Basic algebraic geometry for coding theory

Rolf-Peter Holzapfel

Basic Algebraic Geometry for Coding Theory

Lectures on the CIMPA-UNSA-ICTP-UNESCO-ICIMAF School
"Algebraic Geometry and its Applications
to Error Correcting Codes and Cryptography"
Havanna, 20-th Novembre - 1-st December 2000
vspace5mm Rolf-Peter Holzapfel, Humboldt-Universitaet Berlin

December 12, 2000

Contents

1 Introduction

According to my experience one should start after some historical interesting elementary codes with the original Goppa codes as in [9a] in order to understand error correcting codes living on algebraic curves over finite fields as basically described in Stichtenoth's book [7]. But this is an arithmetic-geometric jump which should be well-prepared. The aim of my lectures was to present the fundamental background knowledges of algebraic geometry hoping that graduate students starting on this field can understand the things better, in a more contineous manner. We avoid in this summery schemes, sheaves, higher cohomology groups and adéles, but the basic definitions, relations and theorems presented in my lectures are also thought as necessary preparation for deeper work in one or the other of these directions. The order of presentation is well-choosen. It corresponds to the order of proofs (in my lectures in Berlin), which are omitted here in general. We concentrate our attention to the case of algebraically closed basic fields. If it is not necessary we will announce it (quite often) and work in more generality. At some places, when derivaties play a role, we are forced to restrict ourselves to characteristic 0. Naturally, on the topological side of Riemann surface theory one has to use basically the complex numbers. Real numbers are necessary for visualisation of plane curves, their singularities and quadratic transforms. We add a MAPLE file with real curves expositing nice singularities and birational transforms. This file "CurvAlbm.mws" must be implanted into the MAPLE-package to be readable. It plays also the role of a foto album for curves I met during the preparation of the school and and in some other lectures there. The picture "Newton's heart" discovered in Newton's knot should be taken as a symbol for all activities of the school.

I want to mention that this guideline of algebraic curve theory contains also little innovations in order to find a most natural and effective way of presentation. On the one hand we introduced the K-Dimension of K-algebras substituting Krull-dimension, see 2.6. It opens some problems which could be solved by advanced students. On the other hand, I believe deeply that the more immediate Mittag-Leffler approach to the Riemann-Roch Theorem using spaces of Laurent tails only can be used to substitute completely the adéle methods in [6] for each characteristics. This should be carefully investigated and written down in detail. At least it is a good preparation for understanding the arithmetic adéle theory with applications.

[0]The author thanks heartly the organizers at CIMPA, UNSA, ICTP, UNESCO, ICIMAF for the invitation as lector to this interesting school.

2 Algebra and Affine Geometry

Definition 2.1 . *Let K be a field; a* commutative K-algebra *is a commutative ring R containing K as subring.*

Since non-commutative K-algebras do not play any role in this summary, we call our commutative K-algebras shortly *K-algebras*. We do the same for *rings* omitting the adjective "commutative", which the reader should have in mind. For instance, the ring $K[X_1, ..., X_n]$ of polynomials with n variables $X_1, ..., X_n$ and coefficients in K is a K-algebra, which plays a fundamental role in algebraic geometry. An *ideal* of a ring R is a subgroup of the aditive group of R, which is closed under R-multiplication. Besides of intersections the most important binary operations in the ordered set of ideals of R are sums and products, defined by

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \{a + b;\ a \in \mathfrak{a},\ b \in \mathfrak{b}\} \\ \mathfrak{a} \cdot \mathfrak{b} &= \{a_1 b_1 + ... + a_k b_k;\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b},\ k \in \mathbb{N}_+\} \end{aligned}$$

The definitions can be extended to sums and products of more than two ideals in obvious manner. It should be mentioned that the distributive law

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$$

holds, which is also extendable to more than two summands.

Ideals of the form

$$\mathfrak{a} = (a_1, a_2, ..., a_k) := Ra_1 + Ra_2 + ... + Ra_k,\ a_i \in R,$$

are called *finitely generated* with $a_1, a_2, ..., a_k$ as (set of) *generators*, sometimes also called *ideal basis* of $\mathfrak{a}$. Ideals (a) generated by one element only, are called *principal*. The *trivial ideals* are the principal ideals (0) and $(1) = R$. All other ideals are called *non-trivial*. The *proper ideals* are the ideals different from R. A ring is a field if and only if it has only trivial ideals.

If $\mathfrak{a}$ is a proper ideal of the a K-algebra R, then the *residue class ring* $R/\mathfrak{a}$ with addition and multiplication defined by representatives) is also a K-algebra. The ideal $\mathfrak{a}$ of a ring R is the kernel of the residue class map $R \longrightarrow R/\mathfrak{a}$, which is a ring homomorphism (sending $r \in R$ to its residue class $r \ mod \ \mathfrak{a}$). An *maximal ideal* $\mathfrak{m}$ is a maximal one in the set of proper ideals of R. It is equivalent to say that $R/\mathfrak{m}$ is a field. The ideal $\mathfrak{p}$ is called *prime*, if and only if $R/\mathfrak{p}$ is a *domain*; this means a commutative ring with unit element but without zero divisors. An element $\pi \in R$ is a *prime element* iff (π) is a prime ideal. We say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ and write $a \,|\, \mathfrak{b}$, iff $a \supseteq \mathfrak{b}$. Prime ideals are characterized by the implication

$$\mathfrak{p} \,|\, \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \,|\, \mathfrak{a} \ or \ \mathfrak{p} \,|\, \mathfrak{b}$$

for all ideals $\mathfrak{a}$, $\mathfrak{b}$ of R. Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are *relatively prime*, if and only if $\mathfrak{a} + \mathfrak{b} = (1)$. It is easy to extend the definition to finitely many ideals.

R is a *finitely generated* K-algebra iff there exist elements $x_1, ..., x_n \in R$ (called *generators*) such that

$$R = K[x_1, ..., x_n] = \{f(x_1, ..., x_n);\ f \in K[X_1, ..., X_n]\}.$$

Up to isomorphy, the proper residue class rings of the polynomial ring $K[X] := K[X_1, ..., X_n]$ and the K-algebras generated by n elements are in bijective correspondence. Namely,

$$K[x_1, ..., x_n] \cong K[X]/\mathfrak{a}, \quad \mathfrak{a} = \{f \in K[X];\ f(x_1, ..., x_n) = 0\}.$$

Not only the residue class rings of ideals of $K[X]$ are finitely generated but also the ideals themselves. More generally, we dispose on the important

Hilbert's Basis Theorem 2.2 . *Each ideal of a finitelely generated K-algebra is finitely generated.*

For a modern argument one defines *noetherian* rings R by the *ascending chain condition*, which says that each strictly ascending chain of ideals of R must terminate (after finitely many steps). It is easy to verify the equivalence with the *finite base property*: each ideal of R is finitely generated. One proves that the noetherian property of R is preserved for the ring $R[T]$ of polynomials over R in one variable T. The original theorem of Hilbert follows by induction from $K[x_1, ..., x_{n-1}]$ to $K[x_1, ..., x_n]$ via factorization of $K[x_1, ..., x_{n-1}][X_n]$.

We are now motivated to assume that all rings R considered in this exposition are noetherian.

Now we work with the polynomial ring $R = K[X_1, ..., X_n]$ over a field K. We correspond ideals with special subsets of the affine space $\mathbb{A}^n(K)$ which can be identified with K^n forgetting the vector space structure. For a polynomial $f = f[X_1, ..., X_n] \in K[X_1, ..., X_n]$ we denote and define the *zero set* of f in K^n by

$$V(f) = V_K(f) = \{P = (p_1, ..., p_n) \in K^n;\ f(P) = 0\}.$$

More generally, the *zero set of an ideal* $\mathfrak{a}$ is defined as

$$V(\mathfrak{a}) = V_K(\mathfrak{a}) = \{P = (p_1, ..., p_n) \in K^n;\ f(P) = 0\ for\ all\ f \in \mathfrak{a}\}.$$

The zero sets $V(\mathfrak{a})$, $\mathfrak{a}$ ideal in $K[X_1, ..., X_n]$, are called *algebraic subsets* of $K^n = \mathbb{A}^n(K)$. Conversely, we correspond to each subset M of K^n the *vanishing ideal* of M

$$\mathfrak{I}(M) = \mathfrak{I}_K(M) := \{f \in K[X_1, ..., X_n];\ f(m) = 0\ for\ all\ m \in M\}.$$

It is clear that

$$\mathfrak{a} \subseteq \mathfrak{I}(V(\mathfrak{a})), \quad M \subseteq V(\mathfrak{I}(M)).$$

Moreover, for algebraic sets $U, W, V_1, .., V_n$ of K^n and ideals $\mathfrak{a}, \mathfrak{c}, \mathfrak{a}_1, .., \mathfrak{a}_n$ of $K[X_1, .., X_n]$ we notice the following rules:

(0) $U \subseteq WK^n \Rightarrow \mathfrak{I}(U) \supseteq \mathfrak{I}(W)$
$\mathfrak{a} \subseteq \mathfrak{c} \Rightarrow V(\mathfrak{a}) \supseteq V(\mathfrak{c})$
$V(\mathfrak{I}(U)) \subseteq V(\mathfrak{I}(W))$
$\mathfrak{I}(V(\mathfrak{a})) \subseteq \mathfrak{I}(V(\mathfrak{c}))$

(1) $\mathfrak{I}(V_1 \cup .. \cup V_n) = \mathfrak{I}(V_1) \cap .. \cap \mathfrak{I}(V_n)$

(2) $V(\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_n) = V(\mathfrak{a}_1 \cap .. \cap \mathfrak{a}_n) = V(\mathfrak{a}_1) \cup .. \cup V(\mathfrak{a}_n)$

Most interesting is the precise understanding of the correspondence between algebraic sets and vanishing ideals. For this purpose we introduce the *radical* of an ideal $\mathfrak{a}$ of an arbitrary ring setting

$$Rad\ \mathfrak{a} = Rad(\mathfrak{a}) := \{f \in R;\ f^k \in \mathfrak{a}\ for\ a\ suitable\ k \in \mathbb{N}_+\}.$$

This is an ideal of R containing $\mathfrak{a}$. We are motivated to look for the greatest ideal of $K[X_1, ..., X_n]$ containing a given ideal $\mathfrak{a}$ with the same zero locus. The radical is obviously a natural candidate.

In general we notice the following properties:

- $\mathfrak{a} \subseteq Rad(\mathfrak{a})$
- $\mathfrak{a} \subseteq \mathfrak{c} \Rightarrow Rad(\mathfrak{a}) \subseteq Rad(\mathfrak{c})$
- $Rad(\mathfrak{a}) = R \Leftrightarrow \mathfrak{a} = R$
- $Rad(Rad(\mathfrak{a})) = Rad(\mathfrak{a})$
- if $\mathfrak{p}$ is prime, then $Rad(\mathfrak{p}) = \mathfrak{p}$
- $Rad(\mathfrak{a}\mathfrak{c}) = Rad(\mathfrak{a} \cap \mathfrak{c}) = Rad(\mathfrak{a}) \cap Rad(\mathfrak{c})$.
- $Rad\ \mathfrak{a}^m = Rad\ \mathfrak{a}$.
- $Rad(\mathfrak{a} + \mathfrak{c}) = Rad(Rad(\mathfrak{a}) + Rad(\mathfrak{c}))$
- $\mathfrak{a}$, $\mathfrak{c}$ are relatively prime, iff $Rad(\mathfrak{a})$ and $Rad(\mathfrak{c})$ are relatively prime.
- $Rad\ \mathfrak{a} = \bigcap\{prime\ ideals\ of\ R\ containing\ \mathfrak{a}\}$

We present now the basic versions of Hilbert's Nullstellensatz (HN). For three of them one has to assume that $K = \bar{K}$ is an algebraically closed field ($\bar{K}$ denotes the *algebraic closure* of K).

Hilbert's Nullstellensatz 2.3 *(affine versions) The correspondences $\mathfrak{I}, V$ between ideals of $\bar{K}[X] = \bar{K}[X_1, ..., X_n]$ and algebraic sets in $\bar{K}^n$ restrict to the following bijective correspondences:*

(HN.0) $\{points\ of\ \bar{K}^n\} \Leftrightarrow \{maximal\ ideals\ of\ \bar{K}[X]\}$

(HN.1) $\{irreducible\ algebraic\ sets\ of\ \bar{K}^n\} \Leftrightarrow \{prime\ ideals\ of\ \bar{K}[X]\}$

(HN.2) $\{algebraic\ sets\ of\ \bar{K}^n\} \Leftrightarrow \{radical\ ideals\ of\ \bar{K}[X]\}$

By definition, an *irreducible algebraic set* cannot be composed by joining any two smaller algebraic sets. Each algebraic set V is a join of finitely many irreducible algebraic sets. They are uniquely determined by V and called (*irreducible*) *components* of V.

The original version of Hilbert's Nullstellensatz is the following:

(HN) Let K be an arbitrary fileld. Each system $f_1, ..., f_r$ of K-polynomials in n variables, which is not relatively prime, has at least one common zero in $\bar{K}^n$.

A ring is called *factorial* or a *unique factorization domain* (UFD), if each element, which is neither 0 nor a unit, has a unique (up to unit factors and numeration) multiplicative decomposition into prime factors. Our third basic result is the following:

Theorem 2.4 . *For each field K the polynomial ring $K[X_1, ..., X_n]$ is factorial.*

The key of proof is the following implication: if R is factorial, then also the ring $R[T]$ of polynomials in one variable with coefficients in R is. This can be proved by means of the

Gauß-Lemma 2.5 . *If the domauin R is factorial, then for each pair of polynomials $f, g \in R[T]$ it holds that*

$$g.c.d.(coefficients\ of\ f \cdot g) = g.c.d.(coeff.\ of\ f) \cdot g.c.d.(coeff.\ of\ g)$$

holds.

Thereby g.c.d. denotes the greatest common divisor, which is uniquely defined for finitely many elements of the UFD-domain R up to a unit factor.

We want to define the dimension of algebraic manifolds in the most easy and natural manner. For this purpose associate "rings of functions". The *coordinate ring* of $\mathfrak{a} \subset K[X_1, ..., X_n]$ is the residue class ring

$$K[x_1, ..., x_n] = K[X_1, ..., X_n]/\mathfrak{a},\ x_i = X_i\ mod\ \mathfrak{a}.$$

The elements are understood as *polynomial functions* on $V(\mathfrak{a})$. Namely, $f(P) \in K$ for $f \in K[x_1, ..., x_n]$ and $P \in V(\mathfrak{a})$ is defined as $F(P)$, where $F \in K[X_1, ..., X_n]$ is an arbitrary representative of f. Belonging to $\mathfrak{a}$ the difference of two representatives vanishes on $V(\mathfrak{a})$. Therefore the definition of $f(P)$ is correct. The pair

$$\mathfrak{V}_\mathfrak{a} = (V(\mathfrak{a}),\ K[x_1, ..., x_n]),$$

is called *affine algebraic manifold* attached to $\mathfrak{a}$. The residue class ring $K[x_1, ..., x_n]$ is also denoted by $K[\mathfrak{V}]$ (with $\mathfrak{V} = \mathfrak{V}_\mathfrak{a}$) and is called the *coordinate ring* of $\mathfrak{V}$. For prime ideals $\mathfrak{p}$ the coordinate ring is a domain. Its quotient field - denoted by $K(\mathfrak{V})$ - is called the (*algebraic*) *function field* of $K(\mathfrak{V}_\mathfrak{p})$, and $\mathfrak{V}_\mathfrak{p}$ is called the *affine algebraic variety* (attached to $\mathfrak{p}$). There will be no danger

of misunderstandings of notations because $\mathfrak{p}$-adisations will not occur in this paper. Now we have also a more precise definition of the affine spaces $\mathbb{A}^n_K$ as "ringed space" $(V(0) = K^n,\ K[X_1, ..., X_n])$. We write $\mathfrak{V} \subseteq \mathfrak{W}$ iff $\mathfrak{V} = \mathfrak{V}_\mathfrak{a}$, $\mathfrak{W} = \mathfrak{V}_\mathfrak{b}$ and $\mathfrak{a} \supseteq \mathfrak{b}$ interpreting the natural K-algebra homomorphism

$$K[\mathfrak{W}] = K[X_1, ..., X_n]/\mathfrak{b} \longrightarrow K[\mathfrak{V}] = K[X_1, ..., X_n]/\mathfrak{a}$$

as restriction of functions.

In the case of principal ideals we write also $\mathfrak{V}_f$ instead of $\mathfrak{V}_{(f)}$. Sometimes we use also the notation $V_{f_1,...,f_r}$ instead of $V_{(f_1,...,f_r)}$. Now we are flexible. If L is an extension field of K we denote and define the zero set of the K-ideal $\mathfrak{a}$ in L^n by

$$\mathfrak{V}_\mathfrak{a}(L) := \{P = (p_1, ..., p_n) \in L^n;\ f(P) = 0\ for\ all\ f \in \mathfrak{a}\}$$

Definition 2.6 . *The (*polynomial, K-algebra *or shortly $K-$)* Dimension $\mathfrak{Dim}_K\ R = \mathfrak{Dim}_K(R)$ *of a K-algebra R is the maximal natural number n such that R contains the polynomial ring $K[X_1, ..., X_n]$ up to isomorphy of K-algebras - supposed it exists. If it does not exist, then we set the Dimension equal to ∞. We use the capital "D" in Dimension in order to distinguish it from the K-dimension of vector spaces. For each finitely generated K-algebras the Dimension is finite.*

If R is a field, then we call the K-Dimension also the transcendence degree *of R over K. The $K-$*Dimension *of an affine algebraic manifold $\mathfrak{V} = \mathfrak{V}_\mathfrak{a}$ is denoted and defined by*

$$\mathfrak{Dim}_K\ \mathfrak{V} = \mathfrak{Dim}_K(\mathfrak{V}) := \mathfrak{Dim}_K\ K[\mathfrak{V}].$$

With help of some commutative algebra one can prove that

$$\begin{gathered}\mathfrak{V} \subseteq \mathfrak{W} \Rightarrow \mathfrak{Dim}_K(\mathfrak{V}) \leq \mathfrak{Dim}_K(\mathfrak{W});\\ \mathfrak{Dim}_K\ K[X_1, ..., X_n] = \mathfrak{Dim}_K\ K(X_1, ..., X_n) = n = \mathfrak{Dim}_K\ \mathbb{A}^n_K;\\ \mathfrak{Dim}_K(R) = \mathfrak{Dim}_K(Quot\,R) = \ transcendence\ degree\ of Quot\,R\ over\ K,\end{gathered}$$

If R is a K-domain with *quotient field* $Quot\,R := \{r/s;\ 0 \neq s, r \in R\}$, L an algebraic extension field of K contained in R and S is a K-algebra, algebraic over R, then

$$\mathfrak{Dim}_K(R) = \mathfrak{Dim}_L(R) = \mathfrak{Dim}_L(S) = \mathfrak{Dim}_K(S).$$

If L is an arbitrary algebraic extension field of K, then

$$\mathfrak{Dim}_K R = \mathfrak{Dim}_L(R \otimes_K L).$$

If there is no doubt about the basic field K (or $\bar{K}$) we work with, then we write shortly $\mathfrak{Dim}\ R$ or $\mathfrak{Dim}\ \mathfrak{V}$ instead of $\mathfrak{Dim}_K\ R$ or $\mathfrak{Dim}_K\ \mathfrak{V}$, respectively.

