ldots, x_n$ does not have a zero in $\mathbb{P}^n$. We call this ideal the *irrelevant ideal.*

Theorem 9 (Projective Nullstellensatz). *If k is algebraically closed and J is any proper homogeneous ideal in $k[x_0, \ldots, x_n]$ not containing any power of the irrelevant ideal, then $Z(J) \neq \emptyset$.*

Proof. Let $\mathfrak{m}$ denote the irrelevant ideal and $\mathfrak{m}^r \subseteq J$ for some positive integer r. We have the inclusion $Z_a(J) \subseteq Z_a(\mathfrak{m}^r) = \{(0, \ldots, 0)\}$. This forces $Z_p(J)$ to be empty. If J does not contain a power of the irrelevant ideal, then the result follows from the usual Nullstellensatz, Theorem 2. □

Projective Variety: A projective algebraic set is called a projective variety if it is irreducible in the Zariski topology.

The dimension of an algebraic variety is defined as its dimension as a closed set in the Zariski topology.

Ideal of a Set: When X is a subset of $\mathbb{P}^n$ define

$$I(X) = \{f \in k[x_0, \dots, x_n] \bigm| f(p) = 0 \text{ for all } p \in X\ \}.$$

This is necessarily a homogeneous radical ideal. For any subsets $X \subseteq Y$, we have $I(X) \supseteq I(Y)$.

Corollary 10. *If J is any proper homogeneous ideal in $k[x_0, \dots, x_n]$ not containing any power of the irrelevant ideal, then $I(Z(J)) = \sqrt{J}$, where $\sqrt{J}$ is the radical of J.*

Proof. With minor adaptations the proof of Corollary 3 works in this case too. □

We now have an inclusion reversing bijection between the homogeneous radical ideals in $k[x_0, \dots, x_n]$ other than the irrelevant ideal and the algebraic sets in $\mathbb{P}^n$.

2. Projective Morphisms

Polynomial Functions: We do not expect any nontrivial polynomial functions on projective varieties. On one hand there is the technical challenge of defining a polynomial which will evaluate to the same value on each point of a line. On the other hand if $k = \mathbb{C}$, then it can be shown easily using the projection π that $\mathbb{P}^n$ is compact in the metric topology and any polynomial function on $\mathbb{P}^n$, being a global holomorphic function on a compact space, is constant. A projective variety of $\mathbb{P}^n$ is a closed subset of a compact space will also be compact and will carry no nontrivial global functions. This heuristic argument suggests that we start defining the rational functions.

Rational Functions: If we define a rational function in the projective case in exactly the same way as we defined it in the affine case, we would encounter the same technical difficulty mentioned above. Namely, there is no canonical way of choosing a representative from $[x_1 : \cdots : x_n]$, and any choice should be available for calculating the value of the function.

This detail is put aside by using homogeneous polynomials. A *rational function* on a projective variety $X \subseteq \mathbb{P}^n$ is defines as

$$\begin{aligned} \phi : \mathbb{P}^n & \dashrightarrow k \\ [x_1 : \cdots : x_n] & \mapsto \frac{F(x_0, \ldots, x_n)}{G(x_0, \ldots, x_n)}, \end{aligned}$$

for some $F, G \in k[x_0, \ldots, x_n]$ which are homogeneous polynomials of the same degree. Two other homogeneous polynomials $F', G' \in k[x_0, \ldots, x_n]$ of the same degree will define the rational function ϕ as F'/G' if and only if $FG' - F'G = I(X)$. The domain of ϕ as a rational function is X, but as a function its domain consists of those points $p \in X$ for which there are homogeneous polynomials F, G of the same degree such that $\phi(p) = F(p)/G(p)$ and $G(p) \neq 0$.

The set of rational functions form a field, the *rational field* of X, and is denoted by $k(X)$.

Regular Functions: For a point $p \in X \subseteq \mathbb{P}^n$, a rational function $\phi \in k(X)$ is called *regular* at p if there is a representation of ϕ of the form $\phi = F/G$ where $F, G \in k[x_0, \ldots, x_n]$ are homogeneous of the same degree and $G(p) \neq 0$. The set of all functions regular at $p \in X$ form a ring, the ring of regular functions at p, and this ring is denoted by $\mathcal{O}_{p,X}$, or by $\mathcal{O}_p$ if the reference to X is unambiguous.

If U is a subset of X, then as before we denote by $\mathcal{O}(U)$ the ring of regular functions on U. Clearly

$$\mathcal{O}(U) = \bigcap_{p \in U} \mathcal{O}_p.$$

The heuristic arguments of the first paragraph of this section are justified now with the following theorem.

Theorem 11. *If $X \subseteq \mathbb{P}^n_k$ is a projective variety, then*

$$\mathcal{O}(X) = k.$$

In other words, the only global regular functions are constants.

□

Morphisms of Algebraic Sets: If $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ are algebraic sets, then a *morphism* from X to Y is given by

$$\begin{array}{rcl} \phi : X & \longrightarrow & Y \\ p & \mapsto & [f_0(p) : \cdots : f_m(p)] \end{array}$$

where $f_0, \ldots, f_m \in k[x_0, \ldots, x_n]$ are homogeneous polynomials of the same degree not vanishing simultaneously on X. Projective morphisms are locally affine morphisms in the sense that if $D_i \subset X$ is the set on which f_i does not vanish then

$$\phi(p) = [\frac{f_0(p)}{f_i(p)} : \cdots : \frac{f_m(p)}{f_i(p)}]$$

where each f_j/f_i is a regular function on D_i.

Two projective varieties X and Y are *isomorphic* if there are morphisms $f : X \to Y$ and $g : Y \to X$ such that $g \circ f$ and $f \circ g$ are identity maps on X and Y respectively.

Biregular Theory: The affine biregular theory involved coordinate rings. Two affine varieties are isomorphic if and only if their coordinate rings are isomorphic. This fact follows from the fact that the affine coordinate ring $k[X]$ of an affine variety $X \subseteq \mathbb{A}^n$ has two identical descriptions. Both the ring of global regular functions and the quotient ring $k[x_1, \ldots, x_n]/I(X)$ can be taken as $k[X]$. However in the projective case we just saw that the ring of global regular functions consists of only the constants. We can still define the *projective coordinate ring* $k[X]$ of a projective variety $X \subseteq \mathbb{P}^n$ as the quotient ring

$$k[X] = k[x_0, \ldots, x_n]/I(X).$$

This ring however is not a biregular invariant of X since it does not reflect the properties of the global regular functions on X.