Example 2.7 . *The Fermat polynomial $f = X^3 - Y^3 - 1$ has coefficients in each subfield K of the field $\mathbb{C}$ of complex numbers. For $K = \mathbb{Q}$ (rational numbers)*

the algebraic set $V_{\mathbb{Q}}(f) = \{(1,0),(0,1)\}$ consits of two points only, which has naive dimension zero. But the algebraic sets $V_{\mathbb{R}}(f)$, $V_{\mathbb{C}}(f)$ have real dimension 1 or 2, respectively. The latter set is a punctured torus (elliptic curve without ∞) and has complex dimension 1. In the case of rational numbers we come also to dimension 1, if we take the coordinate ring $\mathbb{Q}[x,y] = \mathbb{Q}[X,Y]/(f)$ or the function field $\mathbb{Q}(x,y)$ into consideration. They have $\mathbb{Q}$-Dimension 1. We get the same dimension for $\mathbb{R}[x,y]$ and $\mathbb{C}[x,y]$ over $\mathbb{R}$ in both cases and over $\mathbb{C}$ for the latter one.

After the definition of dimension it is quite natural to ask for calculations. Most cases are not so simple as the above example. Especially, one wants to know when a set of algebraic equations defines an *affine algebraic curve*, which has dimension 1 by definition. Calculation programs for dimensions exist (e.g. CASA, SINGULAR, MACAULEY). We will present now the basic theorems, which one needs for such procedures. First we introduce another "codimension", which looks not so natural at first glance but is o.k. and near to calculations. We give also an idea why both notions of dimension must coincide.

We denote the set of all prime ideals of a ring R by Prim R (the usual notation in higher algebraic geometry is *Spec* R, the *spectrum* of R, Grothendieck). $Prim^* R$ denotes the subset of all prime ideals of R consisting not only of zero divisors. Neglecting zero divisor ideals we denote the set of minimal elements of $Prim^* R$ by $Prim_{min}\, R$. So, *minimal prime ideals* of a domain are the minimal ones among all prime ideals excluding (0). For an ideal $\mathfrak{a}$ of a ring R we introduce also

$$Prim_{min}\, \mathfrak{a} = Prim_{min}(\mathfrak{a}) := \{\textit{minimal elements of } Prim\, R \textit{ containing } \mathfrak{a}\}.$$

Principal Ideal Theorem 2.8 . *Let R be a noetherian domain, The following properties are equivalent:*

(i) $\mathfrak{p}$ *is a minimal prime ideal of* R

(ii) $\mathfrak{p} \in Prim_{min}(f)$ *for a suitable* $0 \neq f \in R \setminus R^*$.

For the factorial ring $R = K[X_1, ..., X_n]$, K algebraically closed, the minimal prime ideals correspond to *irreducible hypersurfaces* of $\mathbb{A}^n_K$. Since $K[X_1, ..., X_n]$ is factorial, the biunivoque correspondence extends - up to K^*-factors - to the set of irreducible polynomials.

Ascending chains of prime ideals have to stagnate by definition of noetherian rings. A deeper result is the following

Proposition-Definition 2.9 . *Each strictly descending chain of prime ideals of a noetherian ring R*

$$\mathfrak{p}_h \supset \mathfrak{p}_{h-1} \supset \mathfrak{p}_{h-2} \supset \ .....$$

terminates after finitely many steps. For each $\mathfrak{p} \in Prim\, R$ there is a maximal number $h(\mathfrak{p})$ of possible descend steps starting from $\mathfrak{p}$. It depends only on $\mathfrak{p}$. This maximal number $h(\mathfrak{p})$ is called the hight *of $\mathfrak{p}$. More generally, we call*

$$h(\mathfrak{a}) := min\{h(\mathfrak{p});\ \mathfrak{p} \in Prim\, R,\ \mathfrak{p} \supseteq \mathfrak{a}\}$$

the hight *of* $\mathfrak{a}$.

The background for the descending property of prime ideals is the

Relative Principal Ideal Theorem 2.10 . *For each ideal* $\mathfrak{a} = (f_1, ..., f_r)$ *of the (noetherian) ring* R *it holds that* $h(\mathfrak{a}) \leq r$.

Theorem 2.11 . *For each proper ideal* $\mathfrak{a}$ *of* R *the set* $Prim_{min}(\mathfrak{a})$ *is finite and*

$$Rad\ \mathfrak{a} = \bigcap Prim_{min}(\mathfrak{a}).$$

With the Relative Principal Theoerem one feels and really can prove that any prime ideal $\mathfrak{p}$ of $K[X_1, ..., X_n]$ contains $h(\mathfrak{p})$ K-algebraically independent elements and not more. Changing to the coordinate ring

$$K[\mathfrak{V}] = K[X_1, ..., X_n]/\mathfrak{p},\ \mathfrak{V} = \mathfrak{V}_{\mathfrak{p}},$$

the elements of $\mathfrak{p}$ are mapped to the zero class. One can prove that the polynomial K-Dimension of $K[\mathfrak{V}]$ is complementary to hight:

Proposition 2.12 . *With the above notations it holds that*

$$h(\mathfrak{p}) + \mathfrak{Dim}_K\ K[\mathfrak{V}_{\mathfrak{p}}] = n.$$

This motivates already to define the *Codimension* of ideals $\mathfrak{a}$ of finitely generated K-algebras R and corresponding affine algebraic manifolds $\mathfrak{V}_{\mathfrak{a}}$ in the case $R = K[X_1, ..., X_n]$ as

$$Codim_K\ \mathfrak{a} := h(\mathfrak{a}) =: Codim_K\ \mathfrak{V}_{\mathfrak{a}}.$$

The above proposition can be generalized to

Theorem 2.13 . *For each ideal* $\mathfrak{a}$ *of a noetherian* K*-algebra it holds that*

$$Codim_K\ \mathfrak{b} + \mathfrak{Dim}_K\ R/\mathfrak{b} = \mathfrak{Dim}_K\ R. \tag{1}$$

In the standard literature one defines the *Krull dimension* of $R/\mathfrak{p}$ as maximal length of ascending prime ideal chains connecting $\mathfrak{p}$ with a maximal ideal. But the relation (1) is not true for all noetherian rings R if one substitutes there our K-Dimension by Krull dimension. When it is true for all (prime) ideals, then R is called a *Cohen-Macauley ring*. For instance, the polynomial rings $K[X] = K[X_1, ..., X_n]$ are Cohen-Macauley. Here is no difference between Krull and polynomial K-Dimension. Cohen-Macauley rings can be also characterized by the property that all maximal prime ideal chains joining two given prime ideals $\mathfrak{p} \subset q$ have the same length.

The hights of prime ideals $\mathfrak{p}$ of $K[X]$, hence the Dimension of $\mathfrak{V}_{\mathfrak{p}}$ can be calculated by means of Hilbert's theory of syzygies. Knowing an ideal basis $f_1, .., f_r$ of $\mathfrak{p}$ one starts with the exact sequence

$$0 \longrightarrow S_1 \longrightarrow K[X]^r \longrightarrow K[X] \longrightarrow K[X]/\mathfrak{p},$$

of noetherian K[X]-modules, where the middle homomorphism sends the canonical basis of $K[X]^r$ to the elements $f_1, ..., f_r$. S_1 is called the *first syzygy module* of the ideal basis. This procedure can be extended in the same manner using (finitely many) generators of S_1. So one gets with $r = r_0$ longer exact sequences

$$0 \to S_d \to K[X]^{r_d} \to K[X]^{r_{d-1}} ..... \to K[X]^{r_0} \to K[X] \to K[X]/\mathfrak{p}$$

We stop, if the d-th *syzygy module* S_d is a free $K[X]$-module. Hilbert proved that the number d exists, is smaller than n and independent of the choices of bases in the modules. Moreover this number coincides with the height $h(\mathfrak{p})$. The heights can be effectively calculated via Groebner bases of ideals and modules. For instance, the computer packages SINGULAR, CASA and MACAULEY work on this line.

Important for us are function fields of algebraic curves. They have a simple structure.

Theorem 2.14 . *The function field of an irreducible curve C in $\mathbb{A}^n_K$ has two generators, if K is either a finite field, an algebraically closed field or a field of characteristic* 0*:*

$$K(C) = K(x, y) = K(x)[y],$$

x transcendental over K, y algebraic over $K(x)$.

So each such curve is "almost" determined by one equation with two variables only: consider the minimal polynomial of y over $K(x)$. This polynomial defines a plane curve. So the theorem has the following

Theorem 2.15 *(Geometric Version). Each irreducible algebraic curve C over a finite field, an algebraically closed field or a field with characteristic* 0 *has a* plane model. *This means that there exists a plane irreducible curve C' with the same function field $K(C) = K(C')$.*

The proof of the theorem joins two basic results of field theory.

Definition 2.16 . *Let L be an algebraic field extension of K. An element $\alpha \in L$ is called* separable *over K, iff the minimal polynomial $p_\alpha(T) \in K[T]$ of α has only simple zeros. L is* separable *over K, iff each element of L is. A field K of characteristic p (inclusively $p = 0$) is called* perfect*, iff each element of K has a p-th root in K.*

It is clear that all fields of characteristic 0, all finite and algebraically closed fields are perfect.

Proposition-Definition 2.17 *(of primitive elements). Each finitely generated separable algebraic field extension L of K can be generated by one element only: $L = K(\alpha)$. Such an element α is called a* primitive *element of the field extension L of K.*

Proposition-Definition 2.18 *(F.K.Schmidt). Each field extension L of a perfect field K of K-Dimension (transcendence degree) r is* separably generated. *This means that there exist r K-algebraically independent elements $x_1, ..., x_r \in L$ such that L is a separable extension of $K(x_1, ..., x_r)$. Each set of such elements is called* separating transcendental basis *of L.*

Taking into account that the function field $C(K)$ of an affine algebraic irreducible curve is finitely generated we have only to summerize the above propositions (and definitions) for proving Theorem 2.14.

Plane irreducible curves (in $\mathbb{A}^2_K$) correspond bijectively (up to a K^*-factor) to irreducible polynomials in two variables with coefficients in K. It is an old problem to ask whether an irreducible curve in $\mathbb{A}^n_K$ can be described by $n-1$ equations. By rather recent research one knows

Theorem 2.19 *(Cowsik-Nori). Assume that the charactristic of $\bar{K}$ is a prime number. Then each affine algebraic curve C over $\bar{K}$ is a (settheoretical) complete intersection. This means that $C(\bar{K})$ is the intersection of (the algebraic sets of) $n-1$ hyperplanes.*

Remark 2.20 . *For fields of characteristic 0 a similar result is only known for connected smooth curves (Ferrand-Szpiro-Mohan Kumar). In general it remains to be an open problem.*

3 Projective Geometry

The n-dimensional projective set $\mathbb{P}^n(K)$ consists of points $(z_0 : z_1 : ... : z_n)$, $z_i \in K$, $i = 0, ..., n$, not all zero simultaneously. Precisely, it is defined as factor set

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{O\})/K^*,$$

where K^* operates multiplicatively on K^{n+1} considered as K-vector space. In the case of complex numbers $\mathbb{P}^n(\mathbb{C})$ has the structure of a connected and compact topological space descending the topology of $\mathbb{C}^{n+1}$ along the quotient map $\mathbb{C}^{n+1} \setminus \{O\} \longrightarrow \mathbb{P}^n(\mathbb{C})$ (factor topology). It has a holomorphic affine $\mathbb{C}^n$-atlas consisting of $n+1$ cards isomorphic to $\mathbb{C}^n$, namely

$$U_i = \{(z_0 : z_1 : ... : z_n) \in \mathbb{C}^{n+1};\ z_i \neq 0\},\ i = 0, ..., n.$$

Especially, one identifies $\mathbb{A}^n(\mathbb{C})$ with U_0 sending $(z_1, ..., z_n)$ to $(1 : z_1 : ... : z_n)$ and consideres $\mathbb{P}^n(\mathbb{C})$ as (algebraic / analytic) compactification of $\mathbb{C}^n$. The same can be done with U_i instead of U_0. The complements are the hyperplanes

$$\mathbb{P}^n(\mathbb{C}) \setminus U_i =: \ H_i : \ Z_i = 0,\ i = 0, ..., n.$$

The set H_0 is also denoted by H_∞ called the *infinite hyperplane*. A polynomial $F(Z_0, ..., Z_n) \in K[Z_0, ..., Z_n]$ is called *homogeneous* of degree d, iff it is a K-linear combination of monomials

$$Z^{\mathfrak{i}} := Z_0^{i_0} \cdot ... \cdot Z_0^{i_n},\ d = i_0 + ... + i_n,$$

of degree d. The topological closures of affine complex manifolds in $\mathbb{C}^n$ are also compactifications. They appear as projective complex manifolds in $\mathbb{P}^n(\mathbb{C})$, which will be defined now. A *projective algebraic set* in $\mathbb{P}^n(K)$ is the zero set of an ideal $\mathfrak{A}$ of $K[Z_0, ..., Z_n]$ generated by homogeneous polynomials. Such ideals are called *homogenoeus ideals*. For algebraically closed fields $\bar{K}$ there is a bijection

$$\begin{array}{c} \{algebraic\, sets\, in\, \bar{K}^n\} \\ \Updownarrow \\ \{proj.\, alg.\, sets\, in\, \mathbb{P}^n(\bar{K})\, without\, irred.\, components\, in H_\infty\} \end{array}$$

where irreducible sets and compononents are defined in obvious analogy to the affine case. The map from below to above is the intersection with $U_0(\bar{K}) = \mathbb{P}^n(\bar{K}) \setminus H_\infty$. We have to explain the map from the upper to the lower set. For this purpose we have to homogenize polynomials in n variables. This is done for arbitrary fields K by the *homogenization map*

$$\begin{aligned} \square^\natural :\ K[Z_1, ..., Z_n] &\longrightarrow K[Z_0, Z_1, ..., Z_n], \\ f \mapsto\ F = f^\natural &:= Z_0^{deg\, f} \cdot f(Z_1/Z_0, ..., Z_n/Z_0). \end{aligned}$$

It is linear, injective, multiplicative (compatible with multiplication of polynomials), degree preserving but not additive and not surjective. The image consists of all homogeneous polynomials of $K[Z_1, Z_0, ..., Z_n]$, which are not divisible

by Z_0. The inverse map sends a homogeneous polynomial $F(Z_0, Z_1, ..., Z_n)$ to ${}^aF = f(Z_1, ..., Z_n) := F(1, Z_1, ..., Z_n)$.

The homogenization map extends to

$$\square^\mathfrak{h} : \{ideals\ of\ K[Z_1, ..., Z_n)]\} \longrightarrow \{homogeneous\ ideals\ of\ K[Z_1, ..., Z_n)]\}$$

corresponding

$$\mathfrak{a} \mapsto \mathfrak{A} = \mathfrak{a}^\mathfrak{h} := (f^\mathfrak{h};\ f \in \mathfrak{a})$$

(the $K[Z_0, Z_1, ..., Z_n)]$-ideal generated by the $f^\mathfrak{h}$'s). Conversely, we define

$${}^a\mathfrak{A} := \{{}^aF = F(1, Z_1, ..., Z_n);\ F \in \mathfrak{A}\}$$

getting ideals in the polynomial ring of n variables. One checks easily the following properties and compatibilites (with obvious notations).

$$\begin{aligned}
(\mathfrak{a} + \mathfrak{b})^\mathfrak{h} &= \mathfrak{a}^\mathfrak{h} + \mathfrak{b}^\mathfrak{h}, \\
(\mathfrak{a}\mathfrak{b})^\mathfrak{h} &= \mathfrak{a}^\mathfrak{h}\mathfrak{b}^\mathfrak{h}, \\
(\mathfrak{a} \cap \mathfrak{b})^\mathfrak{h} &= \mathfrak{a}^\mathfrak{h} \cap \mathfrak{b}^\mathfrak{h}, \\
(Rad\ \mathfrak{a})^\mathfrak{h} &= Rad\ (\mathfrak{a}^\mathfrak{h}), \\
{}^a(\mathfrak{A} + \mathfrak{B}) &= {}^a\mathfrak{A} + {}^a\mathfrak{B}, \\
{}^a(\mathfrak{A}\mathfrak{B}) &= {}^a\mathfrak{A}\,{}^a\mathfrak{B}, \\
{}^a(\mathfrak{A} \cap \mathfrak{B}) &= {}^a\mathfrak{A} \cap {}^a\mathfrak{B}, \\
{}^a(Rad\ \mathfrak{A}) &= Rad\ {}^a\mathfrak{A}, \\
{}^a(\mathfrak{a}^\mathfrak{h}) &= \mathfrak{a}, \\
\mathfrak{p}\ is\ prime\ iff\ \mathfrak{p}^\mathfrak{h}\ is.&
\end{aligned}$$

A basic motivation for the introduction of projective spaces is the following theorem, which can be proved by means of the Relative Principal Ideal Theorem.

Theorem 3.1 . *Each system of homogeneous polynomials*

$$F_1, ..., F_n \in K[Z_0, Z_1, ..., Z_n]$$

has at least one zero in $\mathbb{P}^n(\bar{K})$.

This means geometrically that the intersection of n hypersurfaces in $\mathbb{P}^n(\bar{K})$ is not void. For instance, the intersection of two different plane projective K-lines consists of a point in $\mathbb{P}^2(K)$. This was a historical starting point.

Essential homogeneous ideals of $K[Z_0, Z_1, ..., Z_n]$ are precisely those whose radicals are different from the maximal homogeneous ideal $\mathfrak{M}_0 = (Z_0, Z_1, ..., Z_n)$. In analogy to the affine geometry the zero set correspondence

$$\begin{gathered}
\{essential\ homogeneous\ radical\ ideals\ of\ \bar{K}[Z_0, Z_1, ..., Z_n]\} \\
\Updownarrow \\
\{(non-void)\ projective\ algebraic\ sets\ in\ \mathbb{P}^n(\bar{K})\}
\end{gathered}$$

sending $\mathfrak{A}$ to

$$V(\mathfrak{A}) = \{(z_0 : z_1 : ... : z_n) \in \mathbb{P}^n(\bar{K});\ F(z_0, z_1, ..., z_n) = 0\ for\ all\ F \in \mathfrak{A}\},$$

is bijective.

Now we intersect the a projective algebraic set $V = V(\mathfrak{A})$ with K^n. Then we get an affine algebraic set denoted by ${}^aV$, namely

$$V(\mathfrak{A}) \cap K^n = {}^aV(\mathfrak{A}) = V(\mathfrak{A}) \setminus H_\infty = V({}^a\mathfrak{A}).$$

The affine algebraic set ${}^aV(\mathfrak{A})$ coincides with ${}^aV(\mathfrak{B})$ if and only if $V(\mathfrak{A})$ and $V(\mathfrak{B})$ coincide up to components lying in the infinite hyperplane. Conversely, we send affine algebraic sets $V_0 = \mathfrak{I}(\mathfrak{a})$ to the projective ones $(V_0)^\mathfrak{h} := V(\mathfrak{a}^\mathfrak{h}) \subseteq \mathbb{P}^n(K)$. With obvious notations the following relations are immediate:

$$\begin{aligned} {}^a\mathfrak{I}(V) &= \mathfrak{I}({}^aV), \\ (\mathfrak{I}(V_0))^\mathfrak{h} &= \mathfrak{I}((V_0)^\mathfrak{h}), \\ V({}^a\mathfrak{A}) &= {}^aV(\mathfrak{A}), \\ V(\mathfrak{a}^\mathfrak{h}) &= V(\mathfrak{a})^\mathfrak{h}. \end{aligned}$$

In the case of algebraic closed fields we get a bijective correspondence between affine algebraic sets in $\bar{K}^n$ and projective algebraic sets in $\mathbb{P}^n(\bar{K})$ without components in H_∞.

In both spaces K^n and $\mathbb{P}^n(K)$ there is a *Zariski topology* defined by complements of all algebraic sets as a topology basis of open sets. In this topology the projective algebraic sets $V(\mathfrak{a}^\mathfrak{h})$ is the closure of $V_0(\mathfrak{a}) := V(\mathfrak{a}) \subseteq K^n$ in $\mathbb{P}^n(K)$. Thanks to Hilbert's Nullstellensatz the correspondence $V_0 \mapsto V = (V_0)^\mathfrak{h}$ does not depend on the choice of the vanishing ideal $\mathfrak{a}$ of V_0, if K is algebraically closed. If K is the field of complex numbers, then V is also the topological closure of V_0 in $\mathbb{P}^n(\mathbb{C})$, which is also regarded as a complex compactification.

For essential homogeneous ideals $\mathfrak{A} \subset K[Z_0, ..., Z_n]$ we define the attached *projective manifold* in analogy to affine geometry as pair

$$\mathfrak{V}_\mathfrak{A} = (V(\mathfrak{A}),\ K[\mathfrak{V}(\mathfrak{A})])$$

of a projective algebraic set and a coordinate ring. The *coordinate ring* is defined as $K[\mathfrak{V}_\mathfrak{A}] = K[Z_0, Z_1, ..., Z_n]/\mathfrak{A}$. A *projective* (*algebraic*) *variety* (defined) *over* K is a projective manifold $\mathfrak{V}_\mathfrak{P}$, which belongs to an essential homogeneous prime ideal $\mathfrak{P}$ of $K[Z_0, ..., Z_n]$.

We write $\mathfrak{V} \subseteq \mathfrak{W}$, if $\mathfrak{V} = \mathfrak{V}_\mathfrak{A}$, $\mathfrak{W} = \mathfrak{V}_\mathfrak{B}$ and $\mathfrak{A} \supseteq \mathfrak{B}$. The projective space $\mathbb{P}^n_K$ is defined to be $\mathfrak{V}_0 = \mathfrak{V}_{(0)}$, (0) the zero ideal of $K[Z_0, ..., Z_n]$. The projective algebraic L-sets of $\mathfrak{V} = \mathfrak{V}_\mathfrak{A}$, L a field extension of K, is written and defined as

$$\mathfrak{V}(L) = \{P = (p_0 : ... : p_n) \in \mathbb{P}^n(L);\ F(P) = 0\ for\ all\ homogeneous\ F \in \mathfrak{A}\}.$$

The *projective dimension* of $\mathfrak{V}$ is defined to be equal to

$$Dim^\mathfrak{h}_K(K[\mathfrak{V}]) := -1 + Dim_K(K[\mathfrak{V}]).$$

The reason for the -1-shift is the following: For proper ideals $\mathfrak{a}$ of $K[Z_1, ..., Z_n]$ it holds that

$$Dim_K^{\mathfrak{h}} K[\mathfrak{a}^{\mathfrak{h}}] = Dim_K K[\mathfrak{a}] = Dim\, \mathfrak{V}_{\mathfrak{a}} = Dim\, \mathfrak{V}_{\mathfrak{a}^{\mathfrak{h}}}.$$

In geometric words, the projective closure applied to affine manifolds is dimension preserving as it should be. For algebraically closed fields we notice the following

Hilbert's Nullstellensatz 3.2 *(projective version). The zero set correspondence between ideals of $\bar{K}[Z_0, Z_1, ..., Z_n]$ and projective algebraic sets in $\mathbb{P}^n(\bar{K})$ restricts to bijective correspondences*

(HN.0)$^{\mathfrak{h}}$ $\{$*points of* $\mathbb{P}^n(\bar{K})\}$
$\Updownarrow$
$\{$*maximal essential homogenous ideals of* $\bar{K}[Z_0, Z_1, ..., Z_n]\}$

(HN.1)$^{\mathfrak{h}}$ $\{$*irreducible algebraic sets in* $\mathbb{P}^n(\bar{K})\}$
$\Updownarrow$
$\{$*essential homogenous prime ideals of* $\bar{K}[Z_0, Z_1, ..., Z_n]\}$

(HN.2)$^{\mathfrak{h}}$ $\{$*projective algebraic sets in* $\mathbb{P}^n(\bar{K})\}$
$\Updownarrow$
$\{$*essential homogeneous radical ideals* $\in \bar{K}[Z_0, Z_1, ..., Z_n]\}$

The most classical version is

(HN)$^{\mathfrak{h}}$ Each essential homogeneous ideal of $K[Z_0, Z_1, ..., Z_n]$, has at least one common zero in $\mathbb{P}^n(\bar{K})$.

4 Singularities

Now we are able to define and describe the singularities of a projective manifolds. We start with hypersurfaces. Let F be a homogeneous polynomial in $K[Z_0,...,Z_n]$ of degree $d>0$. We say that $P \in \mathbb{P}^n(K)$ is a *singularity* of $\mathfrak{V}_F$, iff the *homogeneous gradient* (or *Jacobian*) of F

$$(\partial F/\partial Z) = (\partial F/\partial(Z_0,...,Z_n)) := (\partial F/\partial Z_0,....,\partial F/\partial Z_n),$$

consisting of $n+1$ polynomials, vanishes at P. At least in characteristic 0 the point P really belongs to $V(F)$, if the *singularity condition*

$$(\partial F/\partial(Z_0,...,Z_n))(P) = 0.$$

is satisfied. This follows from the *Euler Identity*

$$Z_0\partial F/\partial Z_0 + Z_1\partial F/\partial Z_1 + ... + Z_n\partial F/\partial Z_n = d\cdot F,$$

which can be easily proved starting with monomials. If $F = f^\mathfrak{h}$ is the homogenization of $f \in K[Z_1,...,Z_n]$ and $P = (1 : p_1 : ... : p_n) = (p_1,...,p_n) \in \mathfrak{V}_f(K)$, then it holds that P is a *singularity* of $\mathfrak{V}_f$ if and only if the (affine) gradient (or Jacobian) of f

$$grad\, f := (\partial f/\partial(Z_1,...,Z_n)) = (\partial F/\partial Z_1,....,\partial F/\partial Z_n)$$

vanishes together with f at P. So the affine singularities are described by the $n+1$ equations

$$\partial f/\partial Z_1 = ... = \partial f/\partial Z_n = 0 = f(Z_1,...,Z_n).$$

The gradient and homogenizing operations are almost commuting (up to Z_0-power factors at monomials). With this knowledge it is easy to check that the affine set of K-singularities of $\mathfrak{V}_f$ coincides with affine part of the projective set of K-singularities of $\mathfrak{V}_F$. With the notations

$$Sing\,\mathfrak{V}_F = \mathfrak{V}_{\partial F/\partial(Z_0,...,Z_n)} \subset \mathbb{P}^n_K,$$
$$Sing\,\mathfrak{V}_f = \mathfrak{V}_f \cap \mathfrak{V}_{\partial f/\partial(Z_1,...,Z_n)} \subset \mathbb{A}^n_K$$

this means that the *singular loci* are related by

$$(Sing\,\mathfrak{V}_f)(L) = \mathbb{A}^n(L) \cap (Sing\,\mathfrak{V}_F)(L),$$

where L is any extension field of K.

For $P = (p_1,...,p_n) \in \mathbb{A}^n(K)$ we define the *cotangent space* of $\mathbb{A}^n$ at P as space of linear functions vanishing at P, precisely:

$$T^*_P(\mathbb{A}^n_K) : := K\cdot(Z_1 - p_1) + ... + K\cdot(Z_n - p_n)$$

We have a natural coordinate map $\kappa : T^*_P \longrightarrow K^n$, $(Z_i - p_i) \mapsto (0,...,1,...,0)$. The *tangent space* $T_P(\mathbb{A}^n_K)$ is the dual of the K-vector space $T^*_P(\mathbb{A}^n_K)$. The

composition of the gradient map, substitution of point P and inverse of the coordinate map

$$d_P : K[Z] \longrightarrow K[Z]^n \longrightarrow K^n \longrightarrow T_P^*$$

sends $f(Z_1, ..., Z_n)$ to the linear polynomial

$$d_P f := \sum (Z_i - p_i)\partial f/\partial Z_i(P) = < \overrightarrow{PZ}, grad_P(f) >$$

called the *differential* of f at P. The following properties are easy to check:

$$d_P(f+g) = d_P f + d_P g,\ d_P(fg) = g(P)d_P f + f(P)d_P g.$$

The equation $d_P f = 0$ describes the *tangent hyperplane* $T_P(\mathfrak{V}_f)$ of $\mathfrak{V}_f$ at P, if P is not a singular point (remember to gradient properties in analysis).

These considerations can be extended from hypersurfaces to complete intersections of Dimension $n - r$

$$\mathfrak{V}_\mathfrak{f} = \mathfrak{V}_{(f_1,...,f_r)} :\ f_1 = ... = f_r = 0,\ \mathfrak{f} = (f_1, ..., f_r) \in K[Z_1, ..., Z_n]^r.$$

$P \in \mathfrak{V}_\mathfrak{f}(K)$ is a *singular* K-point of this manifold, iff the rank of the *Jacobian matrix* $(\partial\mathfrak{f}/\partial Z) = (\partial f_i/\partial Z_j)$ is smaller than r. Non-singular points are called *regular points*. $\mathfrak{V}_\mathfrak{f}$ is called K-smooth iff it has no singular K-points. It is called (absolutely) *smooth* iff there is no singular $\bar{K}$-point on it. Since the singular points are defined by finitely many algebraic equations depending only on the defining equations of a manifold we receive

Theorem 4.1 . *The singular locus Sing* $\mathfrak{V}$ *is a closed algebraic subvariety of* $\mathfrak{V} = \mathfrak{V}_\mathfrak{f}$.

If P is a regular point of $\mathfrak{V}_\mathfrak{f}(K)$, then the tangent space over K of $\mathfrak{V}_\mathfrak{f}$ at P is defined by a linear system of equations:

$$T_P(\mathfrak{V}_\mathfrak{f}) :\ (\partial(f_1, ...f_r)/\partial(Z_1, ..., Z_n))(P) \cdot^t (Z_1 - p_1, ..., Z_n - p_n) = 0.$$

Let $\mathfrak{V}$ be an affine K-variety, P a K-point on it. The local ring $\mathcal{O}_P$ of $\mathfrak{V}$ at P is the subring of the function field

$$\mathcal{O}_P = \mathcal{O}_{P,\mathfrak{V}} = \{f/g; f, g \in K[\mathfrak{V}],\ g(P) \neq 0\} \subseteq K(\mathfrak{V}).$$

A ring R is called *local*, iff it has a unique maximal ideal. The unique maximal ideal of $\mathcal{O}_P$ is

$$\mathfrak{m}_P = \mathfrak{m}_{P,\mathfrak{V}} = \{f/g; f, g \in K[\mathfrak{V}],\ g(P) \neq 0,\ f(P) = 0\},$$

which is the complement in $\mathcal{O}_P$ of the group $\mathcal{O}_P^*$ of units of $\mathcal{O}_P$. The differential map d_P can be extended from $K[Z] = K[Z_1, ...Z_n]$ to $D_P : \mathcal{O}_P \longrightarrow \mathcal{O}_P$ setting

$$D_P(f/g) := (g(P) \cdot d_P(f) + f(P) \cdot d_P(g))/g^2.$$

Obviously, D_P restricts to the powers

$$D_P : \mathfrak{m}_P^k \longrightarrow \mathfrak{m}_P^k$$

of $\mathfrak{m}_P$ for each $k \in \mathbb{N}$. The *residue field* $\mathfrak{k}_P := \mathcal{O}_P/\mathfrak{m}_P$ containing K acts on the residue modules $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ in obvious manner. As noetherian $\mathfrak{k}_P$- and K-modules they are are finite-dimensional K-vector spaces. If $K = \bar{K}$ is algebraically closed, the residue field $\mathfrak{k}_P$ coincides with $\bar{K}$ because it is finitely generated, hence algebraic over K.

Theorem 4.2 . *If P is a regular point of the $\bar{K}$-algebraic (complete intersection) variety $\mathfrak{V}$, then D_P induces an isomorphism*

$$\delta_P : \mathfrak{m}_P/\mathfrak{m}_P^2 \xrightarrow{\sim} T_P^*(\mathfrak{V}).$$

That's the reason why the cotangent space can be identified with $\mathfrak{m}_P/\mathfrak{m}_P^2$ at regular $\bar{K}$-points. So one defines for all algebraic manifolds at regular points

$$T_P^*(\mathfrak{V}) = \mathfrak{m}_P/\mathfrak{m}_P^2,\ T_P(\mathfrak{V}) = (\mathfrak{m}_P/\mathfrak{m}_P^2)^*.$$

Regular points of arbitrary algebraic variety V over $\bar{K}$ are defined now by the conditioin $dim_{\bar{K}}(\mathfrak{m}_P/\mathfrak{m}_P^2) = \mathfrak{Dim}\, V$. Moreover one has the following general regularity criterion.

Theorem 4.3 . *A point P of the algebraic $\bar{K}$-variety $\mathfrak{V}$ is regular, if and only if the maximal ideal $\mathfrak{m}_P$ of the local ring $\mathcal{O}_P$ has an ideal basis $t_1, ..., t_d$ of length $d = Dim\, \mathfrak{V}$. Such an ideal basis is called a* regular system of parameters *(of $\mathfrak{V}$ at$P$).*

More generally, for a local domain $(R, \mathfrak{m})$ with residue class field $\mathfrak{k} = R/\mathfrak{m}$ a *regular system of parameters* is defined as ideal baisis of $\mathfrak{m}$ of length $dim_{\mathfrak{k}}(\mathfrak{m}/\mathfrak{m}^2)$. A local ring which has a regular system of parameters is called a *regular local ring.*

Theorem 4.4 . *Each regular local domain is a unique factorization domain. Especially, it is a normal domain.*

Thereby we call a domain R *normal*, iff it coincides with its normale closure in its quotient field. The *normal* or *integral closure* of R in a field L containing R is defined by

$$L \cap \{zeros\, of\, normalized\, polynomials\, of\, R[T]\},$$

where a *normalized polynomial* has highest coefficient 1, by definition.

5 Algebraic Curves

For local rings at points of algebraic curves there is no difference between normality and regularity. Namely, it is not difficult to prove the following useful

Theorem 5.1 . *Let R be a local K-domain with maximal ideal $\mathfrak{m} \neq (0)$. Then the following properties are equivalent:*

(i) $\mathfrak{m}$ *is a principal ideal;*

(ii) R *is a principal domain;*

(iii) R *is factorial of K-Dimension* 1*;*

(iv) R *is normal of K-Dimension* 1*;*

(v) R *is a* discrete valuation ring*;*

(vi) R *is regular of K-Dimension* 1*.*

Property (v) means that the quotient field Q of R has a (surjective) *discrete valuation* $v : Q \longrightarrow \mathbb{Z} \cup \infty$, which is defined by the following properties:

(0) $v(r) = \infty \Leftrightarrow r = 0$,

(1) $v(r \cdot s) = v(r) + v(s)$,

(2) $v(r + s) \geq min\,\{v(r), v(s)\}$,

for all $r, s \in Q$. The valuation comes from the multiplicative extension of the correspondence $t \mapsto 1$, where t is an arbitrary local parameter (generating $\mathfrak{m}$). From the valuation v one gets back R, R^* and $\mathfrak{m}$ as $v^{-1}(\mathbb{N} \cup \infty)$, $v^{-1}(0)$ or $v^{-1}(\mathbb{N}_+ \cup \infty)$, respectively.

Proposition 5.2 . *The point P of an irreducible algebraic curve C is regular if and only if $\mathcal{O}_P$ is normal. Almost all local rings $\mathcal{O}_P$, $P \in C(\bar{K})$ are normal.*

"Almost all" means (for curves): up to finitele many points.

Theorem 5.3 . *For (absolutely) smooth projective curves C over an algebraically closed field $\bar{K}$ there is a bijective correspondence*

$$C(\bar{K}) \Leftrightarrow \textit{discrete valuation rings of the function field } \bar{K}(C).$$

It corresponds P to the local ring $\mathcal{O}_P$. The corresponding valuations are denoted by v_P. For $f \in \bar{K}(C)$ the number $v_P(f) \in \mathbb{Z} \cup \infty$ is called the *zero order* of f at P and

$$-v_P(f) = v_P(1/f),\ f \neq 0,$$

is the *pole order* of f at P.