Rational Morphisms: Projective rational maps are defined in exactly the same way as the affine case except that the functions are now projective functions given as the ratios of two homogeneous polynomials of the same degree.

If $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ are projective varieties, a *rational morphism*

$$\phi : X \dashrightarrow Y$$

is given by $\phi(p) = [f_0(p) : \cdots : f_m(p)]$ where each f_i is a rational function on X.

Two projective varieties X and Y are said to be *birationally equivalent*, or simply *birational*, if there exist rational morphisms $f : X \dashrightarrow Y$ and $g : Y \dashrightarrow X$ such that $f \circ g = Id_V$ and $g \circ f = Id_U$ on some open sets $U \subset X$ and $V \subset Y$.

Birational Theory: As in the affine case, any rational map $\phi : X \dashrightarrow Y$ induces a field morphism $\phi^* : k(Y) \to k(X)$. Two varieties are birational if and only if their function fields are isomorphic.

3. Affine Covers

In the projective n-space define the open sets

$$U_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \,\big|\, x_i \neq 0\,\},$$

for $i = 0.\ldots, n$. It follows that $\mathbb{P}^n = \bigcap_{i=0}^{n} U_i$. The advantage of this construction is that each U_i is affine through the following map.

$$\begin{array}{rcl} \phi_i : U_i & \longrightarrow & \mathbb{A}^n \\ (x_0 : \cdots : x_n) & \mapsto & (\frac{x_0}{x_i}, \ldots, \frac{\widehat{x_i}}{x_i}, \ldots, \frac{x_n}{x_i}) \end{array}$$

where $\widehat{}$ means that the term is omitted. Defining coordinates on $\mathbb{A}^n$ as

$$z_j^{(i)} = \begin{cases} \frac{x_{j-1}}{x_i} & \text{If } j < i, \\ \frac{x_j}{x_i} & \text{If } j > i. \end{cases}$$

the transition functions are given by

$$\begin{array}{rcl} \phi_j \circ \phi_i^{-1} : \phi_i(U_i \cap U_j) & \longrightarrow & \phi_j(U_i \cap U_j) \\ z = (z_1^{(i)}, \ldots, z_n^{(i)}) & \mapsto & (f_1(z), \ldots, f_n(z)) \end{array}$$

where each $f_s(z)$ is either $\frac{1}{z_j^{(i)}}$ or of the form $\frac{z_t^{(i)}}{z_j^{(i)}}$ for some $t = s - 1, s, s+1$. This makes $\mathbb{P}^n$ a rational k-manifold in the sense that the transition functions are regular rational functions. If $k = \mathbb{C}$, then $\mathbb{P}^n$ is a complex manifold.

CHAPTER 3

Quasi-Projective Varieties

1. First Definitions

Each $\phi_i : U_i \longrightarrow \mathbb{A}^n$ is a bijective map. If U_i is given the induced Zariski topology from $\mathbb{P}^n$ and $\mathbb{A}^n$ is taken with its usual Zariski topology, then ϕ_i becomes a homeomorphism. If $X \subseteq \mathbb{A}^n$ is an affine variety, then the closure of $\phi_i^{-1}(X)$ in $\mathbb{P}^n$ is a projective variety.

A subset $X \subseteq \mathbb{P}^n$ is called a *quasi-projective variety* if the closure of X in $\mathbb{P}^n$ is a projective variety.

This concept collects together both affine and projective varieties and brings forward the significance of searching for birational invariants.

From now on when we say “variety” we will mean a “quasi-projective variety”.

Since coordinate rings are not biregular invariants of projective varieties, we keep the function field as the main algebraic structure associated to a variety.

Exercises

1. The projective variety $Z(x_0x_2 - x_1^2)$ in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$, yet their coordinate rings are not isomorphic.

2. The Krull dimension of the coordinate ring of a projective variety is equal to $\dim X + 1$. In particular $\dim X = \text{tr.deg} k(X) - 1$. The surplus is contributed by the irrelevant ideal.

2. Smoothness

A quasi-projective variety $X \subseteq \mathbb{P}^N$ is going to be called smooth if it locally looks like $\mathbb{A}^n$ where $\dim X = n$. We want to make precise what it means for a variety to locally look like an affine n-space.

Since smoothness is a local concept we want to define what we expect from X if it is going to be smooth at $p \in X$.

Definition 12. *A variety X is called smooth at $p \in X$ if the local ring $\mathcal{O}_p$ is a regular local ring. Otherwise it is called singular at p. X is called smooth if it is smooth at all of its points. It is called singular if it is not smooth.*

Recall that a Noetherian local ring R with maximal ideal $\mathfrak{m}$ is called regular if $\dim R = \dim_k \mathfrak{m}/\mathfrak{m}^2$ where $k = R/\mathfrak{m}$.

If $\mathcal{O}_p$ is the local ring of X at p, then its maximal ideal $\mathfrak{m}$ consists of all $f \in \mathcal{O}_p$ vanishing at p and the underlying field k is recovered as $\mathcal{O}_p/\mathfrak{m}$.

Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ is a set of generators for the ideal J. Define partial derivatives of a polynomial formally, and for every $p \in X = Z(J)$ let

$$Jac(f_1, \ldots, f_m)(p) = \left(\frac{\partial f_i}{\partial x_j}(p) \right)$$

be the Jacobian matrix at $p \in X$ associated with the given basis. Choose another set of generators $g_1, \ldots, g_r$ for the ideal J. Then

$$\operatorname{rank} Jac(f_1, \ldots, f_m)(p) = \operatorname{rank} Jac(g_1, \ldots, g_r)(p).$$

X is smooth at p if and only if this rank is $n - \dim X$.

Exercises

1. If X is singular at p, then $\dim_k \mathfrak{m}/\mathfrak{m}^2 > \dim \mathcal{O}_p$.

2. The set of singular points of a variety X is a proper algebraic subset of X.

3. If X is a smooth variety then $\dim X = \dim \mathcal{O}_p$ for any $p \in X$.

3. Resolution of Singularities

If X and Y are varieties with X singular and Y smooth, and if there is a surjective morphism

$$\phi : Y \longrightarrow X$$

where ϕ^{-1} is defined as a rational map, we say that Y, or ϕ, resolves the singularity of X. In this case there is an open subset U of X, necessarily containing the singular set of X in its complement, such that the restriction map

$$\phi : \phi^{-1}(U) \longrightarrow U$$

is an isomorphism.