Assume that $K = \bar{K}$ is algebraically closed. For singular points P of hypersurfaces $V = V_f \subset \mathbb{A}^n_K$ we look for a measure of deviation from regularity. Without loss of generality we assume that $P = O \in V(K)$ is the zero point. We define first the *contact order* at O of V and the line $L = L_{\mathfrak{a}} = K\mathfrak{a}$, $\mathfrak{o} \neq \mathfrak{a} \in K^n$, as the zero order $v_O(f(t\mathfrak{a})) > 0$ of the polynomial $f(t\mathfrak{a}) \in K[t]$ at O. If this order is equal to 1 then O must be a regular point of V and L *crosses* V at O. So it is natural to define the *multiplicity* of V at O as

$$\mu_O(V) := min\,\{v_O(f(t\mathfrak{a}));\ L = K\mathfrak{a}\ line\ through\ O\}.$$

A line $T = K\mathfrak{a}$ with $v_O(f(t\mathfrak{a})) > \mu_O(V)$ is called a *tangent line* of V at O.

Plane Curve Examples 5.4 *: The curves* $Y^2 - X^2(X+1) = 0$ *and* $Y^2 - X^3 = 0$ *have multiplicity* 2 *respectively* 3 *at* O. *In the first case the singularity* O *is a* double point. *Singularities of multiplicity* 3 *are* triple *points. In the first case there are two curve branches at* O, *each of them has a tangent line, crossing each other at* O. *In the latter case there is only one tangent. Triple points of this kind are called* cusps. *There is also the possibility of triple points with three different crossing branch tangents. Take for example the curve with equation* $Y^4 - Y^3 + X^2Y + X^4 = 0$.

Above we defined *multiplicities* of *hypersurface singularities* because V_f is a hypersurface in $\mathbb{A}^n_K$. Especially for $n = 2$, we are able to calculate *multiplicities* of *plane curve singularities* as demonstrated in the above examples. We would like to determine also singualirity multiplicities of curves in $\mathbb{A}^n \subset \mathbb{P}^n$. This can be done more generally for varieties V_f, $f = (f_1, ..., f_r) \in K[Z_1, ...Z_n]^r$. Knowing the complications for the general definition with acceptable qualities, I make only a step in this direction:

Definition 5.5 . *The* contact order *of* V_f *and* $L_{\mathfrak{a}}$ *at* $O \in V_f(K)$ *is the zero order* $v_0(P)$ *at* 0 *of the greatest common divisor polynomial*

$$P(t) = g.c.d._{K[t]}(f_1(t\mathfrak{a}), ..., f_r(t\mathfrak{a}).$$

We would like to resolve curve singularities. The purely algebraic way is the normalization. Let C be an irreducible curve. The affine coordinate ring is not normal in general. But there are only finitely many local rings $\mathcal{O}_P$ which fail to be normal, see Proposition 5.2. These are the singularities. A local global principle of algebra applied to our situation yields

Proposition 5.6 . *The coordinate ring K[C] is normal if and only if all local rings* $\mathcal{O}_P$ *in* $K(C)$ *are normal.*

So , the normal closure $\widetilde{K[C]}$ of $K[C]$ in the function field $K(C)$ is a ring which has only regular local rings. Moreover, it is a finitely generated $K[C]$-module and therefore a finitely generated K-algebra. Looking at the ideal defined by

relations of generators we see that $\widetilde{K[C]}$ is the coordinate ring of the curve $\tilde{C}$ defined by this ideal. The function fields of C and $\tilde{C}$ are the same. So we get a *smooth model* $\tilde{C}$ of C together with a map

$$\tilde{C} \longrightarrow C,\ \tilde{P} \mapsto P \tag{2}$$

sending discrete valuation rings $\mathcal{O}_{\tilde{P}}$ of $K[\tilde{C}] = \widetilde{K[C]}$ to its intersection $\mathcal{O}_P := K[C] \cap \mathcal{O}_{\tilde{P}}$. This map (2) is called the singularity resolution of C. We presented this algebraic procedure of singularity resolution only for affine curves. But it extends to projective curves via finitely many affine cards. We remember to Theorem 5.3 to see that in the case of algebraically closed field $K = \bar{K}$ we resolved all singularities of a given projective irreducible curve. The normalization method leads to a proof of

Theorem 5.7 . *Each irreducible projective curve over an algebraically closed field has a unique smooth projective model together with a unique singularity resolution map (2). Each two projective curve models of the same function field have, up to isomorphy, the same smooth model.*

We want to resolve singularities in a more constructive and more visible geometric manner in the case of plane curves. Since each irreducible curve has a plane model by Theorem 2.15 this is most important. We will explain now the σ-process at the point O of the affine plane $\mathbb{A}^2$. Geometrically, O will be substituted by the space of all tangent lines through O, which is a (projective) line itself. This procedure has an algebraic realization as surface S in

$$\mathbb{A}^2 \times \mathbb{P}^1 = (\mathbb{A}^2 \times U_0) \cup (\mathbb{A}^2 \times U_1), \quad U_i :\ t_i \neq 0,\ i = 1, 2$$

defined by the equation $T_0 Y = T_1 X$. Substitute t_1 by t and t_0 by s. Then

$$S = \{(x, y, (s : t)) \in \mathbb{A}^2 \times \mathbb{P}^1,\ sy = tx\}.$$

Outside of $O \times \mathbb{P}^1$ the points of S are uniquely determined by the $\mathbb{A}^2$-coordinates $(x, y) \neq (0, 0)$. This is understood as an (algebraic) isomorphism

$$S \setminus O \times \mathbb{P}^1 \xrightarrow{\sim} \mathbb{A}^2 \setminus O$$

restricting the natural surjective algebraic projection

$$\sigma :\ S \longrightarrow \mathbb{A}^2, \quad (x, y, (t_0 : t_1)) \mapsto (x, y)$$

with the *exceptional line* $\sigma^{-1}(O) =: L \cong \mathbb{P}^1$. It is clear that the tangents through O represented by $(x : y)$ correspond to the point on $L \subset S$ with the coordinate $(s : t) = (x : y)$ because of $sy = tx$.

The procedure is local. It can be easily defined at any regular point P of a projective algebraic surface X. The corresponding σ-process $\sigma_P :\ S \longrightarrow X$ is also called the *blowing up* of the point P of X or of X at P, and S is the *blown up surface*. It is a projective surface again. *Examples.* The plane curve

$C : Y^2 - X^2(X+1) = 0$ has a double point O. The two curve branches through O are separated after blowing up this point. Namely, look at the pair of crossing tangent lines of the branches. They represent and appear as two different points on the exceptional line $L = \sigma^{-1}(O)$. This means that the branches cross the exceptional line at these points. The singularity is resolved. For cusps as represented by the point O of the curve $C : Y^2 - X^3 = 0$ one needs also one σ-processes to resolve the singularity. In this case the exceptional line appears as tangent of the transformed curve.

Theorem 5.8 . *Let C be a plane projective curve over an algebraically closed field $\bar{K}$ of characteristic 0. There exist finitely many σ-processes at curve singularities such that the properly transformed curve $\tilde{C}$ is smooth.*

The proof needs divisors on smooth projective surfaces X and intersection indices of them. *Divisors* $D = \sum k_i C_i$ on X are $\mathbb{Z}$- linear combinations of irreducible (projective) curves C_i on X called (prime) *components* of D (assume $k_i \neq 0$). They form an additive group denoted by $Div\, X$. *Effective divisors* are those with only positive coefficients. The additive subsemigroup of all of them is denoted by $Div^+ X$. *Prime divisors* are the irreducible curves endowed with coefficient 1. The *support* of the divisor D is the algebraic set $\bigcup C_i$. On a suitable neighbourhood of any point $P \in X(\bar{K})$ each effective divisor is described by a *local equation* $f = 0$, $f = f_P \in \mathcal{O}_{P,X}$. In this equation f is uniquely determined up to a unit of the local ring $\mathcal{O}_{P,X}$ because it is factorial. The relation $f(P) = 0$ means that f belongs to the maximal ideal $\mathfrak{m}_{P,X}$ of the local ring. Now let D, E be two effective divisors intersecting each other properly at P, that means their supports do so. The local equations of D, E at P are $f = 0$ respectively $g = 0$. Then the ideal (f, g) in $\mathcal{O}_P$ is contained in $\mathfrak{m} = \mathfrak{m}_{P,X}$. One can prove that the residue class module $\mathfrak{m}/(f, g)$ is a finite dimensional $\bar{K} = \mathcal{O}_P/\mathfrak{m}_P$-vector space. The *intersection index* of D, E at P is denoted and defined by

$$(D \cdot E)_P := dim_{\bar{K}}\, \mathcal{O}_{P,X}/(f_P, g_P).$$

The definition extends to effective divisors D (and E) not going through P taking a unit f_P of $\mathcal{O}_P$ instead of $\mathfrak{m}_P$. Then the local intersection index at P is 0. It is easy to see that the intersection index is symmetric and biadditive whenever defined. We globalize the intersection index setting

$$(D \cdot E) = \sum_{P \in C} (D \cdot E)_P.$$

This definition is correct if E, D have no common prime component because in this case there exists only a finite number of intersection points. For a generalization to all divisors we firstly introduce principal divisors. Let $0 \neq f$ be an element of the quotient field $\bar{K}(X)$. It has a unique factorization

$$f = \frac{p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}}{q_1^{l_1} \cdot \ldots \cdot q_s^{l_s}}$$

in prime factors of $\mathcal{O}_P$ for each point P of our smooth surface X. The prime factors define prime divisors $C_i : p_i = 0$ and $C'_j : q_j = 0$. Around P, say on a Zariski-open set U, this decomposition defines a local principal divisor

$$(f_U) := k_1C_1 + ... + k_rC_r - (l_1C'_1 + ... + l_sC'_s).$$

Outside of U there are only finitely many closed irreducible curves. We have to add these, along which f vanishes and to subtract those along which f has a pole, each with the correct multiplicity coming from prime factorizations as above. At the end we get with obvious notations a (global) *principal* divisor

$$(f) = \sum_C v_C(f) \cdot C.$$

It holds that $(f \cdot g) = (f) + (g)$ for any two principal divisors. The principal divisors form a subgroup $\mathfrak{P}_X$ of $Div\, X$. The residue class group

$$PicX := Div\, X/\mathfrak{P}_X$$

is called the *divisor class* or *Picard group* of X. We write $D \equiv E$ iff D and E belong to the same divisor class and call D and E *linearly equivalent.*

Proposition 5.9 . *The intersection index $((f), D)$ with a principal divisor (f) vanishes, whenever defined.*

Moving Lemma 5.10 . *For two prime divisors C, D there exists a divisor $E \equiv D$ avoiding the given curves C as component.*

On this way one can define correctly $(C \cdot D)$ as $(C \cdot E)$. Especially selfintersections (C^2) are defined now. By $\mathbb{Z}$-linear extension the intersection pairing

$$(\quad , \quad) : Div(X) \times Div(X) \longrightarrow Pic(X) \times Pic(X) \longrightarrow \mathbb{Z}.$$

is well-defined.

We come back now to the σ-processes $\sigma = \sigma_P : S \longrightarrow X$ with exceptional line $L = \sigma^{-1}(P)$, wishing to understand why singularities can be resolved by them. For $D \in Div^+X$ we denote by $\sigma^*(D)$ the divisor on S which has the same local equations on $\sigma^{-1}(U)$ as D has on U, for any set of small Zariski-open sets U covering X. The *inverse image map* σ^* restricts to $\mathfrak{P}_X \longrightarrow \mathfrak{P}_S$. Together we get group homomorphisms

$$\sigma^* : Div\, X \longrightarrow Div\, S, \quad Pic\, X \longrightarrow Pic\, S.$$

For the intersection indices it holds that

$$(\sigma^*(D) \cdot \sigma^*(E)) = (D \cdot E),\ D,\ E \in Div\, X.$$

The *proper (pre-) image* $C' = \sigma'(C)$ on S of an irreducible curve C on X is defined to be the closure of $\sigma_P^{-1}(C \setminus \{P\})$ on S. The definition extends $\mathbb{Z}$-linearly to

$$\sigma' : Div\, X \longrightarrow Div\, S.$$

For a curve C with multiplicity $k = \mu_P(C)$ at P it holds that

$$\sigma^*(C) = \sigma'(C) + k \cdot L, \quad (\sigma'(C) \cdot L) = k.$$

The singularity P of C splits into intersection points of C' with L and the sum of multiplicities of these points is smaller than $\mu_P(C)$. For instance, if P is an ordinary singularity, then all intersection points of C' and L are regular points of C'. One can prove also

$$(\sigma'(C_1) \cdot \sigma'(C_2)) = (C_1 \cdot C_2) - k_1 k_2, \quad k_i = \mu_P(C_i),$$

especially

$$(C'^2) = (\sigma'(C), \sigma'(C)) = (C^2) - k^2.$$

6 Riemann Surfaces

A *Riemann surface* X is a reell two-dimensional connected smooth manifold with a holomorphic complex structure. This means: there is an atlas consisting of (at most countable many open) cards (homeomorphisms) $X \supseteq U \xrightarrow{\sim} V \subseteq \mathbb{C}$ such that any pair of cards U_1, U_2 is connected by biholomorphic transformations over the intersection $U_1 \cap U_2$. Most interesting for us are compact Riemann surfaces. An example is the *complex torus* defined as coset space $\mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice in $\mathbb{C}$, inheriting the complex structure of $\mathbb{C}$ in obvious manner. The following theorem presents us all smooth complex projective curves as compact Riemann surfaces.

Connectedness Theorem 6.1 . *Each complex affine or projective algebraic variety is connected in the complex topology.*

Notice that the analogeous statement for real algebraic varieties is wrong even in the case of plane curves. For example the set $E(\mathbb{R}) \subset \mathbb{A}^2(\mathbb{R})$ of real points of the elliptic curve $E: Y^2 = X^3 - X$ splits into two connected components, one of them is an oval. Things are complicated for real plane curves in general. Hilbert's 16-th problem is dedecated to them.

Holomorphic maps $X \longrightarrow Y$ of Riemann surfaces X, Y are defined locally via cards of suitable atlasses in obvious manner. The holomorphic maps $X \longrightarrow \mathbb{P}^1$ form a field, the field $\mathfrak{M}(X)$ of *meromorphic functions* of X. For an irreducible smooth complex projective curve C the function field $\mathbb{C}(C)$ coincides with $\mathfrak{M}(C)$. For instance,

$$\mathfrak{M}(\mathbb{P}^1) = \mathbb{C}(\mathbb{P}^1) \cong \mathbb{C}(Z) = Quot\,\mathbb{C}[Z]$$

is the field of complex rational functions. The ring of holomorphic functions on $U \subseteq X$ is denoted by $\mathcal{O}(U)$. Meromorphic functions on U are the elements of the quotient field $\mathfrak{M}(U) = Quot\,\mathcal{O}(U)$. In contrast to the compact (projective) case there are holomorphic functions which are not rational, e.g. the exponential function on $\mathbb{C}$. From elementary function theory one knows

Discreteness Theorem 6.2 . *The set of zeros of a holomorphic function on a Riemann surface is discrete.*

Maximum Theorem 6.3 . *If a holomorphic map $f: U \longrightarrow \mathbb{C}$ has an absolute maximum inside of the Riemann surface U, then f is constant.*

Corollary 6.4 . *Each global holomorphic function on a compact Riemann surface X has to be a constant: $\mathcal{O}(X) = \mathbb{C}$.*

Namely, the absolut value function $|f| : X \longrightarrow \mathbb{R}$ is contineous. Since X is compact, there is an $m \in X$ with maximal value $|f(m)|$.

Corollary 6.5 *(Liouville). Absolutely bounded holomorphic functions on $\mathbb{C}$ are constant.*

For each point $P \in X$ one has a discrete valuation $v_P : \mathfrak{M}(X) \longrightarrow \mathbb{Z} \cup \infty$ corresponding to each function its *zero order* at P. Especially, for $P = \infty \in \mathbb{P}^1$ one finds for $f, g \in \mathbb{C}[z]$ using the local parameter $1/z$ there:

$$v_\infty(f/g) = -deg\, f(z) + deg\, g(z),\ g \neq 0.$$

Covering Theorem 6.6 . *Let $\varphi : X \longrightarrow Y$ be a holomorphic map of Riemann surfaces, $Q \in Y$, X compact. Then the preimage $\varphi^{-1}(Q)$ is finite, ϕ is surjective and Y is compact.*

Definition 6.7 . *The* multiplicity *of φ at P is defined as $mult_P(\varphi) = v_P(f)$, where $f = \varphi|U : U \longrightarrow \mathbb{C}$ sending P to 0, U a card around P.*

Definition 6.8 . Ramification points $P \in X$ *of φ: $mult_P(\varphi) > 1$;* branch points*: all φ-images of ramification points.*

Both are discrete, hence finite sets of the compact Riemann surfaces X or Y, respectively: Use the local criterion: $f'(z) = 0$ for ramification points together with Discreteness and Covering Theorem. The multiplicity of φ at P is also called *ramification order* or *ramification index*of φ at P. It is also frequently denoted by $e_P(\varphi)$.

The *local degree* of φ at Q is defined as

$$d_Q(\varphi) := \sum_{P \mapsto Q} mult_P(\varphi).$$

Proposition-Definition 6.9 . *$d_Q(\varphi)$ is constant, that means not depending on Q. It defines the* degree *of φ: $deg\, \varphi := d_Q(\varphi)$.*

Corollary 6.10 . *$\varphi : X \longrightarrow Y$ is an isomorphism iff $deg\, \varphi = 1$.*

Corollary 6.11 . *The following properties are equivalent:*

(i) $X \cong \mathbb{P}^1$*;*

(ii) there exists $f \in \mathfrak{M}(X)$ with precisely one zero P and $v_P(f) = 1$;

(iii) there exists $f \in \mathfrak{M}(X)$ with precisely one pole P and $v_P(f) = -1$.

Proposition 6.12 . *Let X be compact Riemann surface, $f \in \mathfrak{M}(X)$; then $\sum_{P \in X} v_P(f) = 0$.*

Definition 6.13 . *Let Δ be a triangulation, of the compact Riemann surface X and v, k, s the number vertices, edges respectively faces. The number*

$$e(X) = e_\Delta(X) := v - k + f$$

is called the Euler number *of X.*

The definition is correct, that means it does not depend on the choice of triangulation. For instance, the Euler number of $\mathbb{P}^1$ (Riemann sphere) is equal to 2 by *Euler's Polyhedron Theorem.* With same methods as already Euler used one can prove that the Euler number of a torus is equal to 0. The genus, defined below, of the Riemann sphere or of a torus is 0 or 1, respectively.