When $\operatorname{char} k = 0$, it is known, by Hironaka's famous work [**6**], that a resolution of singularities always exist. Moreover there is a way of obtaining Y from X through a process called blowing up.

We first describe the blowing up of $\mathbb{A}^n$ at the origin. The process consists of replacing the origin by the set of lines through the origin. As a result of this, two distinct lines passing through the origin in $\mathbb{A}^n$ are assigned to two different points in the new space at the origin while keeping their other points unchanged. Thus they no longer intersect in the new space. We need to show how this is accomplished.

Define

$$B_0(\mathbb{A}^n) = \{((x_1, \ldots, x_n), [y_1 : \cdots : y_n]) \in \mathbb{A}^n \times \mathbb{P}^{n-1} \bigm| x_i y_j = x_j y_i,\ 1 \le i, j \le n\ \}.$$

This is a smooth quasi-projective variety which is called the blowing up of $\mathbb{A}^n$ at the origin. We have the canonical projection

$$\begin{array}{rcl} \pi : B_0(\mathbb{A}^n) & \longrightarrow & \mathbb{A}^n \\ ((x_1, \ldots, x_n), [y_1 : \cdots : y_n]) & \mapsto & (x_1, \ldots, x_n) \end{array}$$

which is an isomorphism outside the origin

$$\pi : \pi^{-1}(\mathbb{A}^n - \{(0, \ldots, 0)\}) \xrightarrow{\approx} \mathbb{A}^n - \{(0, \ldots, 0)\}.$$

Moreover the origin is replaced by $\mathbb{P}^{n-1}$ in the sense that

$$\pi^{-1}\left((0, \ldots, 0)\right) = \mathbb{P}^{n-1}.$$

If $X \subseteq \mathbb{A}^n$ is an affine variety with $(0, \ldots, 0) \in X$, then by restricting π to $\pi^{-1}(X)$ we obtain $B_0(X)$, the blowing up of X at the origin. It turns out that

$$B_0(X) = \{((x_1, \dots, x_n), [y_1 : \cdots : y_n]) \in X \times \mathbb{P}^{n-1} \bigm| x_i y_j = x_j y_i,\ 1 \le i, j \le n \},$$

and $\pi : B_0(X) \to X$ the canonical projection on the first component.

CHAPTER 4

Arf Rings and Closure

1. Heuristics

In this preliminary section we will describe how the geometric properties of a curve singularity can be translated into an arithmetic problem involving integers. For this we first associate a particular local ring to the singularity and then we describe in terms of integers what is happening at each step of the resolution of the singularity. The narration in this section is intended to be inspirational rather than rigorous.

Curve Branch: Consider a resolution of a curve C

$$\pi : \tilde{C} \longrightarrow C,$$

and take a point p on C. In general $\pi^{-1}(p) = \{p_1, \ldots, p_r\}$. Here $r = 1$ if p is a smooth point, but it can be larger than one when p is singular. We want to narrow than our attention to a particular neighborhood of the singularity where r is always one.

If U_i is an open neighborhood of p_i not containing any of the other p_j's and moreover if U_i is such that $\pi(U_i)$ does not meet any singular point of C other than p itself, then we call $\pi(U_i)$ a *branch* of the curve at p. This is clearly a local consideration. If $\mathcal{O}_p$ is the local ring of regular functions at p, then the completion of this local ring with respect to its maximal ideal splits up as the sum of several complete local rings. Each of these rings is the completion with respect to its maximal ideal of the local ring of regular functions at p of some branch of C at p.

Multiplicity Sequence: Let C denote a branch at $p \in C$ and assume that $\pi = \pi_m \circ \cdots \pi_1 : \tilde{C} \longrightarrow C$ is a resolution of the branch singularity at $p \in C$. Since $\tilde{C}$ is smooth, there is an open neighborhood of $\pi^{-1}(p)$ which is an isomorphic image of some open subset U of the origin in $\mathbb{A}^1_k$. Composing this with π gives an isomorphism of U with a neighborhood of p with $\mathbb{A}^1$. If C is in $\mathbb{A}^n$, this isomorphism is given by n regular functions on some open neighborhood of $\mathbb{A}^n$. Each of these regular functions are of the form $f_i(t)/g_i(t)$ with $g_i(0) \neq 0$ and $f_i(0) = 0$, $i = 1, \ldots, n$. The *multiplicity* of C at p is defined to be the smallest of the orders of these f_i's, where the order of a polynomial in one variable is its order of vanishing at the origin. Note that the multiplicity of a smooth point is 1.

Let m_i be the multiplicity of $(\pi_i \circ \cdots \pi_1)^{-1}(C)$ at $(\pi_i \circ \cdots \pi_1)^{-1}(p)$, for $i = 0, \ldots, m$ where m_0 is set as the multiplicity of C at p. The sequnce

$$m_0, \ldots, m_r, 1, 1, \ldots$$

is called *the multiplicity sequence* of C at p.

Effect of Blowing up: Assume that C lies in $\mathbb{A}^n$ and p is the origin. If we blow up $\mathbb{A}^n$ at the origin and consider the local affine charts of the blow up, we obtain $(x_1, \ldots, x_n) \mapsto (\frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, x_i, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$. Assume now that $x_j = \phi_j(t)$, $j = 1, \ldots, n$ is a parametrization of C at p. Assuming that the order of ϕ_i is smallest among the orders of the ϕ_j's, the corresponding expression

$$(\frac{\phi_1}{\phi_i}, \ldots, \frac{\phi_{i-1}}{\phi_i}, \phi_i, \frac{\phi_{i+1}}{\phi_i}, \ldots, \frac{\phi_n}{\phi_i})$$

is a parametrization of the first blow up.

2. Formal Set Up

For this section k can be any field. Let $k[[t]]$ denote the ring of formal power series in the variable t. Any element of this ring can be represented as a formal power series of the form

$$\phi(t) = c_0 + c_1 t + \cdots + c_r t^r + \cdots, \text{ where } c_i \in k.$$

This is a unique factorization domain.

We define the order of $\phi(t)$ as

$$\mathrm{ord}\phi(t) = m \text{ if } c_m \neq 0 \text{ and } c_i = 0 \text{ for all } i < m.$$

We note that every element of order zero is invertible in $k[[t]]$. Moreover if $\mathrm{ord}\phi_1(t) < \mathrm{ord}\phi_2(t)$, then $\phi_1(t)|\phi_2(t)$. In other words there is a unique element $(\phi_2/\phi_1)(t) \in k[[t]]$ such that $\phi_2(t) = (\phi_2/\phi_1)(t)\phi_1(t)$.

For any subring H of $k[[t]]$ we define

$$S(H) = \{\mathrm{ord} w \in \mathbb{N} \mid w \in H \}$$

which is a semigroup of $\mathbb{N}$. The greatest common divisor of the elements of $S(H)$ is denoted by $\gcd(S(H))$.

A formal curve branch C is defined to be the set up

$$\begin{aligned} x_1 &= \phi_1(t) \\ &\vdots \\ x_n &= \phi_n(t) \end{aligned}$$

where each $\phi_i(t) \in k[[t]]$ and for the formal power series ring $H = k[[\phi_1, \dots, \phi_n]]$ generated by the ϕ_i's in $k[[t]]$ is such that $\gcd(H) = 1$. We say that the branch passes through the origin if $\phi(0) = \cdots = \phi_n(0) = 0$, or equivalently if the order of each $\phi_i(t)$ is zero. The formal power series ring $H_0 = k[[\phi_1(t), \dots, \phi_n(t)]]$ is called the ring associated to the branch. Note that m_0 is the smallest nonzero integer in H_0, $m_0 = \min S(H_0 \backslash \{0\})$.

If $\text{ord}\phi_1(t) \leq \text{ord}\phi_i(t)$ for all $i = 2, \dots, n$, we say that the multiplicity of the origin on this branch is $m_0 = \text{ord}\phi_1(t)$. In this case we define the blow up of this branch at the origin to be the branch defined by

$$\begin{aligned} x_1 &= \phi_1(t) = \psi_1(t) \\ x_2 &= \frac{\phi_2(t)}{\phi_1(t)} - (\phi_2/\phi_1)(0) = \psi_2(t) \\ &\vdots \\ x_n &= \frac{\phi_n(t)}{\phi_1(t)} - (\phi_n/\phi_1)(0) = \psi_n(t). \end{aligned}$$

This can be interpreted as the image of the blow up in the first open affine chart, where the preimage of the origin is made the origin again by a change of variables. The multiplicity of this branch is $m_1 = \min S(H_1 \backslash \{0\})$, where $H_1 = k[[\psi_1(t), \dots, \psi_n(t)]]$.

Continuing in this way we obtain the sequence of rings $H_0, H_1, \dots$ and integers $m_0, m_1, \dots$ where $m_i = \min S(H_i \backslash \{0\})$ for all $i = 0, 1, \dots$.

The sequence $m_0, m_1, \dots$ is called the *multiplicity sequence* of the branch C, or equivalently of the ring H_0.

Main question: The main question is to find the multiplicity sequence starting with H_0. Since each $\phi_i(t)$ is a formal power series with infinitely many terms, we cannot attack the problem directly as we would not know beforehand how many terms of the division $\phi_i/\phi_j)(t)$ we should keep at each stage so that none of the relevant terms of future blow up constructions will be missed.

The ideal situation would be to recover the multiplicity sequence using only the semigroup $S(H_0)$.

Exercises

1. Let the semigroup $S(H_0)$ consist of the integers $\{i_0, i_1, \dots, i_h, \dots\}$ where $i_h < i_{h+1}$ for all $h = 0, 1, \dots$. Show that $S(H_1)$ is the semigroup of $\mathbb{N}$ generated by the integers $i_2 - i_1, i_3 - i_1, \dots, i_h - i_1, \dots$.

2. The multiplicity eventually stabilizes in the sense that there exists an integer r such that $m_{r+i} = 1$ for all $i = 0, 1, \dots$. Equivalently $H_{r+i} = k[[t]]$ for all $i \geq 0$. The geometric interpretation of this is that branch singularities are eventually resolved.

3. Arf Semigroups

The multiplicity sequence will be obtained through the generators of a certain semigroup associated to the local ring of the branch singularity. We will therefore give a through analysis of the kind of semigroups that will be used. Our main source is Arf's classical article [**1**].

A *semigroup* is defined as a nonempty subset of nonnegative integers, containing zero and is closed under addition.

We say that the semigroup G is generated by the nonnegative integers $a_1, \dots, a_n$ if all elements of G are of the form $c_1 a_1 + \cdots + c_n a_n$ where each c_i is a nonnegative integer. In this case we use the notation $G = \langle a_1, \dots, a_n \rangle$ and say that the semigroup is *finitely generated.*

If d is the greatest common divisor of all the elements of a semigroup G, we can divide every element of G by d and obtain a new semigroup G' with $gcd\, G' = 1$. Any property of G' which will interest us can easily be translated back to G. Therefore we will assume throughout this section that $d = 1$ unless we need and announce it otherwise.

We will first settle two fundamental properties of semigroups. Since we are assuming that the greatest common divisor of the elements of the semigroup G is 1, the first fundamental property of G is that it contains all integers n where $n \geq n_0$ for some $n_0 \in \mathbb{N}$. In other words, the complement of G in $\mathbb{N}$ is finite.

The other fundamental property is that a semigroup is finitely generated in the sense explained above.

We prove these properties in the next two lemmas.

LEMMA 13. *If G is a semigroup with $\gcd G = 1$, then there exists an integer $n_0 \in \mathbb{N}$ such that $n \in G$ for every $n \geq n_0$.* □

LEMMA 14. *Every semigroup is finitely generated.* □

Let $G = \{i_0, i_1, i_2, \dots, i_h, \dots\}$ be a semigroup where $i_0 = 0$ and the elements are given in increasing order, $i_\ell < i_{\ell+1}$ for every $\ell \geq 0$. For every $h \geq 0$ we define the set

$$[G - i_h] := \{i_n - i_h \mid n \geq h\},$$

and the semigroup G_h to be the smallest semigroup in $\mathbb{N}$ containing the set $[G - i_h]$. The elements of G_h are finite linear combinations of elements of $[G - i_h]$ with coefficients from $\mathbb{N}$.