Definition 6.14 . *The number* $g = g^{top} = g(X) := 2 - e(X)$ *is called the (*topological*)* genus *of* X.

There is a theorem of differential topolology, which says that each Riemann surface can be embedded smoothly as $\mathbb{R}$-manifold into $\mathbb{R}^3$. The compact Riemann surface appear on this way as compact real surfaces in $\mathbb{R}^3$ with some holes. We connect two such topological surfaces X, Y by opening both, each at a point, and join the arising open holes by an open cylinder. The new compact topological surface we denote by $X \boxplus Y$. Triangulations on X and Y can be joined in obvious manner to a triangulation on $X \boxplus Y$. It is elementary to prove the following additive property of the topological genus and its consequences:

Lemma 6.15 . $g(X \boxplus Y) = g(X) + g(Y); \quad g(X) = \#\{holes\ of\ X\} \geq 0.$

By means of lifting triangulations including the set $B = B(\varphi)$ of branch points as (some) vertices it is again a matter of elementary combinatorics to prove for coverings $\varphi : X' \longrightarrow X$ of compact Riemann surfaces the

Hurwitz' Genus Formula 6.16 .

(i) $e' - \#' = d(e - \#)$,

(ii) $2g' - 2 = d(g-2) + \sum_{P' \in X'}(mult_{P'}(\varphi) - 1)$,

where $d = deg\,\varphi$, $\# = \#B(\varphi)$, $\#' = \#\varphi^{-1}(B)$, $g = g(X)$, $g' = g(X')$.

Corollary 6.17 . *With the above notations it holds that*

(i) $g = 0$ *and* $deg\,\varphi > 1 \Rightarrow B(\varphi) \neq \emptyset$;

(ii) if $g = 1$ *then:* $g' = 1 \Leftrightarrow \varphi$ *is* unramified *(that means* $B(\varphi) = \emptyset$*),*

(iii) $g' \geq g \geq 0$;

(iv) if $g \geq 2$ *and* φ *is not isomorphic then* $g' > g$.

Remember to the notions of divisors and principal ones on curves and the degree map. It is easy to transfer them to Riemann surfaces. For a complex smooth complete intersection curve $C = V(F_1, ..., F_{n-1}) \subset \mathbb{P}^n$, and hypersurfaces $H : G = 0, G$ not in $(F_1, ...F_n - 1)$, we introduce the *intersection index* at P with the help of an (arbitrary) auxiliary homogenous polynomial G_1 of the same degree as that of G satisfying $G_1(P) \neq 0$ via restriction of functions

$$(H \cdot C)_P := v_P((\frac{G}{G_1})_{|C}).$$

The *intersection divisor* is defined as

$$H \cdot C := \sum_{P \in C} (H \cdot C)_P P \in Div^+ C.$$

It holds that $H_1 \cdot C \equiv H_2 \cdot C$ for two hypersurfaces H_1, H_2 of the same degree. Therefore the *global intersection index* $(H \cdot C) := deg\, H \cdot C$ is well-defined. For hyperplanes H it is called the *degree of the embedding* $C \hookrightarrow \mathbb{P}^n$.

Lemma 6.18 . *For plane smooth curves* $\mathbb{P}^2 \supseteq C : F = 0$ *it holds that* $deg(H \cdot C) = deg\, F$.

You are not far away now to prove

Bezout's Theorem 6.19 . *For two smooth plane projective curves* $C_i : F_i = 0$ *it holds that*

$$(C_1 \cdot C_2) = deg\, C_1 \cdot C_2 = (deg\, C_1) \cdot (deg\, C_2) = (deg\, F_1) \cdot (deg\, F_2).$$

There are two important consequences, namely the genus formulas

$$g(C) = (d-1)(d-2)/2$$

for smooth projective plane curves C of degree d and

$$deg\, K = 2g - 2 = 2g^{top} - 2$$

for each canonical divisor on C (defined below). One has to combine Hurwitz' genus formula and Bezout's theorem for a proof of the first formula and to apply the Hurwitz formula to any covering (non-constant meromorphic function) $f : C \longrightarrow \mathbb{P}^1$ knowing the canonical divisors on $\mathbb{P}^1$.

Differential forms are defined locally around a point O of X as $f(z)dz$, where z is a local parameter at O and f a meromorphic function.. The local differential form $g(t)dt$ at P is identified with the former iff $f(z)dz = g(t)dt$. So each local differential form defines a global one. The vector space of *meromorphic differential forms* on X is denoted by Ω_X. It is clear that for each meromorphic differential form $\omega \neq 0$ it holds that

$$\Omega_X = \mathfrak{M}(X)\omega.$$

We dispose also on valuations of meromorphic differential forms at points P setting $v_P(fdt) := v_P(f)$, t a local parameter at P. We get surjective maps

$$v_P : \Omega_X \longrightarrow \mathbb{Z} \cup \infty$$

on this way. They define zero and pole orders of differential forms at points. The space of differential forms on X without poles on an open set $U \subseteq X$ is denoted by $\Omega_X(U)$. Its elements are called *holomorphic* or *regular* differential forms on U.

The *residue* of a meromorphic differential form ω at P is the number

$$res_P\omega = \frac{1}{2\pi i}\oint \omega,$$

where one has to integrate along a small circle around P such that inside of the circle there is no pole of ω except, perhaps, at P. Knowing the Residue Theorem for meromorphic functions on on $\mathbb{C}$ it is via triangulation not difficult to prove

Residue Theorem 6.20 . *For meromorphic differential forms ω on compact Riemann surfaces it holds that*

$$res\ \omega\ := \sum_{P\in X} res_P\omega = 0.$$

Keep in mind that Ω_X is a one-dimensional $\mathfrak{M}(X)$-vector space. Since

$$(f\cdot\omega) = (f) + (\omega)$$

for $f \in \mathfrak{M}(X)$, $\omega \in \Omega_X$, the differential forms sit in precisely one class in $Pic\,X$, called the *canonical class*. The elements of this class are called *canonical divisors*. Furthermore we define for divisors D on X the function and differential form spaces

$$\mathfrak{L}(D)\ := \{f \in \mathfrak{M}(X);\ (f) \geq -D\}\ ,\ \Omega(D)\ := \{\omega \in \Omega_X;\ (\omega) \geq D\}.$$

The corresponding dimensions are finite and are denoted by $l(D)$ or $l^*(D)$, respectively. We have

- $\mathfrak{L}(O) = \mathbb{C}$;
- $\Omega(O)$ = regular differential forms;
- $\Omega(K) = \mathbb{C}$ for canonical divisors $K = (\omega)$;
- $(\eta) \geq (\omega) \Rightarrow (\eta) - (\omega) = O$;
- $\mathfrak{L}(D) = O$ for $D < O$;
- $D \leq E \Rightarrow \mathfrak{L}(D) \subseteq \mathfrak{L}(E)$ and $\Omega(D) \supseteq \Omega(E)$;
- $D \equiv D' \Rightarrow \mathfrak{L}(D) \cong \mathfrak{L}(D')$, hence $l(D) = l(D')$,
  and $\Omega(D) \cong \Omega(D')$, hence $l^*(D) = l^*(D')$.

We have also for divisors D, E a bilinear map

$$\mathfrak{L}(E-D)\otimes\Omega(E) \longrightarrow \Omega(D), \quad (f,\omega)\mapsto f\omega;$$

especially, for any canonical divisor $E = K = (\omega)$ one gets an isomorphy

$$\mathfrak{L}(K-D)\otimes\Omega(K) = \mathfrak{L}(K-D) \xrightarrow{\sim} \Omega(D).$$

Any fixed canonical divisor K defines an involution on the divisor group

$$^* : Div\, X \longrightarrow Div\, X, \quad D \mapsto D^* := K - D.$$

It is convenient to keep in mind the dual style of writing

$$\mathfrak{L}(D^*) \cong \Omega(D), \quad l^*(D) = l(D^*) = l(K - D) = dim\, \Omega(D).$$

Riemann-Roch Theorem 6.21 *(topological or geometric version). For each divisor D on a compact Riemann surface X it holds that*

$$l(D) - l^*(D) = deg\, D + 1 - g, \quad g = g^{top} \text{ the topological genus of } X.$$

Especially, for $D = O$ one gets

$(\mathrm{RR})_0$ $g^{an} := l(K) = dim\Omega(O) = g = g^top.$

We defined the *analytic genus* g^{an} and change to

Riemann-Roch Theorem 6.22 *(analytic version). For each divisor D on a compact Riemann surface X it holds that*

$$l(D) - dim\, \Omega(D) = deg\, D + 1 - g^{an}.$$

We attack the proof of the analytic version by Mittag-Leffler theory. For this purpose we need (finite) tails of Laurant-series. For $P \in X$, t a local parameter at P, $f \in \mathfrak{M}(X)$, $\omega \in \Omega_X$, we assume that $v_P(f) = m = v_P(\omega)$. Then there exist unique *Laurent series*

$$f = a_m t^{-m} + ... + a_{-1} t^{-1} + \ Taylor\, series\, in\, t, \quad a_m \neq 0,$$
$$\omega = f dt = (a_m t^{-m} + ... + a_{-1} t^{-1} + \ Taylor\, series) dt.$$

Principal tails look like

$$a_m t^{-m} + ... + a_{-1} t^{-1}, \quad (a_m t^{-m} + ... + a_{-1} t^{-1}) dt$$

One can prove that

Proposition 6.23 . *With the above notations the local residues of differential forms can be algebraically expresed as*

$$res_P \omega = a_{-1},$$

independently of the local parameter choice.

Corollary 6.24 . *If ω is regular at P, then $res_P \omega = 0$.*

Mittag-Leffler Theorem 6.25 . *For given principal tails $\omega_1, ..., \omega_r$ at different points $P_1, ..., P_r \in X$ there exist differential forms ω with principal tails ω_i at P_i, $i = 1, .., r$, which are regular elswhere, if and only if*

$$res(\omega_1 + ... + \omega_r) = a_{-1}^{(1)} + ... + a_{-1}^{(r)} = 0.$$

(with obvious notations).

One direction comes immediately from the Residue Theorem.

Corollary 6.26 . *For any negative divisor* $D = m_1P_1 + ... + m_rP_r < O$ *it holds that*

$$dim\Omega(D) = -deg\, D + dim\Omega(O) - 1$$

It is not difficult to prove that the analytic version of the Riemann-Roch Theorem is equivalent to Mittag-Leffler Theorem. The proof direction ($\Rightarrow$) is an easy exercise, deduce it from $(RR)_-$ below. We give some steps for proving the other direction.

1-st step: Substitute l(D) = 0 in the 6.22 to get

$(RR)_-$ $l(D) - dim\,\Omega(D) = deg\, D + 1 - g^{an}$ for all $D < O$.

This follows easily from 6.25 by counting constants (coefficients) in the given tails there.

2-nd step: Observe that D^* is negative for $D > K$. The proof of

$(RR)_{>K}$ $l(D) - dim\,\Omega(D) = deg\, D + 1 - g^{an}$ for $D > K$

can be easily reduced to the first step.

3-rd step: $\lambda(D) := l(D) - l^*(D) - deg\, D$ is an increasing function:

For this step is sufficient to prove that $\lambda(D+P) \leq \lambda(D)$ for $P \in X$, $D \in Div\, X$.

Let t be a local parameter at P and

$$D = dP + ...other\ points....$$

The map $f \mapsto ft^{d+1}$ yields an exact sequence

$$0 \longrightarrow \mathfrak{L}(D) \longrightarrow \mathfrak{L}(D+P) \longrightarrow \mathcal{O}_P/\mathfrak{m}_P = \mathbb{C}.$$

It follows that

$$l(D+P) = l(D) + \epsilon, \quad l(D^*) = l(D^* - P) + \delta, \quad \epsilon, \delta \in 0, 1,$$

hence

$$l(D^*) = l(D) + \epsilon + \delta - 1.$$

We show that $\epsilon = \delta = 1$ is impossible. Assume the contrary.
Take $f \in \mathfrak{L}(D+P) \setminus \mathfrak{L}(D)$, $\omega \in \Omega(D) \setminus \Omega(D+P)$. It follows $f\omega \in \Omega(-P)$ because $(f\omega) = (f) + (\omega) \geq -(D+P) + D = -P$ and $(f\omega)_P = -P$ because

$$(f) = -(d+1)P + ..., \quad (\omega) = dP + ...$$

We get a contradiction to the Residue Theorem:

$$0 = res\,\omega = res_P\omega \neq 0.$$

3-rd step: For negative divisors $N < O$ and $D' > K$ we know already that the Riemann-Roch formula holds, that means $\lambda(D') = \lambda(N) = 1 - g^{an}$. For an arbitrary divisor D choose N , D' as above such that $N < D < D'$. Since λ is increasing we get also $\lambda(D) = 1 - g^{an}$, which is the analytic Riemann-Roch formula.

Now we are a littlebit prepared for the use of Laurent tails in order to prove the analytic version of Riemann-Roch Theorem. Consider the *local Laurent tail space* space $\mathfrak{T}_P$ consisting of all Laurent tails at P. The subspace $\mathfrak{T}_P(kP)$, $k \in \mathbb{Z}$, consists, by definition, of all tails $\tau \in \mathfrak{T}_P$ with $v_p(\tau) \geq -k$. For a divisor $D = k_1P_1 + ... + k_rP_r$ we define the subspace

$$\mathfrak{T}(D) = \bigoplus_{i=1}^{r} \mathfrak{T}_{P_i}(k_iP_i) \oplus \bigoplus_{Q \neq P_i} \mathfrak{T}_Q(0 \cdot Q)$$

of the *global Laurent tail space* $\mathfrak{T} := \bigoplus_{P \in X} \mathfrak{T}_P$. For instance, $\mathfrak{T}(O)$ is the space of finite sums of regular (local) tails. Now we introduce the *truncation map*

$$\tau_D : \mathfrak{M}(X) \longrightarrow \mathfrak{T}(D),$$

which cuts away (to set 0) from the local Laurent series of a meromorphic function all summands of v_P-value $\geq -v_p(D)$, where $v_P(D)$ is defined as coefficient of D at P (0 if P doesn't occur in D). For instance, the image of τ_O consists of finite sums of principal tails. We get exact sequences

$$0 \longrightarrow \mathfrak{L}(D) \longrightarrow \mathfrak{M}(X) \longrightarrow \mathfrak{T}(D) \longrightarrow H^1(D) \longrightarrow 0$$

Exactness on the laeft side comes from the definitions. The right part is nothing else but a definition of the *first cohomology group* $H^1(D)$ as cokernel of the truncation map τ_D. Stepwise one can to prove the following facts:

Proposition 6.27 . $h^1(D) := dim\, H^1(D) < \infty$.

Riemann-Roch Theorem 6.28 *(cohomological version).*

$$l(D) - h^1(D) = deg\, D + 1 - h^1(O).$$

Theorem 6.29 *(Serre duality). There is a canonical isomorphism* $H^1(D) \cong \Omega(D)^\vee$ *onto the dual space of* $\Omega(D)$.

The proof is based on the residue map

$$\mathfrak{T}(D) \times \Omega_X(D) \longrightarrow \mathbb{C}, \quad (tail\ sum, \omega) \mapsto \sum_{P \in X} res_P(tail_P \cdot \omega)$$

It factorizes through $H^1(D) \times \Omega(D)$. This is the pairing of Serre duality.

Corollary 6.30 . $h^1(D) = dim H^1(D) = dim \Omega(D) = l^*(D)$.

Now we are able to finnish the analytic Riemann-Roch Theorem. We have only to substitute in the cohomological version $h^1(D)$ by $l^*(D) = dim\ \Omega(D)$ and $h^1(O)$ by $l^*(O) = l(O^*) = l(K) = g^{an}$ to get 6.22.

For $D = K$ we get

$$l(K) - l^*(K) = deg\, K + 1 - l(K)$$

We know that $l^*(K) = l(K^*) = l(O) = 1$ and $deg\, K = 2g^{top} - 2$. We substitute both and receive $2 \cdot l(K) = 2g^{top}$, hence $g^{an} = l(K) = g^{top}$. It clear that the most classical geometric version follows now immediately from the analytic version.

We mention without detailed proofs some applications of the Riemann-Roch Theorem.

Theorem 6.31 . *Each compact Riemann surface X can be embedded into a projective space $\mathbb{P}^N$.*

So - up to isomorphy - there is no difference between Riemann surfaces and smooth projective complex algebraic curves. For embeddings one uses completions of maps

$$(f_0 : f_1 : ... : f_n) :\ X \hookrightarrow \mathbb{P}^n, \quad P \mapsto (f_0(P) : ... : f_n(P))$$

defined outside of the locus of common zeros of any basis $f_0, f_1, ..., f_n$ of $\mathfrak{L}(D)$ of suitable divisors D on X.

Most important for curves of genus > 2 are canonical embeddings working - by definition - with a canonical divisor $D = K$. Sometimes the canonical divisor does not embed the Riemann surface. This happens if and only if the curve is *hyperelliptic*. But the canonical map is a covering map onto its image curve for each curve of genus ≥ 2.

7 Plane Curves

We write a short dictionary for plane projective curves over algebraically closed fields. In the file "RealCurves.mws" we present a list of nice real pictures of plane curves visualizing singularities and resolution (steps) with the $\sigma - process$. To open the file one has to implant it into MAPLE.

Flex point (also *inflection point*): Regular point P of a projective curve C with tangent line contacting C of order ≥ 3, or equivalently: the tangent hyperplane of C at P meets C at P with multiplicity ≥ 3. There are only finitely many flex points on C.

Flex tangent: Tangent at a flex point.

Tangent hyperplane of a projective curve C at a regular point P: A hyperplane meeting C at P with multiplicity ≥ 2.

Double tangent: Projective lines of a plane projective curve C, which is a tangent at two different points of C.

Ordinary singularity: Plane curve singularity with multiplicity $m > 1$ having m different tangent lines.

Node: Ordinary double point of a plane curve singularity.

Cusp (sometimes *hypercusp*): Curve singularity P with only one tangent line of the curve at P.

Simple cusp: Hypercusp of plane curve with multiplicity 3.

Dual curve C^* of a projective plane curve C (not a line): The algebraic closure of the curve in the dual space $\check{\mathbb{P}}^2$ of $\mathbb{P}^2$-lines consisting of all tangents on C. The correspondence $C \mapsto C^*$ is an involution on the set of projective curves not being lines. This involution restricts to the subset of all irreducible curves and to the set of Plücker curves.