DEFINITION 15. *A semigroup G is called an* Arf semigroup *if $G_h = [G - i_h]$ for every $h \geq 0$.*

The simplest Arf semigroup is $\mathbb{N}$. Thus every semigroup is contained in an Arf semigroup. This prompts the concept of the smallest Arf semigroup containing a semigroup, if such an object can be uniquely defined. The following lemma addresses this issue.

LEMMA 16. *The intersection of two Arf semigroups is an Arf semigroup.* □

PROOF. If G and H are Arf semigroups, then clearly $^*(G \cap H)$ is contained in both G and H and must therefore be contained in their intersection. It then turns out that $^*(G \cap H)$ is contained in and also contains $G \cap H$, so must be equal to it. □

We can now define the *Arf closure* of a semigroup G as the smallest Arf semigroup containing G. We denote the Arf closure of G by $^*G$.

The set of all Arf semigroups containing G is nonempty since $\mathbb{N}$ is Arf and contains G. Using Zorn's lemma and the above lemma it can be shown that the Arf closure of a semigroup exists and is uniquely defined.

We now take up the task of actually constructing the Arf closure of any semigroup. Let $G = \{i_0, i_1, i_2, \ldots, i_h, \ldots\}$ be a semigroup where the notation is as above. First construct the semigroup G_1 as described above and notice that the set

$$i_1 + G_1 = \{i_1 + g \mid g \in G_1\}$$

is closed under addition, since $i_1 = 2i_1 - i_1$ is in G_1. This set is almost a semigroup except that it misses the zero element. We use the notation $\{0, i_1 + G_1\}$ to denote the semigroup obtained by introducing the zero element into the set $i_1 + G_1$. The following inclusions are obvious but important to observe.

$$G \subset \{0, i_1 + G_1\} \subset {}^*G.$$

From these inclusions and from the definition of Arf closure it now follows that

$$\{0, i_1 + G_1\} \subset {}^*\{0, i_1 + G_1\} \subset {}^*G.$$

It is straightforward to see that actually

$${}^*\{0, i_1 + G_1\} = \{0, i_1 + {}^*G_1\}.$$

This makes $\{0, i_1 + {}^*G_1\}$ the smallest Arf semigroup containing G, and hence we have

$${}^*G = \{0, i_1 + {}^*G_1\}.$$

This reduces the task of finding ${}^*G$ to that of finding ${}^*G_1$. But is it really a reduction?

We know that $G = \{i_0, i_1, \ldots, i_r + \mathbb{N}\}$ where the notation is meant to mean that $i_r - 1 \notin G$ but $i_r + n \in G$ for every $n \in \mathbb{N}$. Using the same notation we write $G_1 = \{j_0, j_1, \ldots j_s + \mathbb{N}\}$. It can be shown that $j_s < i_r$, so this is an actual reduction.

To construct ${}^*G_1$ we repeat the above process. Define $G_{1,1}$ to be the semigroup generated by the set $\{j_n - j_1 | j_n \in G_1,\ n \geq 1\}$. Then we have ${}^*G_1 = {}^*\{0, j_1 + {}^*G_{1,1}\}$. Continuing in this way we will eventually have $G_{1,\ldots,1} = \mathbb{N}$ which is already an Arf ring. Thus the process will terminate after finitely many steps.

We can now give a full description of all Arf semigroups. For this we rewrite the entries of a semigroup G as follows:

$$G = \{0, m_1, m_1 + m_2, m_1 + m_2 + m_3, \dots, m_1 + \dots + m_r + \mathbb{N}\}.$$

The sequence $m_1, \dots, m_r$ is a non-increasing sequence of non-negative integers. We complete this finite sequence to an infinite sequence by adjoining infinitely many 1s.

$$m_1, m_2, \dots, m_r, 1, 1, \dots.$$

The notation is meant to imply that $m_r > 1$.

We can now describe all Arf semigroups.

Lemma 17. *A semigroup $G = \{0, m_1, m_1 + m_2, m_1 + m_2 + m_3, \dots, m_1 + \dots + m_r + \mathbb{N}\}$ is an Arf semigroup if and only if there exists a non-increasing sequence $m_1, m_2, \dots m_r, 1, 1, \dots$ of non-negative integers terminating in a sequence of repeating 1s where $m_r > 1$ and such that*

$$m_n \in \{m_{n+1}, m_{n+1} + m_{n+2}, \dots, m_{n+1} + \dots + m_r + \mathbb{N}\} \textit{ for } n = 1, \dots, r - 1.$$

□

The question of finding the Arf closure of a semigroup G now reduces to finding the above sequence of integers once the generators of G are given. In other words, if $G = \langle a_1, \dots, a_n \rangle$, for some finite set of non-negative integers $a_1, \dots, a_n$, then how do we find $m_1, m_2, \dots$ which describe *G?

The sequence $m_1, \dots, m_r, 1, 1, \dots$ must be encoded in the set of generators $a_1, \dots, a_n$, but how do we recover them? To answer this we describe now Du Val's version of the Jacobi algorithm. The Jacobi algorithm is an algorithm for finding greatest common divisor of a finite set of non-negative integers, which generalizes the Euclidean algorithm for finding the greatest common divisor of two integers. Du Val slows down the process in the Jacobi algorithm to bring out a sequence of non-decreasing non-negative integers, see [**2**].

The Du Val-Jacobi algorithm consists of the following procedure:

Start with $\{S = \{a_1, \dots, a_n\}, i\}$. Assume without loss of generality that $a_1 \leq a_2 \leq \dots \leq a_n$. We now set $q = \lfloor a_2/a_1 \rfloor$ and define $m_{i+1} = \dots = m_{i+q} = a_1$. The new set S is defined as $S = \{a_1, a_2 - qa_1, \dots, a_n - qa_1\}$. We then repeat this process with $\{S, q\}$. The process terminates when S is a singleton. Assuming that the greatest common divisor of the integers $a_1, \dots, a_n$ is 1, the last integer obtained through the algorithm is $m_s = 1$. We adjoin to this finite sequence infinitely many 1s to obtain the sequence

$$m_1, m_2, \dots, m_r, 1, 1, \dots$$

with the understanding that $m_r > 1$.

Lemma 18. *The sequence $m_1, \dots, m_r, 1, 1, \dots$ describing the Arf closure of a semigroup $G = \langle a_1, \dots, a_n \rangle$ can be recovered from the generators of G by Du Val's modified Jacobi algorithm where we start with $\{S = \{a_1, \dots, a_n\}, 0\}$.* □

The construction of Arf closure of a semigroup is now totally understood. We therefore dare to ask deeper questions. For example experience with the Jacobi algorithm suggests that sometimes a proper subset of the generators $a_1, \dots, a_n$ also give the same sequence. So what is the minimal set of integers which will give the same sequence $m_1, m_2, \dots$?

We start this road of investigation with the following observation.

Lemma 19. *If G and H are two semigroups with ${}^*G = {}^*H$, then ${}^*(G \cap H) = {}^*G = {}^*H$.*

Proof. If $G = \{0, i_1, i_2, \dots\}$ and $H = \{0, j_1, j_2, \dots\}$, then clearly $i_1 = j_1$ since ${}^*G = {}^*H$. This gives

$${}^*G = \{0, i_1 + {}^*G_1\} \text{ and } {}^*H = \{0, i_1 + {}^*H_1\}.$$

Thus the problem reduces to showing that ${}^*(G_1 \cap H_1)$. If we repeat this process we will eventually get $G_{1,\dots,1} = \mathbb{N}$ when the statement of the claim is trivial. □

Let G_χ be the intersection of all semigroups whose Arf closures are equal to ${}^*G$. We just showed that ${}^*G_\chi = {}^*G$. Let $\chi_1, \dots, \chi_n$ be the minimal set of generators of G_χ over $\mathbb{N}$.

This semigroup G_χ is called the *characteristic semigroup* of G, and its minimal generators $\chi_1, \dots, \chi_n$ are called the *Arf characters* of G.

Finally, we observe the following.

Lemma 20. *The set of characters of $G = \langle a_1, \dots, a_n \rangle$ is a subset of the set of generators $a_1, \dots, a_n$, and the sequence obtained from the set* *of characters by the Du Val-Jacobi algorithm is the same as the one obtained from the generators of G.* □

Observe also that if $\chi_1, \ldots, \chi_n$ is the set of Arf characters of G giving the sequence $m_1, m_2, \ldots$ through the Du Val-Jacobi algorithm, then the set of integers obtained from the set of Arf characters of G adjoining any number of elements from $^*G$ give the same sequence through the Du Val-Jacobi algorithm.

Exercises

1. Give proofs of all the lemmas whose proofs are not given in the text.

2. Report any errors, ambiguities, misspellings suggestions etc. immediately to *sertoz@bilkent.edu.tr*.

4. Arf Rings

As in the previous section let $H = k[[\phi_1(t), \ldots, \phi_n(t)]]$ be the subring of $k[[t]]$ generated by the formal power series $\phi_1(t), \ldots, \phi_n(t)$ such that

$$\gcd\{\text{ord}\phi_1(t), \ldots, \text{ord}\phi_n(t)\} = 1.$$

For every nonnegative integer m define

$$I_m = \{s \in H \mid \text{ord}s \geq m \},$$

and for every $m \in S(H)$ let s_m denote a fixed element of order m in H. Clearly if s'_m is another element of order m, then $s_m = \alpha s'_m$ where $\alpha \in k[[t]]$ is a unit.

For every $m \in S(H)$ we define the set

$$I_m/s_m = \{\frac{\phi}{s_m} \mid \phi \in I_m \}.$$

This set is closed under addition but not necessarily under multiplication.

Let $[I_m/s_m]$ denote the ring generated in $k[[t]]$ by the set I_m/s_m. If I_m/s_m is closed under multiplication then $[I_m/s_m]$ is nothing but I_m/s_m itself. The ring $[I_m/s_m]$ does not depend on the choice of the element s_m, so we use the notation

$$[I_m] = [I_m/s_m]\,.$$

Definition 21. *A subring H of $k[[t]]$ is called an* Arf ring *if the set I_m/s_m is always closed under multiplication for every $m \in S(H)$ and every element s_m of order m. The smallest Arf ring containing H in $k[[t]]$ is called the* Arf closure *of H and is denoted by ${}^*H$*

Since $k[[t]]$ is clearly an Arf ring, and since the intersection of two Arf rings is again an Arf ring, Arf closure of any ring exists.

We have a dual definition for semigroups.

Definition 22. *A subsemigroup S of $\mathbb{N}$ is called an* Arf semigroup *if the set $\{m' - m \mid m' \in S$ and $m' \geq m\ \}$ is a semigroup. The smallest Arf semigroup in $\mathbb{N}$ containing S is called the* Arf closure *of S and is denoted by ${}^*S$.*

Again by observing that $\mathbb{N}$ is an Arf semigroup and that the intersection of two Arf semigroups is an Arf semigroup, we conclude that Arf closure of any semigroup exists.

The multiplicity sequence can now be redescribed using the above concepts. Suppose we have: $H = k[[\phi_1(t), \ldots, \phi_n(t)]]$ where each $\phi_i(t) \in k[[t]]$ with $\gcd\{\mathrm{ord}\phi_1(t), \ldots, \mathrm{ord}\phi_n(t)\} = 1$. Assume that the multiplicity sequence of the branch formally parameterized by the $\phi_i(t)$'s is $m_0, m_1, \ldots$. We want to describe a procedure to obtain this multiplicity sequence.

Let $H_0 = H$. Then clearly m_0 is the smallest nonzero integer in $S(H_0)$. Define H_1 to be $[I_{m_0}]$ for the ring H_0. Then m_1 is the smallest nonzero integer in $S(H_1)$.

Having defined $H_0, \ldots, H_i$ and the sequence of integers $m_0, \ldots, m_i$, we define H_{i+1} to be $[I_{m_i}]$ of the ring H_i, and then m_{i+1} is define to be the smallest nonzero integer in $S(H_{i+1})$.

The point of all these definitions is the following theorem.

Theorem 23. *The multiplicity sequence obtained from H is the same as the one obtained from ${}^*H$.* □

Observe that if H is an Arf ring, then necessarily $S(H)$ is an Arf semigroup but not conversely.

Exercises

1. If H is the subring of $k[[t]]$ generated by some elements $\phi_1(t), \ldots, \phi_n(t) \in k[[t]]$ where the greatest common divisor of the orders of the ϕ_i's is one, then H is isomorphic to the ring $k + ks_1 + \cdots + ks_m + k[[t]]s_{m+1}$ where the s_i's are elements of $k[[t]]$ with $\mathrm{ord}s_1 < \cdots < \mathrm{ord}s_{m+1}$.