Plücker curve: Plane irreducible projective curve with at most nodes and simple cusps as singularities.

Class of a projective curve C: maximal number $n^* = n^*(C) = n^*_Q(C)$ of tangents at regular points of C through a fixed point $Q \in \mathbb{P}^2$. This number is

the same for almost all points $Q \in \mathbb{P}^2$. It coincides with the degree $deg\, C^*$ of the dual curve C^*.

Plücker formulas (for Plücker curves). Let C be a projective curve of degree $n > 1$. Set

$$d = d(C) := \#\{double\, points\, of C\}, \quad d^* := d(C^*),$$

$$s = s(C) := \#\{cusps\, of\, C\}, \quad s^* = s(C^*).$$

It holds that

a) $d^* = \{double\, tangents\, of\, C\}$,

b) $s^* = \#\{inflection\, points\, of C\}$,

a*) $d = \#\{double\, tangents\, of\, C^*\}$,

b*) $s = \#\{inflection\, points\, of\, C^*\}$;

1) $n^* = n(n-1) - 2d - 3s$ (*class formula*),

2) $s^* = 3n(n-2) - 6d - 8s$ (*inflection point formula*),

1*) $n = n^*(n^*-1) - 2d^* - 3s^*$,

2*) $s = 3n^*(n^*-2) - 6d^* - 8s^*$.

Clebsch's genus formula for Plücker curves C: The genus $g = g(C)$ of (a smooth model of) C is equal to $1/2(n-1)(n-2) - (d+s)$.

Canonical map of smooth projective curves C (Riemann surfaces) of genus $g \geq 2$ is the regular (holomorphic) map

$$(\omega_0 : \omega_1 : ... : \omega_{g-1}) : \; C \longrightarrow \mathbb{P}^{g-1}$$

extending

$$(1 : f_1 : ... : f_{g-1}) : \; P \mapsto (1 : f_1(P) : ... : f_{g-1}(P))$$

where $\omega = \omega_0$, $\omega_1 = f_1\omega$,..., $\omega_{g-1} = f_{g-1}\omega$ is a basis of the space of regular differential forms on C.

Canonical model: The image curve of a canonical map.

Hessian $H(C)$ of a smooth plane curve $C : F = 0$: defined by $H(F) = 0$, where

$H(F)$ is the determinant of $(\partial^2 F/\partial\ z_i \partial z_j)$, $i\,,\, j = 0,1,2$. The intersection of $H(C)$ and C coincides with the set of inflection points of C.

n-gonal curve (also *superelliptic curve*): n-cyclic covering of $\mathbb{P}^1$. In characteristic 0 such a curve has a plane model of affine equation type

$$Y^k = p_n(X), \quad p_n(X) \in K[X]\, of\, degree\, n.$$

Picard curve (smooth): 3-gonal curve of genus 3. In characteristic 0 such a curve has a plane model of affine equation type

$$Y^3 = X^4 + aX^3 + bX^2 + cX + d = p_4(X),\ p_4(X)\, without\, multiple\, zero.$$

Hyperelliptic curve: smooth 2-gonal curve. In characteristic 0 such a curve C has a plane model of affine equation type

$$Y^2 = p_n(X), \quad p_n(X)\, without\, multiple\, zero, \quad n = 2m+1\, odd.$$

The genus g of a smooth model C is equal to m. The point $\infty := (0:1:0)$ is regular only in the elliptic case $g = m = 1$. The projection $(x,y) \mapsto x$ onto the x-axes extends projectively to the canonical map $C \longrightarrow \mathbb{P}^1$, which is a 2-sheeted Galois covering. Among the smooth curves of genus $g \geq 2$ the hyperelliptic curves of are characterized by each of the following properties:

(i) The canonical map $C \longrightarrow \mathbb{P}^{g-1}$ factorizes through a 2-sheeted Galois covering onto a smooth rational curve.

(ii) There is a 2-sheeeted Galois covering of C onto $\mathbb{P}^1$.

(iii) The canonical map $C \longrightarrow \mathbb{P}^{g-1}$ is not an embedding.

Rational curve: Curve of genus 0. A smooth rational curve is isomorphic to $\mathbb{P}^1$. Smooth projective plane rational curves are the *quadrics* (degree 2 curves) and the projective lines.

Elliptic curve: Smooth curve of genus 1. In characteristic 0 such a curve has a plane model of affine equation type

$$Y^2 = X^3 + aX^2 + bX + c = p_3(X), \quad p_3(X)\, without\, multiple\, zero.$$

All smooth projective plane cubic curves are elliptic.

Genus 2 curve: All genus 2 curves are hyperelliptic. In characteristic 0 such a curve has a plane model of affine equation type

$$Y^2 = X^5 + aX^4 + bX^3 + cX^2 + dX + e = p_5(X), \quad p_5(X)\, without\, multiple\, zero.$$

genus 3 curve: The non-hyperelliptic smooth genus 3 curves are characterized by the property to have a smooth plane quartic model. These are the canonical

models of the curves.

Cremona transformation (also: *quadratic transformation*): Birational transformation of $\mathbb{P}^2$ which is projectively equivalent to the standard one $\sigma : (x : y : z) \mapsto (yz : xz : xy)$. This map is well-defined outside of the three points $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$, which are called *fundamental points* of σ. Cremona transformations are involutions, that means $\sigma^2 = Id_{\mathbb{P}^2}$.

Theorem 7.1 . *For each projective plane curve C there is a birational transformation of $\mathbb{P}^2$ (more precisely, a composition of Cremona transformations) such that the proper transform C' of C has at most ordinary singularities.*

birational transformation of a smooth surface S: Composition of some σ-processes at points and some inverses of them: $S \longleftarrow S' \longrightarrow S$.

8 Contents of the Curve Album

1.) Hyperelliptic curve of genus 2

2.) Double point, Newton's knot

3.) Simple cusp

4.) Cusp points (on a heart)

5.) Cusp points (on a sail) with different multiplicities

6.) Ordinary triple point

6.a) Resolution of the ordinary triple point by sigma-process, (t,x)-plane

6.b) Resolution of the ordinary triple point by sigma-process, (s,y)-plane

7.) Non-ordinary singularity

7.a) Resolution step for the non-ordinary singularity by sigma-process, (t,x)-plane

7.b) Resolution step for the non-ordinary singularity by sigma-process, (s,y)-plane

8.) Other node (double point), Pascal snall

9.) Inflection point

10.) Higher singularity, cusp meets curve

11.) Higher singularity, selftouch of a curve

12.) Higher singularity, touching ovals

13.) Higher singularity, branch through cusp

14.) Higher singularity, double cusp

15.) Node and self touch

16.) Three-cusped hypocycloide

16.a) Bell: resolution of one of the 3 cusps by sigma-process

17.) Cardiode

18.) A Plücker curve with nodes only

18.a) the Plücker curve after little moves

19.) (small) quartic perturbation of four lines

20.) Picard curve, with 4 visible inflection points

21.) Degenerated Picard curve, simple cusp

22.) Special Picard curve (having splitting Jacobian threefold)

23.) G. Lachaud's model of the Klein quartic

24.) A diagonal curve of genus 7 with singularity

25.) "Newton's heart": Reciprocal radius transformation of Newton's knot curve

References

[1] Atiyah., M.F., Introduction to Commutative Algebra, Addison-Wesley, 1969

[2] Eisenbud, D., Commutative Algebra, Springer, 1995

[3] Fulton, W., Algebraic Curves, Addison-Wesley, 1989

[4] Kunz, E., Einführung in die algebraische Geometrie, Vieweg, 1974

[5] Miranda, R., Algebraic Curves and Riemann Surfaces, Amer. Math. Soc., 1997

[6] Shafarevich, I.R., Basic Algebraic Geometry, Springer, 1974

[7] Stichtenoth, H., Algebraic Function Fields and Codes, Springer, 1993

[8] Zariski, O., Samuel, P., Commutative Algebra, vol. I,II, van Nostrand, 1960

[9] Holzapfel, R.-P., Lectures on: Algebra, Algebraic curves and Riemann surfaces, Algebraic Coding Theory, Modular Forms, Special Picard Modular Varieties, Humboldt-University Berlin, 1998-2000

[9a] Holzapfel, R.-P. Einführung in die algebraische Codierungstheory, (The original Goppa codes - elementary and selfcontained introduction into the algebraic theory of error correcting codes), based on the lecture manuscript of Rahel Stichtenoth (stud. math.), written by Thorsten Riedel (stud. math.), www-irm.mathematik.hu-berlin.de/my homepage, 2000

Rolf-Peter Holzapfel
Mathematisches Institut
Humboldt-Universität Berlin
Rudower Chaussee 25
10099 Berlin GERMANY
e-mail: holzapfl@mathematik.hu-berlin.de

Presented during the lectures at

CIMPA-UNSA-ICTP-UNESCO-ICIMAF School

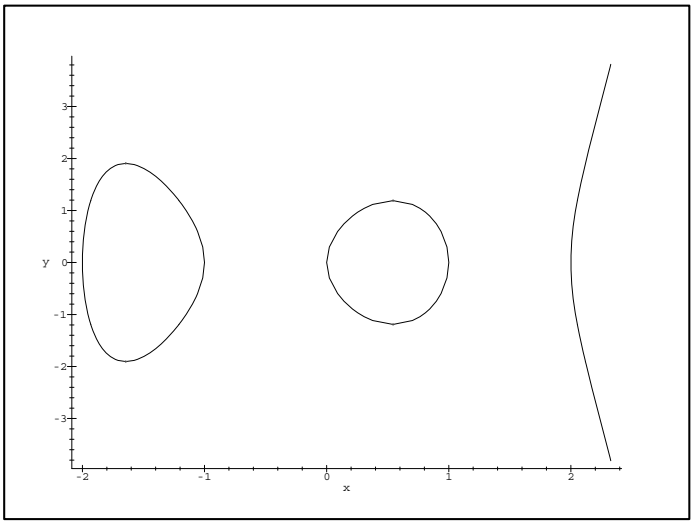
"Algebraic Geometry and its Applications to Error Correcting Codes and Cryptography"

Havanna, 20-th Novembre - 1-st December 2000

R.-P. Holzapfel, Humboldt-University, Berlin

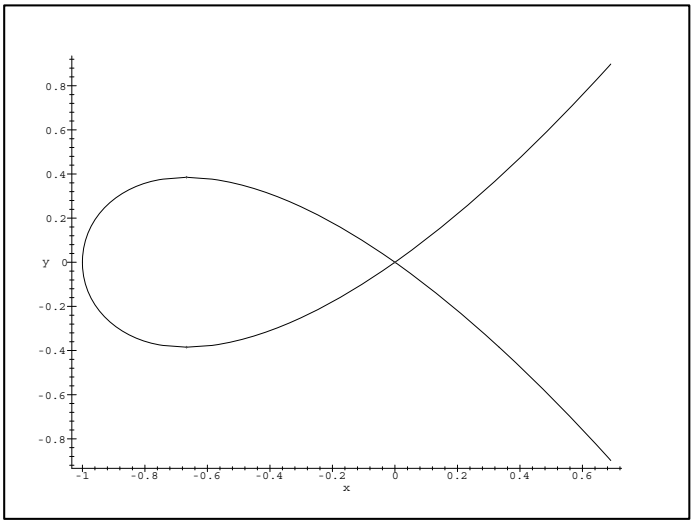
1.
Hyperelliptic curve of genus 2 (topological: # {holes}),
real affine plane section with compact pretzel-like IRˆ3-model:

$$y^2 - (x+2)\,(x+1)\,x\,(x-1)\,(x-2)$$



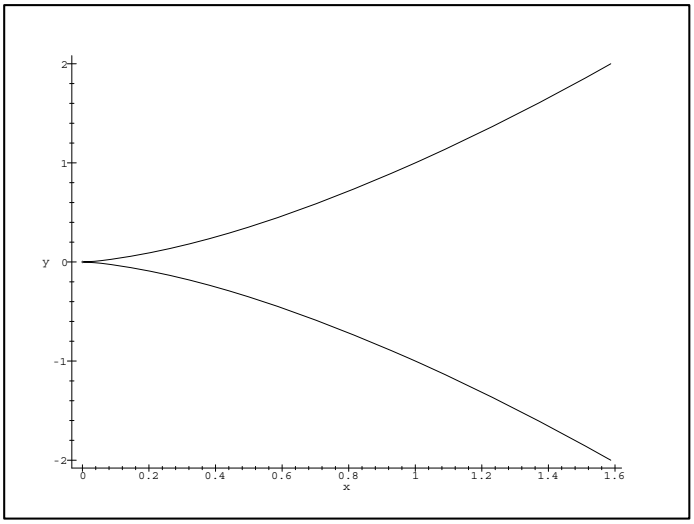
2.
Double point, Newton's knot (old language):
Newton, I., Enumeratio linearum tertii ordinis, London 1704

$$y^2 - x^3 - x^2$$



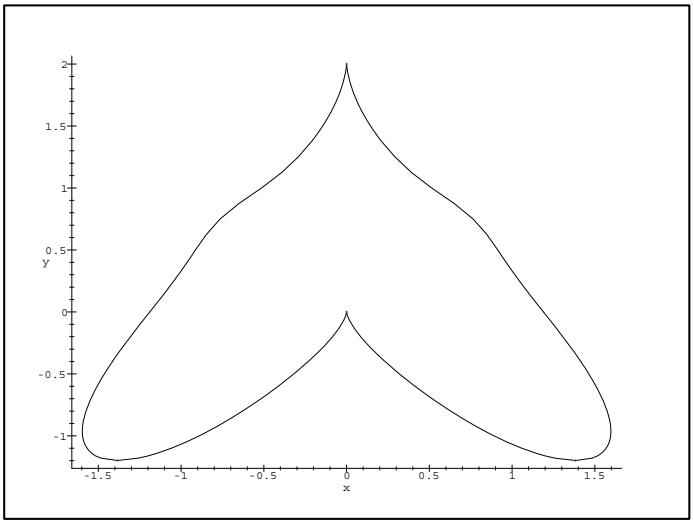
3.
Simple cusp:

$$y^2 - x^3$$



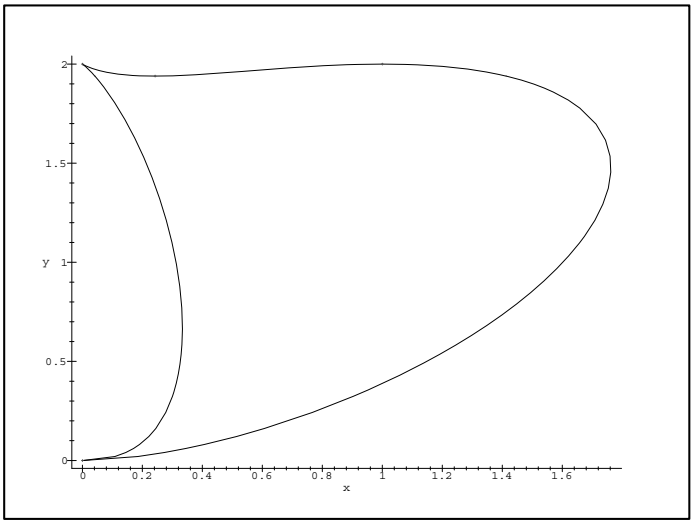
4.
Cusp points (on a heart):

$$16\,x^2\,(x^4+y^4)+2\,(y-2)^3\,(2\,y^3-x^2\,y+2\,x^2)$$



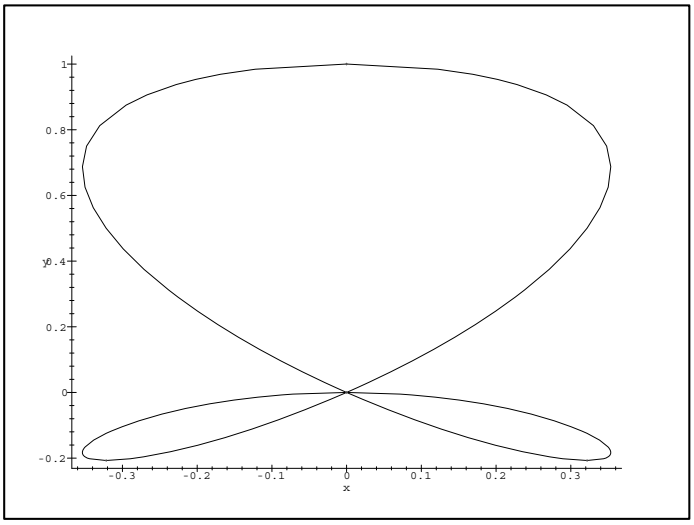
5.
Cusp points (on a sail) with different multiplicities:

$$4\,x^4-4\,x^3\,y+5\,x^2\,y^2+2\,x\,y^3+y^4-4\,y\,(2\,x^2+x\,y+y^2)+4\,y^2$$



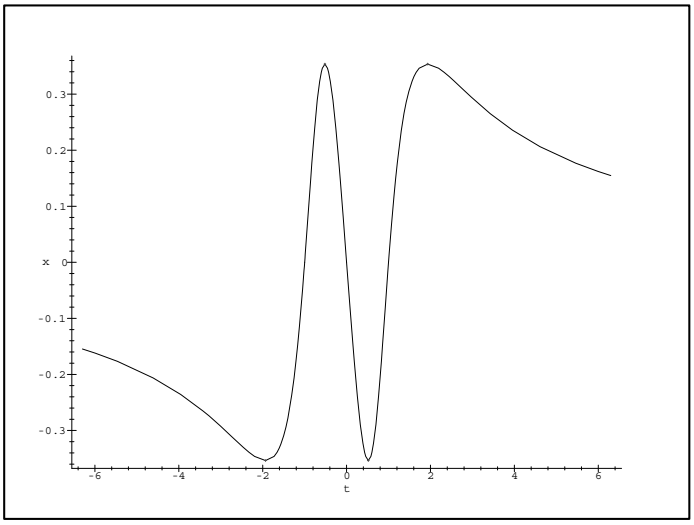
6.
Ordinary triple point:

$$y\,(y^2 - x^2) - x^4 - y^4$$



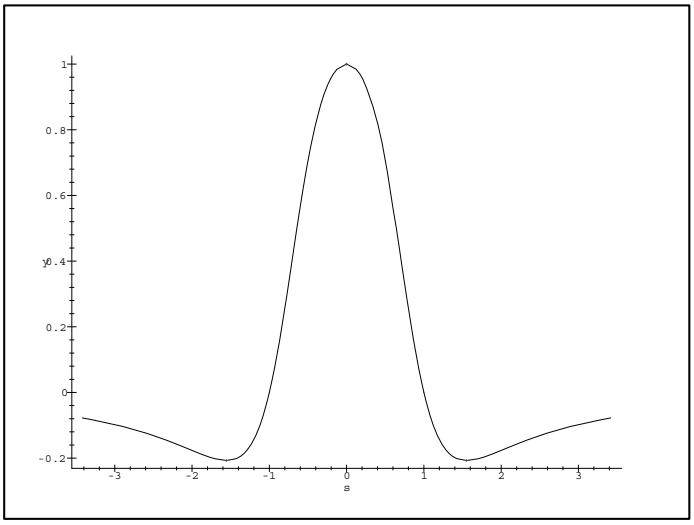
6.a
Resolution of the ordinary triple point by sigma-process, (t,x)-plane:

$$t\,x\,(t^2\,x^2 - x^2) - x^4 - t^4\,x^4$$



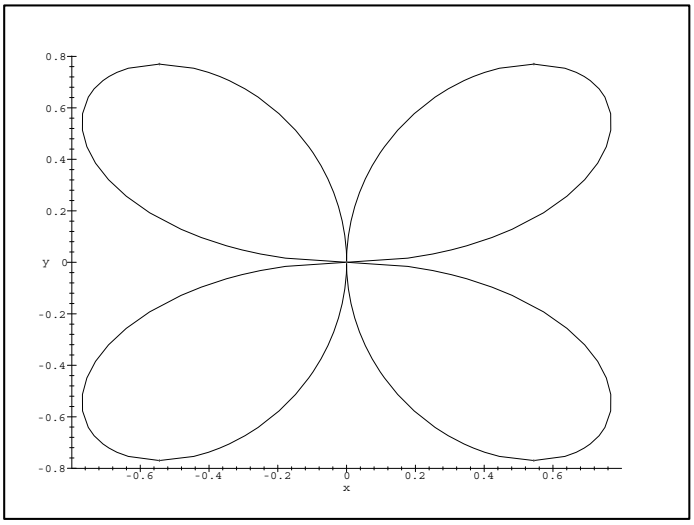
6.b
Resolution of the ordinary triple point by sigma-process, (s,y)-plane:

$$y\,(y^2 - s^2\,y^2) - s^4\,y^4 - y^4$$



7.
Non-ordinary singularity:

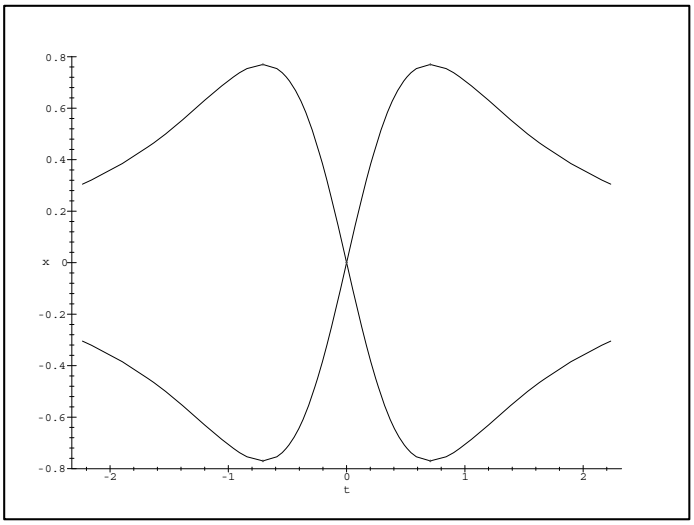
$$(x^2 + y^2)^3 - 4\,x^2\,y^2$$



7.a

Resolution step for the non-ordinary singularity by sigma-process, (t,x)-plane:

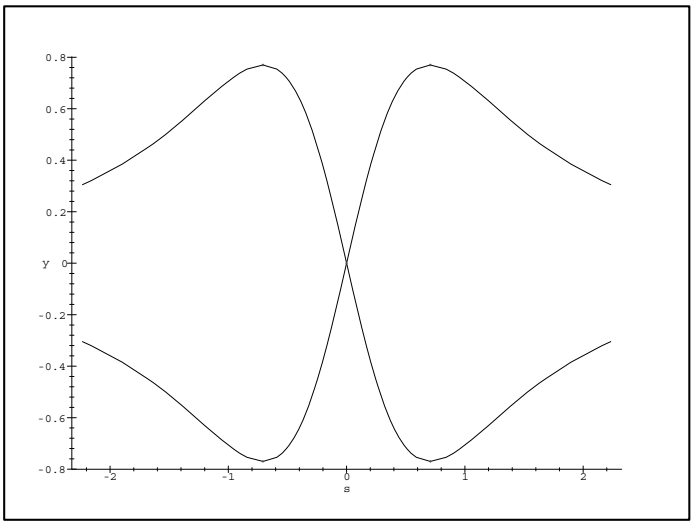
$$(x^2 + t^2\, x^2)^3 - 4\, x^4\, t^2$$



7.b

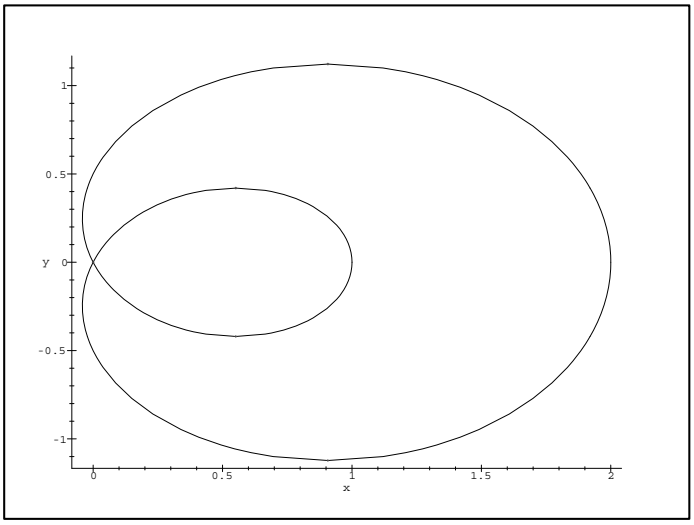
Resolution step for the non-ordinary singularity by sigma-process, (s,y)-plane:

$$(s^2\, y^2 + y^2)^3 - 4\, s^2\, y^4$$



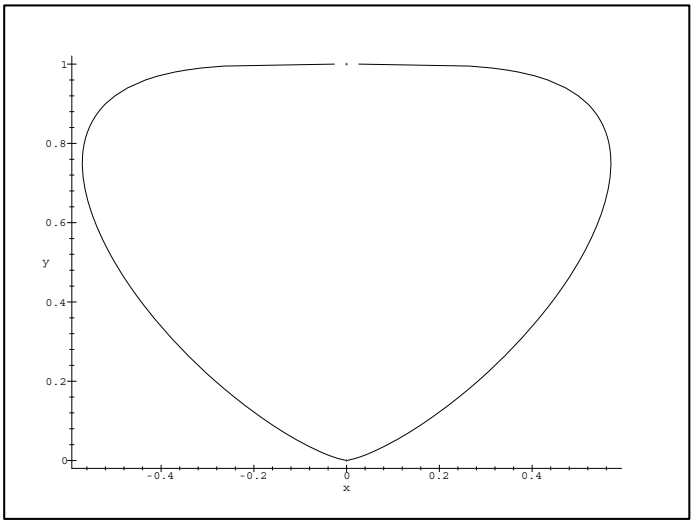
8.
Other node (double point), Pascal snall:

$$(2\,x^2 + 2\,y^2 - 3\,x)^2 - x^2 - y^2$$



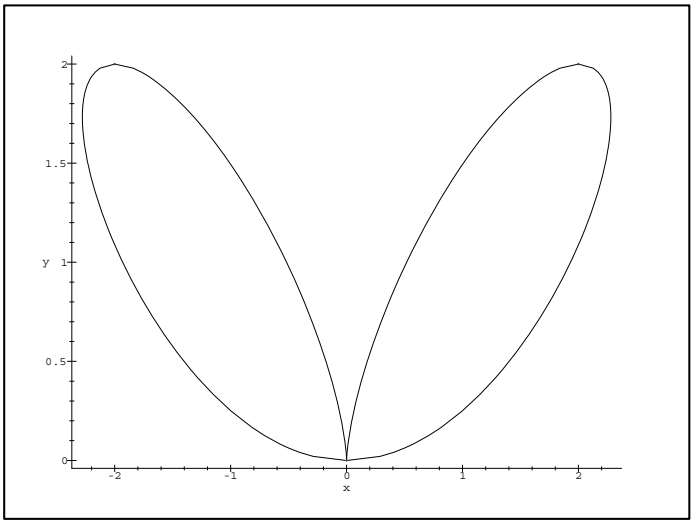
9.
Inflection point:

$$y^3 - y^4 - x^4$$



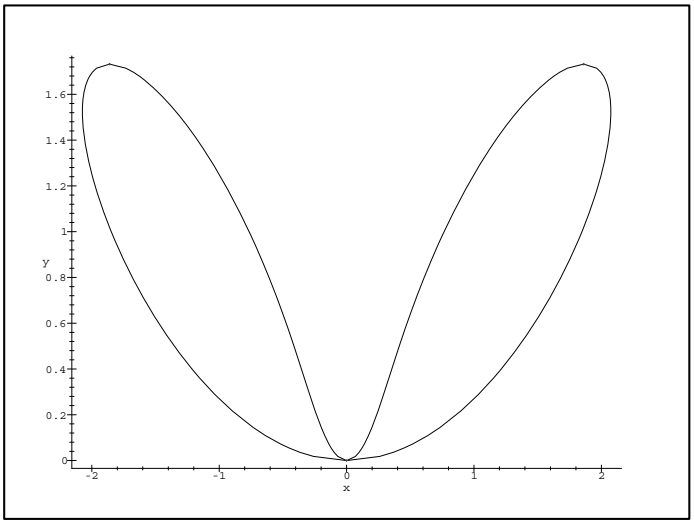
10.
Higher singularity, cusp meets curve:

$$x^4 + y^4 - 4\,x^2\,y$$



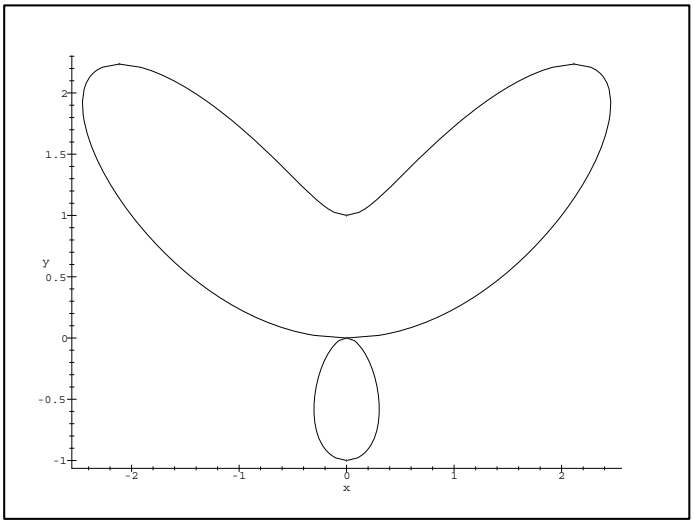
11.
Higher singularity, selftouch of a curve:

$$x^4 + y^4 - 4\,x^2\,y + y^2$$



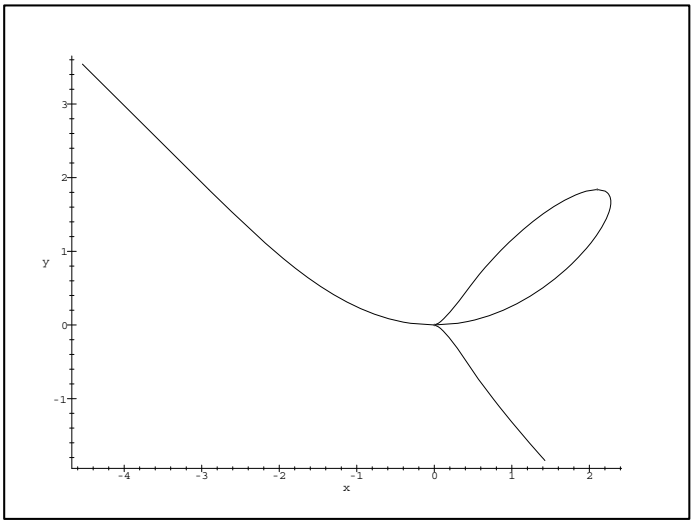
12.
Higher singularity, touching ovals:

$$x^4 + y^4 - 4\,x^2\,y - y^2$$



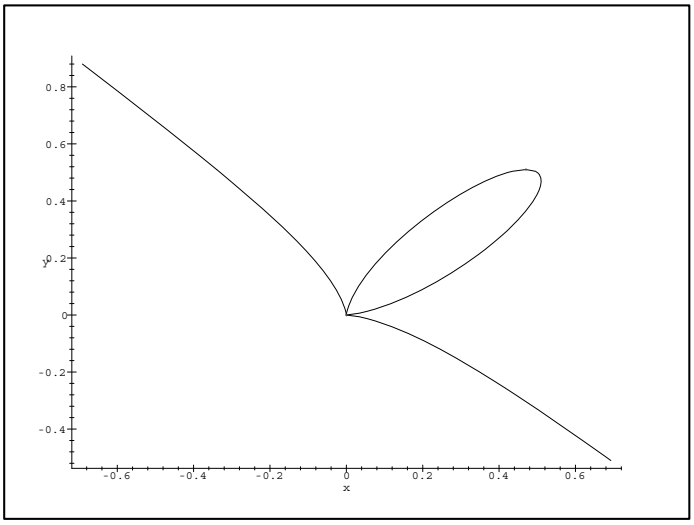
13.
Higher singularity, branch through cusp:

$$y^5 + y^3 - 4\,x^3\,y + x^5$$



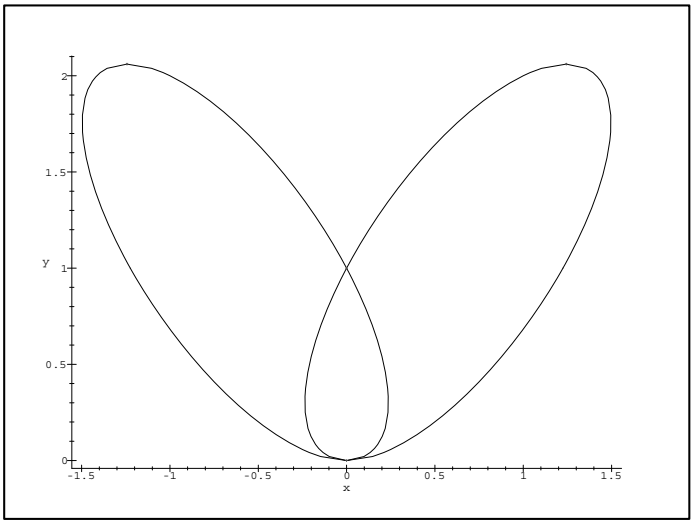
14.
Higher singularity, double cusp:

$$x^5 + y^5 - x^2\,y^2$$



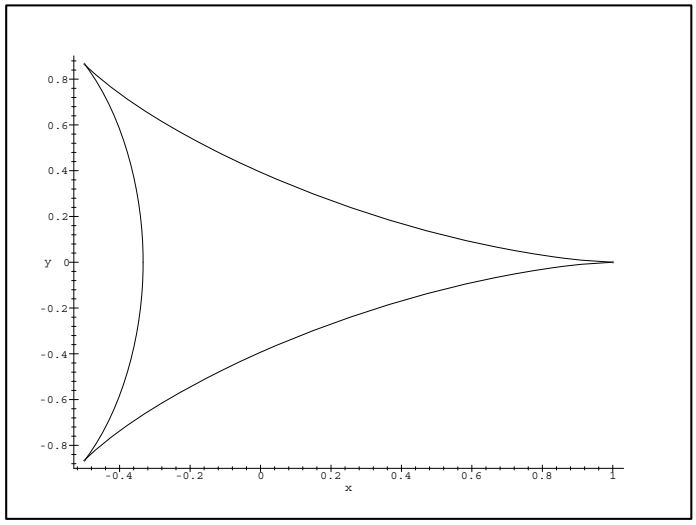
15.
Node and self touch:

$$2\,x^4 - 3\,x^2\,y + y^2\,(y-1)^2$$



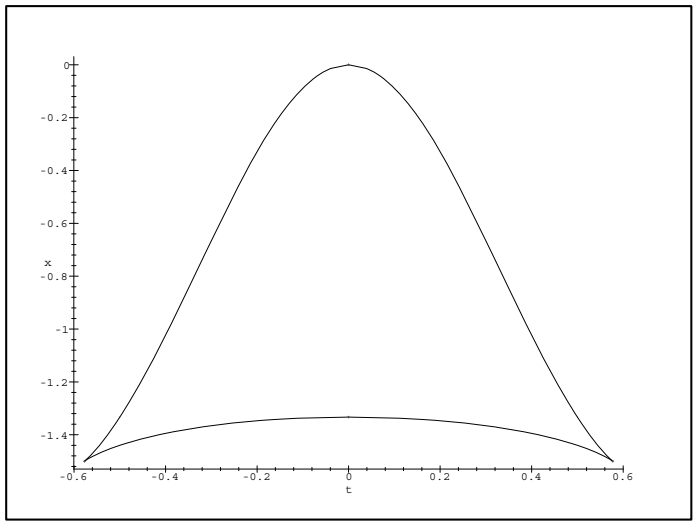
16.
Three-cusped hypocycloide:

$$3\,(x^2+y^2)^2+8\,x\,z\,(3\,y^2-x^2)+6\,z^2\,(x^2+y^2)-1$$



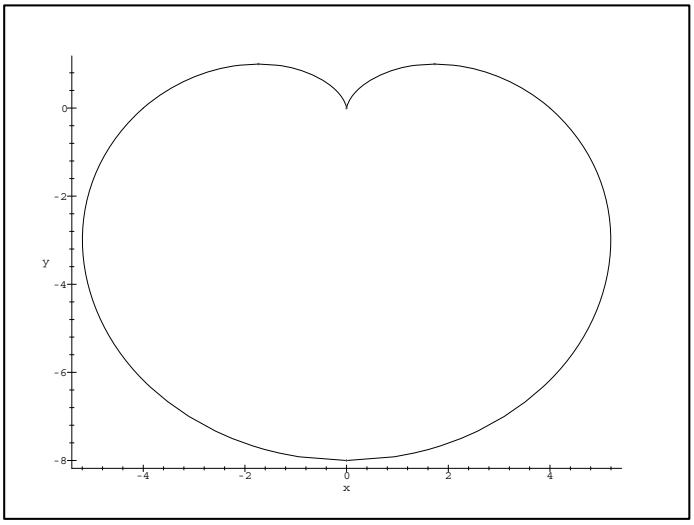
16.a
Bell,
Resolution of one of the 3 cusps by sigma-process, (t,x)-plane:

$$3\,((x+1)^2+t^2\,x^2)^2+8\,(x+1)\,(3\,t^2\,x^2-(x+1)^2)+6\,(x+1)^2+6\,t^2\,x^2-1$$



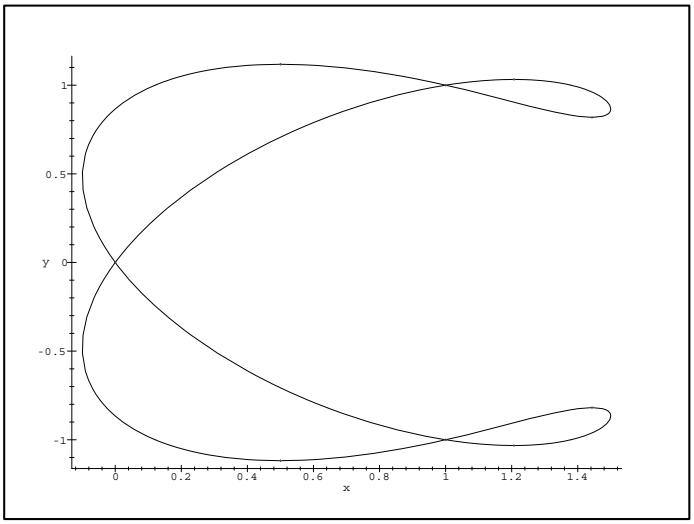
17.
Cardiode:

$$(x^2 + y^2 + 4\,y)^2 - 16\,x^2 - 16\,y^2$$

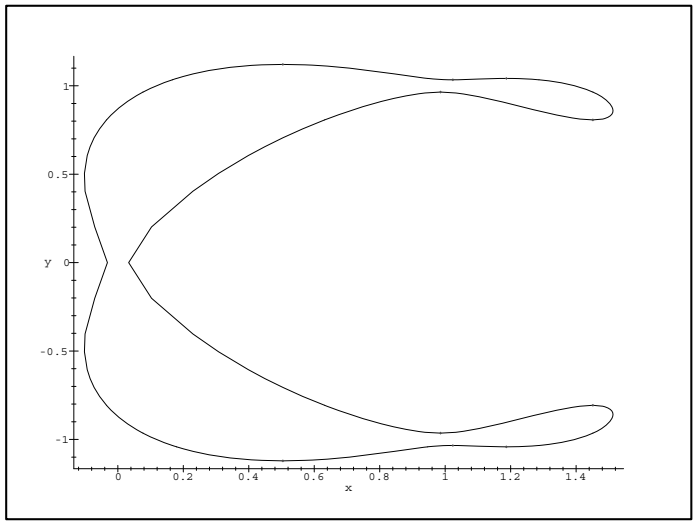


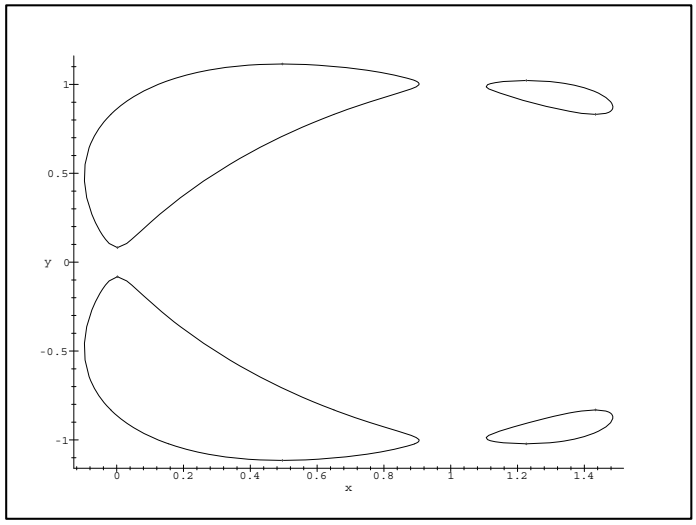
18.
A Plcker curve with nodes only:

$$(y^2 - x^2)\,(x-1)\,(x - \frac{3}{2}) - 2\,(y^2 + x\,(x-2))^2$$



18.a
the Plcker curve after little moves:

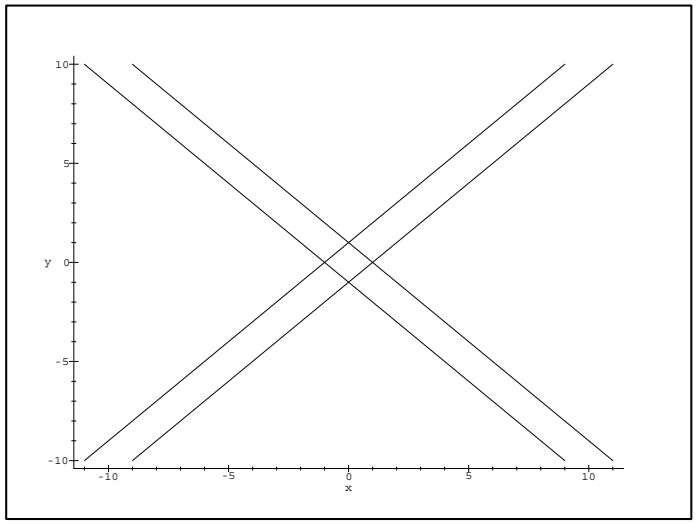


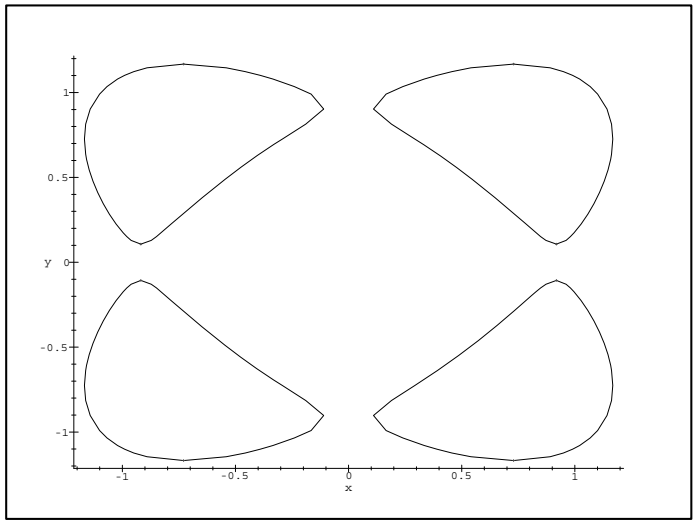


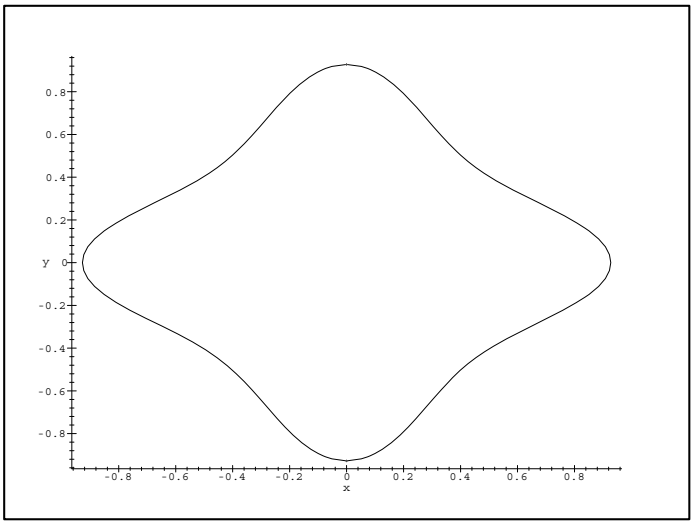
19.

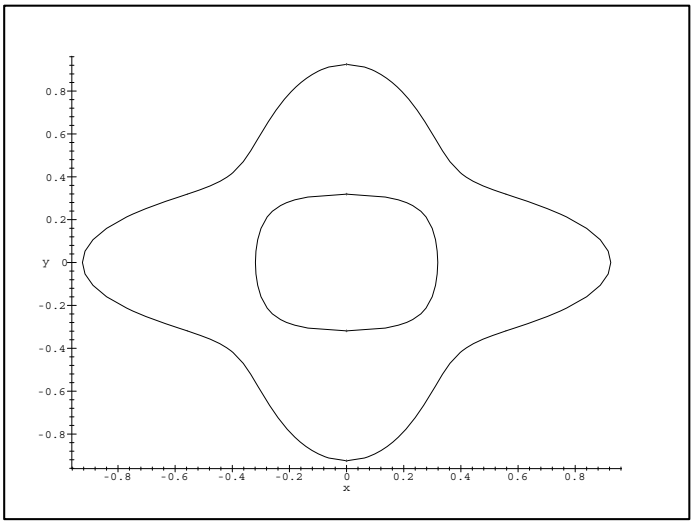
(small) quartic perturbation of four lines

(add r(4x^2 + 4y^2 - 3)^2, -1/12 < r < 1/12 to the 4-line polynomial)






0.8
0.6
0.4
0.2
y 0
-0.2
-0.4
-0.6
-0.8
-0.8 -0.6 -0.4 -0.2 0 0.2 0.4 0.6 0.8
x

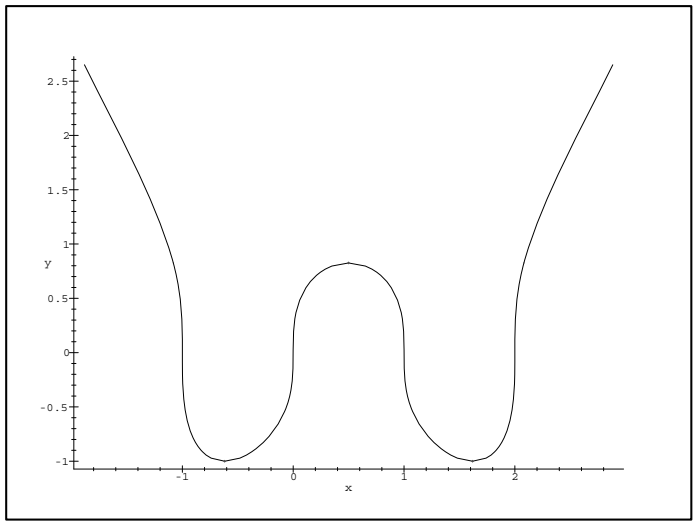

0.8
0.6
0.4
0.2
y 0
-0.2
-0.4
-0.6
-0.8
-0.8 -0.6 -0.4 -0.2 0 0.2 0.4 0.6 0.8
x

20.

Picard curve, with 4 visible inflection points:

(general investigations by E. Reinaldo Barreiro, J. Estrada-Sarlabous, R.-P. Holzapfel)

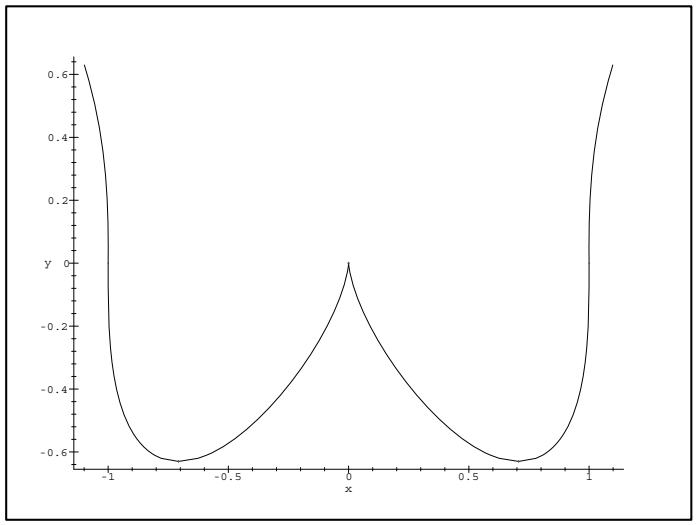
$$y^3 - x^4 + 2\,x^3 + x^2 - 2\,x$$



21.

Degenerated Picard curve, simple cusp, g = 2:

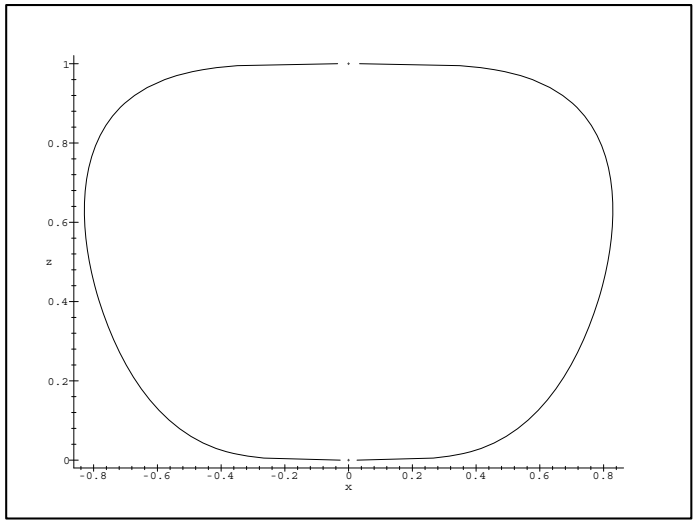
$$y^3 - x^4 + x^2$$



22.
Special Picard curve (having splitting Jacobian threefold), in (x,z)-plane:
(investigated earlier by G. Lachaud)

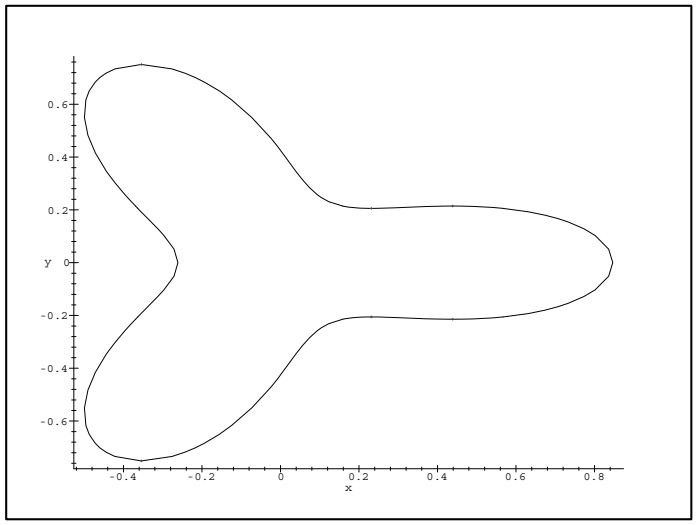
$$y^3 - x^4 - 1$$

$$z - x^4 - z^4$$



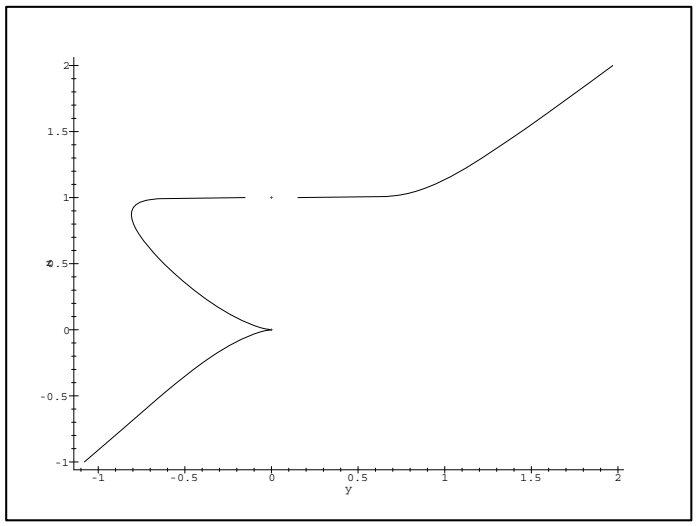
23.
G. Lachaud's model of the Klein quartic x^3y + y^3z + z^3x = 0:

$$49\,(2\,x+1)\,(-x+\sqrt{3}\,y+1)\,(-x-\sqrt{3}\,y+1) - 3\,(4-7\,x^2-7\,y^2)^2$$

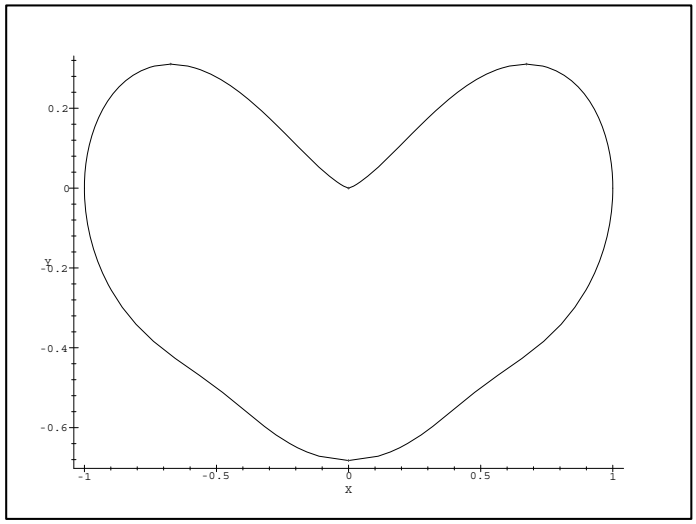


24.
Diagonal curve in F. Nicolea's lecture, (general study by J.-P. Cherdieu),
Singularity at infinity, = O in (y,z)-plane, genus = 7 by CASA / MAPLE:

$$x^3\, z^6 + y^9 - z^9$$



25.
Reciprocal radius transformation (birational) of Newton's knot curve,
Curacon Cincero (de Newton ?):



muchos gracias !

Sources:

[1] Fischer, G., Ebene algebraische Kurven, Vieweg studium, Aufbaukurs Mathematik, Braunschweig, 1994

[2] Simon, M., Analytische Geometrie der Ebene, Sammlung Schubert VIII, Gschen-Verlag, Leipzig, 1900

The pictures have been drawn with help of the MAPLE-subpackage CASA by the author.

"Newton's heart" (25.) hidden in Newtons' knot (2.) has been discovered during experimental preparatory work

dedecated to the school.