5. Constructing Arf Closure: Rings

CHAPTER 5

Curves

1. First Definitions

A curve X is a smooth projective variety of dimension one. At every point $p \in X$ the local ring of regular functions $\mathcal{O}_p$ is a regular ring of dimension one. Such a ring is a principal ideal domain. If $\mathfrak{m}_p$ is the maximal ideal of regular functions vanishing at p, then it is generated by an element t. It follows that every element of $\mathcal{O}_p$ is of the form ut^n where u is a unit and n is a non-negative integer. If $f \in k[X]$ is a rational function then either f or $1/f$ is regular at p. If f is regular at p and is non-zero there, then both f and $1/f$ are regular at p.

Since X has no non-constant global regular functions, there is a point q on X where t is not regular. If we denote a generator of $\mathfrak{m}_q$ by s, then t at q is $1/s$ up to a unit. It follows that every rational function on X is of the form t^n up to a unit. The exponent n is called the order of f at p and is denoted by $\operatorname{ord}_p(f)$. Units at p on the other hand represent rational functions of X that do not vanish at p.

If a rational function f on X is not regular at p, then $1/f$ vanishes at p. In this case p is called a pole of f with order equal to the vanishing order of $1/f$ at p and the order of the pole is $-\operatorname{ord}_p(f)$.

Lemma 24. *The number of zeros of a rational function is equal to its number of poles, both counted with multiplicity.* □

A *divisor* on X is a formal sum $D = \sum_{p \in X} n_p p$ where each n_p is an integer and only finitely many of the integers n_p are non-zero. If $D' = \sum_{p \in X} m_p p$ is another divisor, then we define the sum of D and D' point wise, $D + D' = \sum_{p \in X} (n_p + m_p)p$. The set of all divisors on X, denoted by $\operatorname{Div}(X)$, forms an Abelian group under this addition.

A divisor $D = \sum_{p \in X} n_p p$ is called *effective* if all $n_p \geq 0$. The degree of D is defined as $\deg D = \sum n_p$. We say $\sum n_p p \geq \sum m_p p$ when each $n_p \geq m_p$. It follows from these definitions that $D \geq D'$ if and only if $D - D' \geq 0$ or equivalently if and only if $D - D'$ is effective.

If f is a rational function on X, then we define the divisor of f on X as

$$(f) = \sum_{p \in X} \mathrm{ord}_p(f) p.$$

From the above lemma it follows that $\deg(f) = 0$. We write (f) as the difference of two effective divisors

$$(f) = (f)_0 - (f)_\infty$$

where $(f)_0 = \displaystyle\sum_{\mathrm{ord}_{p(f)>0}} \mathrm{ord}_p(f) p$ and $(f)_0 = \displaystyle\sum_{\mathrm{ord}_{p(f)<0}} \mathrm{ord}_p(f) p$. These are called the divisors of zeros and poles of f respectively.

Two divisors D and D' are called *linearly equivalent* and denoted by $D \equiv D'$ if $D - D' = (f)$ for some rational function f on X.

For any divisor D, the set of all effective divisors linearly equivalent to it is denoted by $|D|$. This is called the *complete linear system* associated to D.

Exercises

1. Show directly that on $\mathbb{P}^1$, a rational function has as many zeros as poles, counting multiplicities.

2. Any two points on $\mathbb{P}^1$ are linearly equivalent as divisors. In fact on $\mathbb{P}^1$ any two divisors of the same degree are linearly equivalent.

3. The complete linear system $|D|$ is empty if $\deg(D) \leq 0$.

2. Riemann's Inequality

For a divisor $D = \sum_{p \in X} n_p p$ we define

$$L(D) = \{f \in k(X) \mid f = 0 \text{ or } (f) + D \geq 0\}.$$

$L(D)$ is a k-vector space. We denote its dimension by $\ell(D)$.

LEMMA 25. *For any divisor $D \in \mathrm{Div}(X)$ we have;*
(i) If $L(D) \neq \{0\}$, then $\deg(D) \geq 0$.
(ii) If $D \geq 0$, then $\ell(D) \geq 1$.

PROOF. If $f \in L(D)$ and f is not zero, then $(f) + D \geq 0$ implies that $\deg(D) \geq 0$ since $\deg(f) = 0$. If on the other hand $D \geq 0$, then for any constant function f we have $(f) + D \geq 0$ since in this case $(f) = 0$. □

It follows in particular that $\ell(D) = 0$ when $\deg(D) < 0$.

LEMMA 26. *For any divisor $D = \sum_{q \in X} n_q q$ and any point p on X we have $\ell(D) \leq \ell(D + p) \leq \ell(D) + 1$.*

PROOF. Clearly $L(D) \subset L(D + p)$ so the first inequality is immediate. For the second inequality choose a generator t of $\mathfrak{m}_p$. Then $\mathrm{ord}_p(t) = 1$. If $f \in L(D + p)$, then $\mathrm{ord}_p(t^{n_p+1} f) = \mathrm{ord}_p(t^{n_p+1}) + \mathrm{ord}_p(f) \geq 0$ and it follows that $t^{n_p+1} f$ is regular at p. This defines a linear map

$$\begin{array}{rcl} \phi : L(D + p) & \longrightarrow & k \\ f & \mapsto & (t^{n_p+1} f)(p). \end{array}$$

If f is in the kernel of ϕ, then $\mathrm{ord}_p(t^{n_p+1} f) > 0$, or $n_p + \mathrm{ord}_p(f) \geq 0$, putting f in $L(D)$. Conversely it is clear that $L(D) \subset \ker \phi$. The lemma now follows since the rank of the range is at most one. □

COROLLARY 27. $\ell(D) \leq 1 + \deg D$ *when* $\deg D \geq 0$.

PROOF. If $n = \deg D$ define $D' = D - (n + 1)p$ for some fixed $p \in X$. Now lemma 26 applied $n + 1$ times gives $\ell(D) \leq \ell(D') + n + 1$. But $\ell(D') = 0$ since $\deg D' < 0$. □

How sensitive is $\ell(D)$ to the degree of D? Is it possible to pick a point $p \in X$ such that $\ell(np)$ remains bounded as n increases beyond bound? The answer to such queries is given by the following theorem.

THEOREM 28 (Riemann's Inequality). *For any curve X, there is an integer g such that*

$$\ell(D) \geq \deg(D) + 1 - g$$

for all divisors $D \in \mathrm{Div}(X)$. The smallest such integer g is called the genus *of X and is also denoted by $g(X)$.* □

We observed before that there are no global non-trivial regular functions on a projective curve X but we did not address the question of existence for global non-trivial rational functions on X. Riemann's inequality now answers this question. Pick any point $p \in X$. Then $\ell(np) > 1$ when $n > g$. It implies that there is a rational function with a pole of order n at p and regular elsewhere.

Exercises

1. The complete linear system $|D|$ is the projectivization of the vector space $L(D)$ and as a projective space its dimension is $\ell(D) - 1$.

2. For any point $p \in \mathbb{P}^1$, we have $\ell(p) = 2$. In fact for any curve X, if for some point $p \in X$ we have $\ell(p) > 1$, then X is isomorphic to $\mathbb{P}^1$, and $\ell(p) = 2$ for all $p \in X$.

3. If $D \in \mathrm{Div}(\mathbb{P}^1)$ with $\deg(D) = n \geq 0$, then $\ell(D) = n + 1$.

4. Show that the genus of $\mathbb{P}^1$ is zero and in fact any curve of genus zero is isomorphic to $\mathbb{P}^1$.

3. Differentials and Canonical Divisors

A differential ω on X is a choice of a rational function f_p at every $p \in X$ subject to the following condition: If t is a local parameter at p and s at q, with $t = \alpha(s)$, where $\alpha(s)$ is an invertible rational function of s, then $f_q(s) = f_p(\alpha(s))\alpha'(s))$. Here the derivative of $\alpha(s)$ with respect to s is defined formally.

We define the divisor associated to the differential $\omega = \{f_p | \, p \in X\}$ as $(\omega) = \sum_{p \in X} \mathrm{ord}_p(\omega) p$ where $\mathrm{ord}_p(\omega) = \mathrm{ord}_p(f_p)$.

If $\omega = \{f_p | \, p \in X\}$ and $\omega' = \{g_p | \, p \in X\}$ are two differentials, then $(\omega) = (\omega') + (h)$ where h is the rational function which is given by f_p/g_p at p. Therefore every differential on X defines the same divisor up to linear equivalence. We call any of these divisors the *canonical divisor* of X and denote it by K.

We can simplify the definition of a differential for practical purposes. If t_0 is a local parameter at $p_0 \in X$, let U_0 be an open set in X on which t_0 is regular. Then consider only those points p_i which are on X but outside U_0 and for each such p_i, consider the open set U_i on which the local parameter t_i is regular. Finitely many of these U_i will cover X. At each p_i choose a rational function f_i subject to the condition that on $U_i \cap U_j$, $f_i(t_i) = f_j(\alpha_{ji}(t_i))\alpha'_{ji}(t_i)$ where $\alpha_{ji}(t_i) = t_j$ is invertible. Then for any $p \in U_i \cap U_j$, we have $\mathrm{ord}_p f_i(t_i) = \mathrm{ord}_p f_j(t_j)$ and this defines the canonical divisor.

We can calculate the canonical divisor of $\mathbb{P}^1$ as follows. Let $[x_0 : x_1]$ be homogeneous coordinates and $t = x_1/x_0$, $s = x_0/x_1$ the local parameters. Here $t = \alpha_{01}(s) = 1/s$. We can choose $f_0(t) = 1$ and $f_1(s) = -1/s^2$. Since $f_1(s) = f_0(1/s)(-1/s^2)$, we see that $K = -2[0 : 1]$.

The term that makes the Riemann's inequality an equality can now be described in terms of the canonical divisor.

Theorem 29 (The Riemann-Roch Theorem). *For any divisor D on a curve X of genus g, we have the equality*

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

where K is the canonical divisor of X.

Using the Riemann-Roch theorem first for $D = 0$ we get

$$\ell(K) = g.$$

Next using this together with the Riemann-Roch theorem for $D = K$, we get

$$\deg(K) = 2g - 2.$$

Since the canonical divisor for $\mathbb{P}^1$ has degree -2, this gives another verification of the fact that its genus is zero. This prompts the question: For any positive integer g, is there a curve of genus g?

Bibliography

[1] Arf, C., Une interprétation algébrique de la suite des ordres de multiplicité d'une branche algébrique, Proc London Math Soc, Series 2, 50 (1949), 256-287.

[2] Du Val, P., The Jacobian algorithm and the multiplicity sequence of an algebraic branch, İstanbul University Faculty of Science Journal, Serie A, Vol VII, no: 3-4, (1942), 107-112.

[3] Du Val, P., Note on Cahit Arf's "Une interprétation algébrique de la suite des ordres de multiplicité d'une branche algébrique", Proc London Math Soc, Series 2, 50 (1949), 288-294.

[4] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag GTM 150, (1995).

[5] Eisenbud, D., Evans, E. G., Every algebraic set in n-space is the intersection of n hypersurfaces, Inv. Math. 19 (1973), 107-112.

[6] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. Math. 79 (1964) 109-326.

[7] Sertöz, S., On Arf Rings, Appendix in: *The Collected Papers of Cahit Arf*, Turkish Mathematical Society, (1990), 416–419.

[8] Sertöz, S., Arf rings and characters, Note di Math, 14 (1994), 251-261 (1997).

[9] Sertöz, S. : On the Number of Solutions of a Diophantine Equation of Frobenius, Discrete Mathematics and Applications, Vol 8, No 2, (1998), 153-162.

[10] Sertöz, S., Özlük, Ali E., On a Diophantine problem of Frobenius. Istanbul Tek. Univ. Bull. 39 (1986), no. 1, 41–51.

[11] Sertöz, S., Özlük, Ali E., On the number of representations of an integer by a linear form. İstanbul University Faculty of Science Journal, 50 (1991), 67–77 (1993).

[12] Shafarevich, I. R., *Basic Algebraic Geometry*, Springer-Verlag (1994).

[13] Zariski, O., Samuel, P., *Commutative Algebra.* Vol I, Graduate Texts in Mathematics no: 28, Springer-Verlag (1975)

[14] Zariski, O., Samuel, P., *Commutative Algebra.* Vol II, Graduate Texts in Mathematics no: 29, Springer-Verlag (1975)